



www.ddsi.org

National Dependability Policy Environments

SWEDEN

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: Cell Network (S)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country's Information Infrastructure	3
Main ICT Regulatory and Legal Developments	4
Legislative measures aimed at enhancing ICT services	4
Initiatives for expanding access to the Internet	4
E-Government initiatives	5
Government initiatives aimed at fostering e-commerce	5
Assessment of Phenomena Undermining Dependability	6
Government Initiatives Tackling Cyber-Security	6
An Information Society for All	6
Society's Security and Preparedness	7
The Cabinet Office Workgroup on Information Operations (AgIO)	8
The Coordination of a National IT-Security Strategy	8
National Structures for Protection against Information Operations	8
The Commission on Vulnerability and Security	8
Industry and Other Non-Government Activities	10
The Industry Security Delegation (NSD)	10
The Swedish IT-industry Association (IT-Företagen)	10
Swedish Information Processing Society	10
Public-Private Partnerships	11
Research and Development	11

Overview of the Country's Information Infrastructure

Sweden is an advanced ICT country. In 1998, 203 000 people were employed in the ICT-sector; this constitutes 5,2 % of the total work force in Sweden.¹ Sweden imported ICT-products worth 10 billion EUROS in 1999, 16% of the total value of imported goods.² Sweden exported ICT-products worth 14,5 billion EUROS in 1999, which is 19% of the total value of goods exported. In the year 1999/2000, almost every individual had access to a fixed telephone in their household. 65% of the individuals have access to a mobile telephone and to a computer. 54% have access to the Internet in their households. There were 5 829 000 PSTN-subscriptions, including ASDL subscriptions by the end of 2001. The trend of private subscribers choosing to abandon PSTN-subscriptions in favour of ISDN-subscriptions has halted, although the steady rise of ISDN-subscriptions is firm. 7 out of 10 households have a mobile telephone. The number of households with access to a mobile telephone has increased during the last five years. Whilst in 1996, a third of households had a mobile telephone, in 2000, the number was up to nearly 70%.

In the spring of 2001 nearly all companies in Sweden had access to the Internet.³ 94% of all companies had access to the Internet and 97% used computers. The size of the organisation has a positive correlation with the access to Internet. All organisations with more than 100 employees have access to the Internet.

Enterprises with access to Internet and use of computers, spring 2001

Number of employees	Access to Internet	Computer usage
10-19	91%	94%
20-49	96%	99%
50-99	98%	100%
100-199	100%	100%
200-499	100%	100%
500 +	100%	100%
Total	94%	97%

The figures of Q4 2001⁴ show that the year ended with an increased growth in e-commerce. Retailers Internet-sales (B2C) have increased at the same time as their own e-procurement has increased (B2B). The retailers' Internet-sales have increased by 17% between Q3 and Q4, 2001, and out of the total volume of sales in Sweden, the percentage of Internet-sales has increased to 1,9%, which equals 750 million EUROS in annual turnover. Swedish retailers now procure 41% of their goods and services electronically, compared with 37% 6 months ago.

¹ *Private Sector ICT-statistics 2000*, Swedish Business Development Agency

² Swedish Institute for Growth Policy Studies, 2001.

³ Statistics Sweden, ICT-use in enterprise 2001.

⁴ *The Internetindikator*, Swedish Federation of Trade, March 2002.

Main ICT Regulatory and Legal Developments

The Swedish Parliament passed its Government's Bill, *An information society for all* (1999/2000:86), in June 2000.⁵ The Bill is commonly known as the 2000 IT Bill and it sets the goals for Swedish IT policy. This chapter will describe the initiatives outlined in the Bill and the progress made since 2000.

Legislative measures aimed at enhancing ICT services

The Swedish Government has invited a special commission to submit proposals for new legislation and for a regulatory authority for electronic communications. The proposals will primarily adapt the Swedish Telecommunications Act and the Radio Telecommunications Act, and prepare for the implementation of the new directives into Swedish law.⁶ The commission is to review the current policy objectives in the area and submit proposals for new legislation aimed at a horizontal and co-ordinated regulation of the electronic communications infrastructure and electronic communications services. The report is to be submitted by April 1, 2002.

UMTS has started to expand in Sweden. In December 2000, the National Post and Telecom Agency (PTS) announced licences for four operators.⁷ Six applications were rejected. Increasing the number of operators is deemed important for improving competition on the market for mobile telephone services. PTS awarded licenses using the 'beauty contest' model. The operators made comprehensive undertakings regarding geographical coverage and rollout speed.

On January 2, 2001, the EU ordinance on access to local loops came into effect.⁸ The ordinance effectively imposes an obligation on Telia AB, the largest operator in Sweden, whereby the organisation rents out its local loops under certain conditions until the market for local loops is judged to be sufficiently competitive. In addition, Telia AB is to satisfy every reasonable request for access to its local loops, to apply the same conditions to its own organisation as to external operators, and to provide access to cost-based pricing.

Initiatives for expanding access to the Internet

The PC-reform was introduced on January 1, 1998 in order to encourage people to acquire a computer.⁹ The reform meant that businesses received tax relief for the purchase of computers that they then offered to their staff, to purchase tax-free and to keep at home. The criteria for such an incentive meant that everybody with a permanent position, regardless of job title, would be included in the offer. The reform gave employees the chance to buy computers for a price far below the standard retail price. Employees paid for their computers by a deduction in their gross salary, normally over a period of three years.

The 2000 IT Bill included measures to improve accessibility to IT infrastructure in rural areas. The following examples describe some of the measures that have been implemented:

⁵ http://naring.regeringen.se/propositioner_mm/propositioner/pdf/it/p19992000_86a.pdf (visited on 21 March 2002)

⁶ *Follow-up on Swedish Government IT Policy*, Ministry of Industry, Employment and Communications, 2001.

⁷ www.pts.se (visited on 21 March 2002)

⁸ *Follow-up on Swedish Government IT Policy*, Ministry of Industry, Employment and Communications, 2001.

⁹ *An Information Society for All – a publication about the Swedish IT policy*, Ministry of Industry, Employment and Communications, 2000.

- An amendment of the Utility Easement Act to facilitate expansion of communications infrastructure with a higher transfer capacity came into effect on July 1, 2000.
- In August 2000, the Government commissioned Affärsverket Svenska Kraftnät, the national power-grid operator, to build an open backbone network in the form of fibre optical cable on their existing trunk network. The expansion is to be on commercial terms and the network is to reach the main urban centre in each municipality by December 2002.
- On January 2001, a law came into effect on tax reduction for expenses for certain rural connections for telecommunications and data communications. The tax reduction applies to property owners and businesses.

E-Government initiatives

In 1999, the Government decided that Swedish ministries and the authorities should lead by example in the use of IT in Sweden. The Swedish Agency for Public Management has been responsible for ensuring this. Its task is to reshape public administration using IT. The Internet is the basis for electronic communication between the public sector, the general public, and businesses in Sweden. Nearly 90% of the country's public institutions have their own website and can be contacted via email. In addition to communication via email, the use of public databases is also increasing and these services are free of charge.¹⁰ For a few years now *Virtual Sweden*¹¹ has been a gateway to Sweden's public sector via the Internet. The objective of Virtual Sweden is to give the population better service through a single portal to all municipalities, county councils, authorities, Government, Parliament and the EU. The Swedish Agency for Public Management is tasked by the Government to stimulate and promote the development of a 24/7 Agency which, together with public institutions, develops methods, guidance and agreements, and which can initiate and implement partnership-projects.¹²

Government initiatives aimed at fostering e-commerce

In the 2000 IT Bill, the Government set the focus on continuing initiatives on e-commerce, stating that the development of e-commerce should be led primarily by the actors on the market and that regulation should only be resorted to when industry standards and agreements are considered inadequate measures. The regulations that are introduced are meant to be technology neutral. The Bill also stated that, where regulations and formal conditions for e-commerce are concerned, it is important that agreements are reached at the international level as far as possible.

In the spring of 2001, the Government commissioned three authorities to monitor and promote the development of e-commerce.¹³ The National Post and Telecom Agency (PTS) has been commissioned to report to the Government on the its ability to stimulate e-commerce in its sector, and to report any hindrances preventing the increased use of e-commerce. The Swedish Business Development Agency has been commissioned to monitor the impact of e-commerce on the operations of SMEs, and to report any

¹⁰ An Information Society for All – a publication about the Swedish IT policy, Ministry of Industry, Employment and Communications, 2000.

¹¹ www.virtualsweden.com (visited on 21 March 2002)

¹² <http://www.statskontoret.se/projekt/projmod.htm#24>, For more information, see the report *The 24/7 Agency*: <http://www.statskontoret.se/pdf/200041.pdf> (visited on 21 March 2002)

¹³ An Information Society for All – a publication about the Swedish IT policy, Ministry of Industry, Employment and Communications, 2000.

hindrances rendering the use of electronic communication difficult for these businesses. The Swedish Agency for Public Management has been commissioned to represent the state interest in the Swedish Alliance for Electronic Commerce.

Assessment of Phenomena Undermining Dependability

During the second half of the 1990s, between 1995/96 and 1997/98, manipulation of information infrastructures in one form or another had increased by 80% and information theft by 22% in Sweden. The most prominent offences and incidents, according to Swedish surveys,¹⁴ concern computer viruses, external and internal computer intrusion, the manipulation of data, information theft and fraud. Virus attacks were the dominant incidents found in the survey. Their number had increased by 47% during the same period.

IT-related offences and incidents in Sweden, Surveys 1995–96 and 1997–98.

	1995-1996	1997-1998
<i>Virus attacks</i>	530	778
<i>Computer intrusions</i>	116	173
<i>Virus</i>		70
<i>Manipulation</i>	76	137
<i>Unauthorised use of information</i>	27	25
<i>Information theft</i>	40	49

External and internal computer intrusion is the next largest offence category in the Swedish survey, after computer virus attacks. The picture that emerges from the Swedish survey shows economic losses involving larger amounts being incurred by businesses. However, despite the potential damage that can be caused by such incidents, manipulation and information theft are regarded by just over half of the Swedish organisations surveyed to be of no major threat to their activities.

Government Initiatives Tackling Cyber-Security

The Swedish policy on cyber-security derives from two government bills: *An Information Society for All* (1999/2000:86), from March 2000¹⁵, and *Society's Security and Preparedness* (2001/2002:158), from March 2002¹⁶.

An Information Society for All

The Bill states that measures on information security are aimed at building up confidence in the new technology by facilitating research into information security. In addition, Sweden will be active in

¹⁴ *IT-related crime*, National Council for Crime Prevention, 2000.

¹⁵ http://naring.regeringen.se/propositioner_mm/propositioner/pdf/it/p19992000_86a.pdf (visited on 21 March 2002)

¹⁶ http://forsvar.regeringen.se/propositionermm/propositioner/pdf/p200102_158.pdf (visited on 21 March 2002)

international projects in this area. The Government is prioritising three areas: protection against information operations, a more secure Internet, and electronic signatures and other technology related to security.

Measures taken following the Bill's introduction:¹⁷

- In November 2000, the National Post and Telecom Agency (PTS) submitted a report on how a special unit could be set up to handle IT incidents involving central authorities.¹⁸
- The Government also commissioned the PTS to work towards an independent Internet. The study was to include a review of the organisational and legal changes needed to enable the agency to verify or ensure that the Swedish part of the Internet could function independently from functions in other countries. The report was submitted in October 2001.¹⁹
- Funds have been allocated to a secure national timing for the Internet. Time synchronisation servers have been placed at three Internet junctions in Sweden. The system will be complete when two more junctions have been constructed in 2002.
- The qualified Electronic Signatures Act came into effect on January 1, 2001. The Act incorporates the EU directive on electronic signatures.
- In December 2000, the Government tasked the National Tax Board with the initial responsibility for co-ordinating the administration and certification of electronic identification and electronic signatures in public administration. Assessment of the project is to be submitted to the Government in March 2003.

Society's Security and Preparedness

In this Bill, the Government highlighted that it is necessary that:

- Systems important to society have a high level of security and that the stakes for information security be increased
- Attacks via information systems aimed at society must be prevented
- Sweden's interests must be promoted within international work on information security

Under this Bill, the Government will establish four areas in order to enhance information security: analysis, IT-incident management, technical competence, and a system for evaluation and certification. The analysis function will be part of the remit of the new "Crisis Preparedness Agency" (no official translation yet). The IT-incident management function will be established at the PTS. A technical competence centre will be launched at the Defence Radio Institute, and the system for evaluation and certification will be implemented at the Defence Materiel Administration.

There are four reports that have subsequently formed the foundation for the Government's deliberations on cyber-security policies. These are briefly introduced below.

¹⁷ *Follow-up on Swedish Government IT Policy*, Ministry of Industry, Employment and Communications, 2001 (visited on 21 March 2002).

¹⁸ <http://www.pts.se/dokument/getFile.asp?FileID=1991> (visited on 21 March 2002)

¹⁹ <http://www.pts.se/dokument/getFile.asp?FileID=2770> (visited on 21 March 2002)

The Cabinet Office Workgroup on Information Operations (AgIO)

The Workgroup was formed in 1996, commissioned and chaired by the Ministry of Defence and consists of members from government entities and some private sector entities. The National Defence College's Centre for Information Operations Studies (CIOS) forms the Secretariat for the Workgroup. Two open reports and one classified one were published in 1997 and 1998.²⁰

The first report outlined three ideas. Firstly, the national economic well-being must be regarded as a national security asset. Second, there is a need for a coherent overview, an integrated strategic-economic analysis within the Cabinet Office, and for a statistical unit that keeps track of IT-incidents. This unit will give an operations related overview of the current situation regarding the infrastructure. The third proposal was to form a co-ordination group within the Cabinet Office, which would vouch for a coherent governmental responsibility.

The second report discussed the protective philosophy needed to safeguard critical infrastructures and information, national structures and responsibilities, and the criteria for a lead-agency. Examples given as part of this protective philosophy included the publication of the hidden statistics of IT-incidents via the formation of a public- private partnership and the establishment of a government helpdesk with responsive functions, a Government IT-incident management system.

The Coordination of a National IT-Security Strategy

The Ministry of Communications commissioned this study in 1997. The directive for the AgIO was to focus on the top-down perspective, using national security strategy as a starting-point. This study's perspective, however, was to be a bottom-up approach with IT-security forming the baseline. A report was published in August 1998.²¹

National Structures for Protection against Information Operations

The Permanent Under-secretary of Defence contracted Cell Network AB to give strategic advice on how to best structure the Government in order to have the capability to counter IT-related threats. The mission included a discussion of existing national structures and components, an identification and mapping of needs and failures in these structures, and a roadmap on how to re-structure government operations relating to the distribution of responsibilities and authorities in order to counter IT-related threats. The report was submitted in December 1999.²²

The Commission on Vulnerability and Security

This study was commissioned by the Ministry of Defence in 1999 and submitted its report *Vulnerability and Security in a New Era* in May 2001.²³ One of the Commission's assignments was to produce a strategy for enhanced IT security and protection against information operations. The report contained

²⁰ <http://www.fhs.mil.se> (visited on 21 March 2002)

²¹ Coordination of a National IT-security strategy, The Swedish Agency for Public Management, 1988, <http://www.statskontoret.se/publi/sakerhet/sakerhet.htm> (visited on 21 March 2001)

²² National Structures for Protection against Information Operations, Cell Network, 1999. (visited on 21 March 2002)

²³ Vulnerability and Security in a New Era, Ministry of Defence, 2001, http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf (visited on 21 March 2002)

recommendations for the establishment of four elements: an information security technical support team, an IT-incident management team, an intelligence and analysis unit and a system for the certification of IT products. These recommendations were then adopted in the Defence Bill.

The National Criminal Investigation Department has a computer-crime squad, which investigates cyber crime.

In its Defence Bill, the Government placed a responsibility on the Defence Materiel Administration to establish an evaluation and certification scheme based on the CCRA ISO/IEC IS-15408 (Common Criteria).

The Defence Materiel Administration would be able to:

- License evaluation-enterprises according to the principles in the CCRA
- Give support and advice when using the standard for specifications
- Supervise those organisations that were licensed
- Follow-up on on-going evaluation assignments
- Distribute certificates
- Participate in international co-operation with the aim of ensuring that Swedish certificates are acknowledged and to promote the effectiveness of the evaluation methods.

The Defence Materiel Administration shall establish the system so it can be authorised by the Swedish Board for Accreditation and Conformity Assessment (SWEDAC), which is a member of the CCRA-group. If another Swedish evaluation and certification organisation is authorised by SWEDAC, it will participate in the CCRA-group on the same conditions as the Defence Materiel Administration.

In May 2000, the Government presented a Bill entitled Act on Qualified Electronic Signatures, to the Swedish parliament (1999/200:117). The Bill entered into law in January 2001. The proposal entailed the implementation of the EC Directive on a Community Framework for Electronic Signatures (1999/93/EC). The new law serves to build public confidence in digital signatures and to encourage the use of electronic communications in society. By enhancing security for consumers and others, the Government hopes to stimulate e-commerce. The legislation also enables public administration to introduce more efficient procedures and to increase accessibility.

The legislation introduces the qualified electronic signatures. These must be based on qualified certificates. The Bill states that, in order to issue a qualified certificate, a certification service provider must notify the relevant supervisory authority.

In its Defence Bill, the Government also proposed that the National Post and Telecom Agency (PTS) should be tasked with establishing a national IT-incident management function.

PTS will initially have four assignments related to IT-incidents:

- Giving active support and guidance on time-critical, acute, IT-incidents
- Developing a system for information exchange between government agencies and the PTS with the possibility of collecting information on incidents that have occurred
- Systems should be designed so that there is a possibility for rapid distribution of information on problems that can interfere with IT-systems

- Collection and analysis of statistics on IT-incidents to be able to continually improve the case work

The Government has deemed that reporting of incidents shall not be mandatory at this stage due to current legislation on secrecy. The PTS is to establish a co-operation group with other agencies, which during 2002-2003 shall support the PTS with the implementation of its IT-incident management function.

The Government proposes in its Defence Bill that the Defence Radio Institute should form a government support-group for technical competence in the area of information security.

The Defence Research Institute should be able to:

- Support activities during IT-related national crisis
- Participate in the identification of actors involved in threats to critical infrastructures
- Do active IT-control (Red Teaming)
- Give other technical support within the area of information security.

The Government acknowledges the problem associated with having a state-sponsored actor in a functioning market, but suggests that it is imperative that when it comes to critical functions, the State has the responsibility to ensure that there is an organ with national level competence. It also makes it clear that the assignments for the Defence Research Institute do not remove the individual system-owners responsibility for information security in their own enterprises.

Industry and Other Non-Government Activities

The Industry Security Delegation (NSD)

NSD is a delegation within the Confederation of Swedish Enterprises that wants to increase co-operation and a comprehensive view on vulnerability and security issues. It is a network of enterprises, organisations and authorities with the mission to be a forum for idea-, experience-, and knowledge sharing of security-related issues. Its goal is to enhance the security and risk-awareness in both enterprises and throughout the general public, to improve legislation, and to form a public-private partnership. NSD is active within the field of dependability and information security and has drawn up a policy for establishing a private sector CERT.

The Swedish IT-Industry Association (IT-Företagen)

IT-Företagen's goal is to serve as a forum, to lobby decision-makers and to help develop the industry as a whole. One of the key areas in which it is active is in promoting IT industry credibility and responsibility. The association has a Telecommunication Security Group, which discusses strategic security topics related to telecommunications, data communications and Internet-services. The chairman of the group is the Chief Security Officer of Telia AB.

Swedish Information Processing Society

The Society is an organisation for professionals within the IT industry. It has 38 000 members and is organised in networks and special interest groups (SIG). One of those groups is SIG Security with 2 500 members, the largest congregation of information security professionals in Sweden. SIG Security develops

methodologies for creating new solutions within the area of information security and promotes awareness raising and community building.

Public-Private Partnerships

In the Defence Bill 2002, the Government concluded that there is a common interest in developing a public-private partnership with the purpose of establishing a secure critical infrastructure. Measures to enhance security in infrastructures have previously been regarded as a common good, which the state should fund, with most of the critical infrastructures being state-owned. With the new situation of national security, and the deregulated society, the Government argues that a partnership is an important step in the new structure for crisis management.

The Government wants to see partnerships established not only on a central level, but also at regional and local levels. The Bill notes that the authorities in charge should develop a partnership with the private sector for of the following reasons:

- The interests of the public- and private sectors coincide when it comes to stable and secure infrastructures
- A working partnership under normal low-threat circumstances in order to foresee and lessen vulnerabilities gives bonus-effects for crisis management and for adjustment in a changed security-environment
- The Armed Forces orientation towards a net-centric defence demands functioning civil infrastructure and a larger portion of dependability of civil resources and services

There are two existing public-private partnerships today that address dependability issues: the Industry Security Delegation and the Swedish Alliance for Electronic Commerce.

The Industry Security Delegation is described above. It could be termed a partnership since the Head of the Military Intelligence- and Security Services and the Head of the Security Police sit on the Board of the Industry Security Delegation.

The Swedish Alliance for Electronic Commerce (GEA)²⁴ was founded 1999 as a non- profit organisation and is based on membership fees for basic business. Projects are funded by members and government agencies. The security issues that GEA focuses on are electronic identification and signature, and secure payments.

Research and Development

In the Budget Bill for 2000, the Government allocated funding for new permanent places at the Royal Institute of Technology (KTH) for the years 2000-2002.²⁵ KTH planned to fill approximately half the places, corresponding to 1 275 full year students, at the IT-university. The Government also granted funding to the Swedish Agency for Innovation Systems to help finance the establishment of a centre of expertise for Internet technology at KTH. The 2000 IT Bill states that measures on information security are aimed at building confidence in the new technology by facilitating research into information security.

²⁴ www.gea.nu

²⁵ Follow-up on Swedish Government IT Policy, Ministry of Industry, Employment and Communications, 2001.

The Defence Bill states that well-developed research and development has a major impact on effective planning in the area of civil preparedness. The Government wants a better overview of the research that is undertaken within civil preparedness, severe societal strains and crisis management. The Government has tasked the new Crisis Preparedness Agency to be in charge of presenting a new R&D strategy. This strategy should be the foundation for political priorities, prioritised measures and the way in which funding should be distributed. Research areas that are especially important and, hence, prioritised by the Government includes critical infrastructure protection, crisis management and IT-security.

The major institutions doing research and development into critical infrastructure protection are:

- The Swedish Defence Research Agency
- The National Defence College
- The Defence Materiel Administration
- The Royal Institute of Technology
- The Stockholm University
- The Chalmers University of Technology

It is also important to emphasize that Swedish academic institutions are not just looking at dependability from a technological perspective. There is an increased interest in the socio-political and economic implications. More importantly, this interest does not stay inside academic circles but involves also industry and civil society as a whole. An interesting example in this context is the International Institute for Critical Infrastructures (CRIS Institute).

CRIS brings together international experts from different academic and professional background looking at the dependability and security implications of electricity national and international networks. The founding members of this institute are the Virginia Tech (USA), Institut National Polytechnique de Grenoble (INPG, France), the University of Hong Kong and Hong Kong Polytechnic University (Hong Kong), and EnerSearch (Sweden).

It is also important to present the role and function of EnerSearch AB. This is an industrial research consortium owned in equal parts by ABB Automation Products, Netherlands Energy Research Foundation, Electricidade de Portugal, ENECO Energies, EON Energies, IBM Utility Services and Sydkraft. The goal of this body is to initiate, finance and control cutting edge research dedicated to the future of energy. In this context, particular focus is directed towards issues related to the dependability of energy networks and their potential socio-economic and managerial implications.