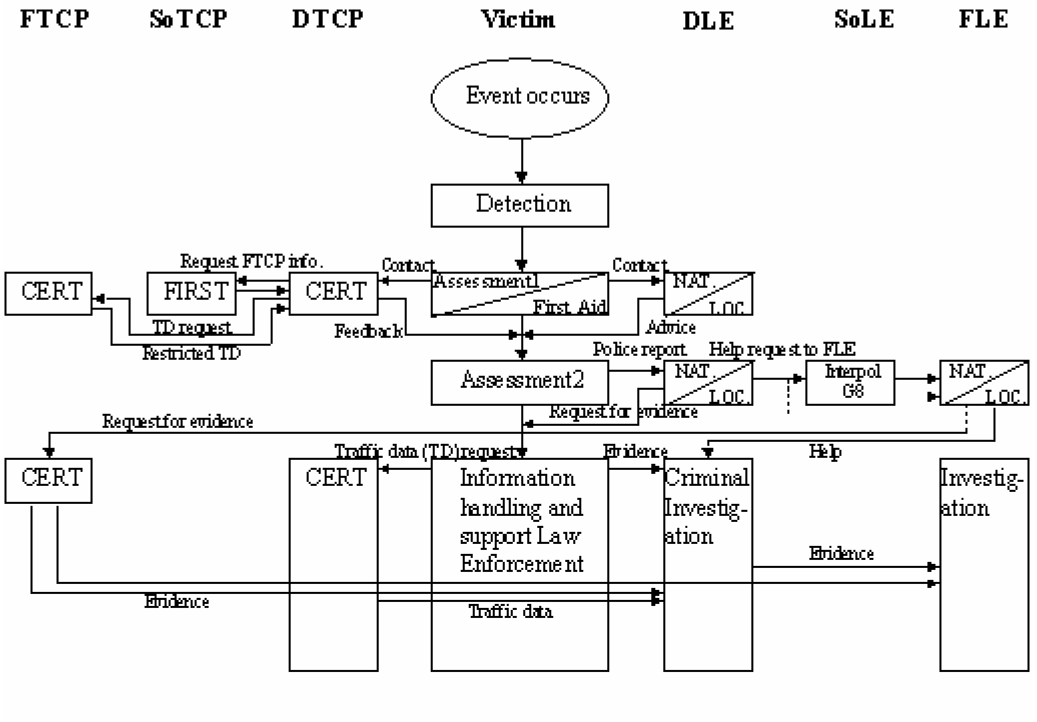
FOI
SWEDISH DEFENCE
RESEARCH AGENCY

FOI-R--1549--SE
January 2005
ISSN 1650-1942

Base data report

Henrik Christiansson, Georg Fischer

CIIP - A Swedish Perspective



Säkring Av Viktig Infrastruktur

Defence Analysis
SE-172 90 Stockholm

SWEDISH DEFENCE RESEARCH AGENCY

Defence Analysis
SE-172 90 Stockholm

FOI-R--1549--SE

January 2005

ISSN 1650-1942

Base data report

Henrik Christiansson, Georg Fischer

CIIP - A Swedish Perspective

Issuing organization FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	**Report number, ISRN** FOI-R--1549--SE	**Report type** Base data report
	Research area code 11 Policy Support to the Government (Defence)	
	Month year January 2005	**Project no.** E1740
	Sub area code 11 Policy Support to the Government (Defence)	
	Sub area code 2	
Author/s (editor/s) Henrik Christiansson Georg Fischer	**Project manager** Henrik Christinasson	
	Approved by Staffan Molin	
	Sponsoring agency Swedish Emergency Management Agency	
	Scientifically and technically responsible	
Report title CIIP - A Swedish Perspective		
Abstract (not more than 200 words) The purpose of this report is to give a general overview of critical information infrastructure protection (CIIP) in Sweden. The report is descriptive to its character and does not contain any assessment of the initiatives taken in Sweden concerning protective measures or the used Swedish procedures in connection to network-mediated attacks. The report is based on findings from two previous studies conducted at the Swedish Defence Research Agency (FOI), one in connection with a trilateral conference with UK, USA and Sweden in 2001 and one related to a contribution to an international handbook on CIIP matters in 2003.		
Keywords Critical infrastructure protection, IT-related threats, network mediated attacks, protective measures		
Further bibliographic information	**Language** English	
ISSN 1650-1942	**Pages** 41 p.	
	Price acc. to pricelist	

Utgivare

Totalförsvarets Forskningsinstitut - FOI

Försvarsanalys

172 90 Stockholm

Rapportnummer, ISRN

FOI-R--1549--SE

Klassificering

Underlagsrapport

Forskningsområde

1. Analys av säkerhet och sårbarhet

Månad, år

Januari 2005

Projektnummer

E1740

Delområde

11 Försvarsforskning för regeringens behov

Delområde 2

Författare/redaktör

Henrik Christiansson

Georg Fischer

Projektledare

Henrik Christiansson

Godkänd av

Staffan Molin

Uppdragsgivare/kundbeteckning

Krisberedskapsmyndigheten

Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel (i översättning)

Skydda av viktig informationsinfrastruktur - Ett svenskt perspektiv

Sammanfattning (högst 200 ord)

Syftet med denna rapport är att ge en allmän överblick av hur skyddet av samhällsviktig informationsinfrastruktur (CIIP) ser ut i Sverige. Rapporten är i huvudsak beskrivande till sin karaktär och innehåller inga värderingar av de skyddsåtgärder som vidtagits i Sverige eller de procedurer som aktiveras i samband med nätverksattacker. Rapporten baseras på resultaten av två tidigare studier vid FOI, en som genomfördes i anslutning till en tri-lateral konferens mellan Storbritannien, USA och Sverige år 2001 samt en som genomfördes år 2003 för att ta fram ett underlag till en internationell handbok om CIIP.

Nyckelord

Skydd av viktig infrastruktur, IT-hot, nätverksattacker, skyddsåtgärder

Övriga bibliografiska uppgifter

Språk Engelska

ISSN 1650-1942

Antal sidor: 41 s.

Distribution enligt missiv

Pris: Enligt prislista

1 Introduction

The rapid technological developments that occurred in the 1990's have brought great societal change in Sweden, as it has in other parts of the world. The technical infrastructure, including electric power supply, telecommunications and information technology systems, plays an increasingly important role in enabling us to maintain vital functions in society. At the same time, the developments in the area of information technology have meant that relatively small interest groups, criminal groups, terrorists and states with relatively weak economies are acquiring an increased attack capacity to influence IT systems, no matter where in the world these actors are actually located. These threats, like environmental threats, have no national borders and require increasing international cooperation and global solutions.

As the nature of cyber related threats and vulnerabilities in modern societies is becoming more and more trans-national there is an increased need to share information on how different countries have addressed the issue of protecting its critical information infrastructure. The purpose of this report is to give a general overview of critical information infrastructure protection (CIIP) in Sweden. The report is descriptive to its character and does not contain any assessment of the initiatives taken in Sweden concerning protective measures or the used Swedish procedures in connection to network-mediated attacks. The report is based on findings from two previous studies conducted at the Swedish Defence Research Agency (FOI), one in connection with a trilateral conference[1] in 2001 and one related to a contribution to an international handbook on CIIP matters[2] in 2003.

The report has the following structure: After this first introductory chapter the ***second chapter*** contains a general description of the threats, vulnerabilities and consequences that are associated with the ever-increasing dependence on information systems in Sweden.

The ***third chapter*** gives an overview of the most important CIIP steps taken in Sweden at the national level since the late 1990s. This includes national initiatives in general and some of the main elements of CIIP policy. Descriptions are given on specific committees, commissions and working groups, and main findings of key official reports and studies. The chapter concludes with a short discussion on legal aspects on information assurance and IT-related incidents.

The ***fourth chapter*** gives an overview of important actors in the national CIIP organisational framework and a description of some of the protective mechanisms that are established for information assurance and the management of network mediated attacks. The focus of the presentation is on organisational aspects; mechanisms that primarily are of a technical nature are not included. Information is also included on organisational structures and protective mechanisms that are established on an international level, to which Swedish actors have some connections. To conclude this chapter some notes are made on Swedish CIIP research and development.

In the concluding ***fifth chapter*** an overview is given of the procedures involved in tracing network-mediated attacks in Sweden. Depending on which network resources that has been

[1] On 20-22 of May, 2001 a trilateral conference was held in Sweden on the theme *International Cooperation for Information Assurance*. The conference was organised by the Swedish National Defence College in collaboration with the Ministry of Defence for invited high-level representatives from Sweden, Great Britain and the United States of America. In preparation for this conference FOI was commissioned in early 2001 to map the Swedish functional and legal procedures relating to tracing perpetrators of network-mediated attacks.

[2] International CIIP Handbook 2003/2004, Swiss Federal Institute of Technology Zurich, see http://www.isn.ethz.ch/crn/.

utilised and from where the attack emanates the procedures for handling an incident varies. To illustrate these procedures the presentation is based on the following three scenarios:

1. In the first scenario the attacker is only using network resources in Sweden.
2. In the second scenario the attacker uses network resources in both Sweden and other countries. In this scenario the attacker is also located in Sweden.
3. In the third scenario the attacker is located outside of Sweden and uses network resources in Sweden and in other countries.

This analysis was performed during the spring in 2001 and some of the protective mechanisms presented in the fourth chapter were not in use at that time. Though the description of the procedures involved in tracing network-mediated attacks is to our best knowledge still valid.

2 IT- related Vulnerabilities and Threats

As in many other countries, Sweden is trying to exploit the benefits of the information economy. Manufacturing industries, financial institutions, transportation providers, countless other businesses, and the central, regional and local governments have continued to build information networks that enable increased efficiency, cost reductions, and new and desirable services. For example, producers and suppliers now use electronic links and databases to lower costs through just-in-time manufacturing. Electric power and telecommunications providers have coupled their control systems to their normal information/computer networks to provide faster and cheaper services. Interconnected computer networks now often control the flow of power, water, financial services, and transportation services.

With few exceptions, these networks are vulnerable to disruption and intrusion by technology-savvy actors. Increasingly, these networks have become targets for hackers, criminals, terrorists, political extremists, intelligence organisations and other antagonists.

Experiences from security inspections made in Sweden clearly show that there are flaws in different computer network systems.

Insufficient awareness of the risks involved in computer networking means that resources are not allocated for sufficient protective security measures when networks are established. External connections often open up ‘back doors’ and increase the risk of computer intrusions. In general it could be said that there is an insufficient awareness in Sweden of security risks associated with IT systems.

As a consequence of a broadened security policy concept, the Swedish parliament decided in 1997 on a specific ambition for the preparedness against so called major societal crises. This type of situation refers to an event, or a number of events, that develop or escalate to affect multiple sectors and levels of society. The reorientation of the Swedish security policy implied an extension of the defence and emergency management systems and resources. This has affected the military sector, the civil defence and the security and preparedness of the Swedish society as a whole. The main emphasis is no longer on the supporting role of civil defence in relation to military defence. The critical infrastructure, rather than military resources, could be the primary target for a potential aggressor. The Swedish security policy aims at addressing the whole spectra of military and other threats.

In a Bill from November 1999, the Swedish Government described the IT-related threat as follows:

The threat against the information society has become increasingly important at the same time as systems and functions important to the society are becoming more dependent on information technology. The question of society’s vulnerability in this respect has a strong bearing on security policy.

Intelligence activities in Sweden emanating from foreign powers have been on the increase in recent years. It is a fact that human resources are used to a larger extent than before for such intelligence activities in the country. Furthermore, the use of technical aids for such purposes is considerable. Bearing in mind the relatively low level of protective security measures in IT-systems, this threat can be considered to be serious.

Recent developments in political extremist movement worldwide indicate several trends. Possibly the most obvious one being the increased use of network structures with trans-national extensions for the organisation of extra-parliamentary and cross-border activities with common objectives, irrespective of activist nationality. At the same time, the Internet and other IT-related technologies are used to an ever-increasing extent for communication within and between groups, and even for computer-aided attacks.

On the basis of an investigation undertaken by the Swedish National Council for Crime Prevention (BRÅ)[3] among companies, public authorities, municipalities and county councils with more than 50 employees, it appears that the number of IT-related crimes has increased with 50 per cent since 1995 and 1996. This means that every fourth organisation has been victimised. During the same period the number of connections to public networks such as Internet has almost doubled. At the same time the control and reporting systems of the various organisations have been improved. The marked increase of this kind of crime is probably explained by a combination of increased exposure to risks and a growth in control measures. The increase in IT-related crimes has occurred primarily in the private sector. It has been far less noticeable in the public sector. The majority of offences and incidents in the survey concerned computer viruses, external and internal computer intrusions, data manipulation, information thefts and frauds.

Virus attacks were the most frequent incidents found in the survey. Their number has increased by 47 per cent since the middle of the 1990's.

External and internal computer intrusions are the second most frequent offence category after computer virus attacks. The survey showed that computer intrusions have increased by 48 per cent since the middle of the 1990s. The largest increase has occurred among private companies. In this crime category the threat posed by employees (insiders) is significantly more serious than that posed by external attackers (outsiders). Despite this, companies report far more cases of outsider intrusions to the police than insider intrusions, the proportion being 60:40. One reason for this may be that companies prefer to deal with insider intrusions themselves. Another reason could be that they fear that their reputation could be damaged if it would be known that a serious IT-crime has occurred. According to the survey a total of 239 incidents of external or internal computer intrusions were reported to the police during the years of 1997 and 1998.

Data manipulation and theft of information are incidents that companies did not consider being particularly widespread. Even so, these kinds of incidents can potentially cause extensive damage and must therefore be taken seriously. Information on product development, marketing, contracting, staff, etc. has a significant commercial value to a company. The picture that emerges from the BRÅ survey indicates that organisations have suffered considerable economical losses due to these incidents. Since 1995, the manipulation of data in one form or another has increased by 80 per cent and information theft by 22 per cent.

In the BRÅ survey the estimated value of the total damage caused by IT-related crime and misuse amounts to between USD 5–20 million. The average cost of damage to a victimised company is on a yearly basis approximately USD 12,200.

Despite the potential damage that can be caused by data manipulation and information theft, more than half of the surveyed companies and public authorities did not consider these crimes to be major threats to their activities.

In the survey, more than half of the IT-related incidents reported to the police (329 of 608) during 1997 and 1998 concerned fraud via the Internet. The most common form of fraud was unauthorised use of other people's Internet connections or the buying of products and services through the Internet using another person's credit card information. A considerable increase

[3] *IT-related crime* (in Swedish), BRÅ-report 2000:2.

in reported Internet related frauds occurred between 1997 and 1998. Private persons reported a majority of these frauds. When it comes to reporting information theft nearly half of all companies, public authorities, municipalities and county councils lacked appropriate routines.

Other IT-related offences reported to the police during 1997 and 1998 included threats and harassment (7 reported), physical sabotage (16) and violations of protection of personal integrity (17).

When it comes to virus attacks and computer intrusions it seems that most of the offences and incidents are the work of outsiders. When these offences – which are the most common – are excluded, it is insiders (63 per cent) who are responsible for the remaining offences and incidents, for example data manipulation, information theft, etc.

2.1 National CIIP Initiatives, Policy and Legislation

Critical information infrastructure protection issues have been on the security policy agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures, as electric power systems and telecommunication systems, have been implemented since at least the end of WWII. The vulnerability problems that is associated with society’s increasing dependence on IT and information infrastructures was early identified as an area of relevance for national security. In addition, the management of IT-related vulnerabilities has been discussed since the beginning of the 1970´s. The present Swedish policy on CIIP can be derived from these historical developments and from some more recent initiatives as described in this chapter.

2.2 CIIP Initiatives

2.2.1 The Cabinet Office Workgroup on Defensive Information Operations

On 12 December 1996, the government appointed a working group on defensive information operations within the cabinet (AG IO/IW). In addition to the representatives from the cabinet office and ministries, the group also included representatives from relevant private companies and organisations. The tasks of the working group were to monitor developing threats and risks within the area of information warfare and to disseminate information about these matters. The working group prepared a proposal on how to assign responsibilities and to formulate guidelines for a strategy for protection against information operations. During its existence the working group presented two main reports. Today the group has ended its work and some of their tasks have been transferred to the Swedish Emergency Management Agency, see below.

2.2.2 Commission on Vulnerability and Security

Following a decision on 23 June 1999 the Swedish Government authorised the Minister of Defence to appoint a Special Investigator to head a commission of inquiry with a mandate to analyse and submit proposals for principles concerning a more integrated approach to civil defence and emergency preparedness planning.[4] The findings and proposals of the Commission on Vulnerability and Security, as presented in May 2001, has been the most important step in the implementation of a new structure for civil defence and emergency preparedness planning in Sweden.

With regard to a strategy for improving the general stability of critical technical infrastructures the commission suggested several measures. In its final report the Commission also proposed measures designed to specifically enhance information assurance and improve protection against information operations. The Commission noted that, unlike many other countries, Sweden lacked a coherent system for dealing with serious IT threats. On the basis of experience in other countries, the Commission considered it necessary to establish a new organisational structure for information assurance. This structure was to be established following the government bill on Society's Security and Preparedness, see below.

In the Commission's view, the central government must assume responsibility in these areas. At the same time, the Commission emphasised that all managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and provide functions and facilities that are beyond the resources of other sectors in society.

2.2.3 Committee on Electronic Communications

Through a decision on 19 April 2001 the Swedish Government authorised the institution of the Committee on Electronic Communications.[5] The task was to review the policy objectives, analyse the legislation and to propose new legislation as found necessary, with an orientation towards a coordinated regulation of the whole area of electronic communications infrastructure and services. In its interim report the committee proposed a new comprehensive formulation of the policy objective for the electronic communications sector, amongst them was:

- Electronic communications shall be so efficient that they promote growth, increase Swedish competitiveness and contribute to enhanced productivity in society.
- Individuals and authorities shall have the greatest possible access to efficient and secure electronic communications with the best possible options, price and quality. The primary means to achieve this is through efficient competition.
- The policy for electronic communication shall also ensure that individuals are able to contact emergency services, the protection of personal integrity, the sustainability and accessibility during major societal crises and in a state of enhanced preparedness or war.

In addition, the policy shall also promote sustainable development towards a healthy and good environment and harmonise with international policies.

[4] The Swedish Commission on Vulnerability and Security. Vulnerability and Security in a New Era – A Summary. (SOU 2001:41, Stockholm, 2001). http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf.

[5] Committee on Electronic Communications, SOU 2002:60, http://www.regeringen.se/propositioner/sou/sou2002.htm

2.2.4 Committee on Information Assurance in the Swedish Society

Through a decision on 11 July 2002 the Swedish Government authorised the institution of the Committee on Information Assurance in the Swedish Society. The committee was given the task to present an assessment of the need for information protection within critical functions in society and to give a proposal on organisational matters of the Swedish signal protection service. In addition to this the committee was given the tasks to submit proposals regarding:

- The development of a national strategy for information assurance,
- The form and focus of the future Swedish engagements in international cooperation on information assurance,
- How to implement the OECD Guidelines for the Security of Information Systems and Networks.

The committee is also expected to monitor the implementation of information assurance measures within state agencies in accordance with the government bill on Society's Security and Preparedness (see below).[6] The committee will finish its work during 2005.

2.2.5 Committee on Joint Radio Communication for Public Safety and Security

At present there is no single radio communication infrastructure in Sweden for public safety and security (PSS), i.e. emergency services. There exist about two hundred different systems for radio communication within the domain of PSS in Sweden. These systems are primarily adapted to the needs of their owners, which is something that prevents the much-needed coordination of different emergency service organisations. This further complicates the radio communication across national borders, which has increased in importance in light of the EU collaboration and other international commitments. Often, the systems are technically outdated.

In light of this, and other issues, the government authorised the institution of the Committee on joint radio communication for public safety and security through a decision on 10 June 2002. In January 2003 the committee presented its report on organisational, economical and technical aspects on the matter[7]. In September 2003 the government decided to allocate the necessary funding to finance a new radio system for PSS. In December 2003 it was decided that the Swedish Emergency Management Agency shall implement, manage and develop the system. The radio system will be based on the Tetra standard and is initially intended for the police, coast guard, emergency service and the Swedish armed forces. The construction of the technical systems will be made in stages and will be completed in 2009.

2.3 CIIP Policy

The aim of the government's policy on telecommunications is to give people and Swedish authorities access to reliable and effective electronic communications. Everyone should have access to telecom services on equal terms. The communication systems shall also be robust and accessible during situations of crisis and war.[8] Robust telecommunications shall be achieved through long-term and systematic preparatory efforts. The government stresses that

[6] Government Bill 2001/02:158.

[7] Committee report "Trygga medborgare - säker kommunikation", SOU 2003:10, Stockholm, Sweden.

[8] Government Bill 2001/02:158 and 2002/03:110.

it is essential to continuously analyse how the changed threat spectrum and the evolution of the telecommunication infrastructure affects the need for measures and to take necessary steps to ensure a robust and secure infrastructure.

2.3.1 Government Bill "An Information Society for All"

The Government bill "An Information Society for All"[9] defined the Swedish overall IT policy objectives. It stated that Sweden should become the first country to create an information society for all. The Swedish government proposed that for the purpose of creating an information society for all, state investment should be focused primarily on three areas: regulatory systems, education and training, and infrastructure.[10]

2.3.2 Government Bill on Society's Security and Preparedness

In March 2002 the government presented its bill on the Swedish security and preparedness policy. The bill was to a large extent based on the findings and proposals of the Commission on Vulnerability and Security (see above).

In the bill the government presented a framework for a new planning system for the preparedness for major societal crises and for activities specifically related to the threat of war. Further, the bill gave an account on how the crisis management structure in society will be strengthened. All of this has implications on the assurance of critical infrastructures in general and on critical information infrastructures in particular.

As formulated by the government the goal for the work on IT-security should be to maintain a high degree of information assurance in Sweden, which means that it should be possible to prevent and manage disruptions in critical societal functions. The strategy to achieve this goal should be based, as for other crises management in Sweden, on the principles of responsibility, parity and proximity.

The principle of responsibility means that whoever is responsible for an activity under normal conditions should assume corresponding responsibility in crises or times of war. This means that the activity's robustness has its foundation in society's basic capacity and that measures are then taken on the basis of the entire threat spectrum, from major societal crises to state of enhanced preparedness and war.

The principle of parity implies that as far as possible, during crises or war, authorities should be organised and geographically located as in normal, peacetime circumstances.

The principle of proximity means that crises should be dealt with at the lowest possible level. With regard to IT-security the principle is that the owner of an information system also has the responsibility to make sure that the system has an adequate level of security so that the system can maintain critical operations. One important role for the state is therefore to cater for the overall need of information assurance in Sweden and implement those measures that reasonably cannot lie with individual system owners.

Based on the findings and proposals of the Commission on Vulnerability and Security the government presented a new organisational structure for Swedish information assurance (see also chapter 3):

[9] Government Bill 1999/2000:86 "An Information Society for All".

[10] Ministry of Industry, Employment and Communication. An Information Society for All. Fact Sheet No. 2000.018. (March 2000).

- The overall responsibility for information assurance and for policy intelligence and analysis in the public sector rests with the Swedish Emergency Management Agency.
- A Computer Emergency Response Team is established at the Swedish National Post and Telecom Agency. The team is engaged in monitoring IT incidents; gathering statistics and, when necessary, provide warnings to IT-system owners.
- An Information Security Technical Support Team manned by experts and support staff with a high level of technological expertise is established at the Swedish National Defence Radio Establishment.
- A system for security-oriented evaluation and certification of IT products and systems is established at the Swedish Defence Materiel Administration.

2.4 Legal Aspects on Information Assurance and IT-Related Incidents

Over the years several different laws have been implemented to handle some of the specific risks that are associated with information technology systems and their uses, e.g. the Data Protection Act, the Personal Data Act, the Bulletin Board Systems Act, the Protection of Business Secrets Act and the Secrecy Act.

Sweden was the first country to implement a Data Protection Act (SDPA). The act originates from 1972 and was adjusted 1998 to conditions in the European Community. The Data Protection Act was abolished 1998 and replaced by the Personal Data Act. These sections in the Data Protection Act that concerned IT-related crime were transferred to the Swedish Criminal Code.

The Personal Data Act (PDA) regulates the handling of personal data, in both electronic and non-electronic form. This act is based on European Community directives concerning personal data. The guiding rule in PDA is that information concerning a person can only be used with that person’s specific permission or if there is a legitimate interest from the owner of the register. The PDA also contains restrictions regarding publication of personal data on the Internet. The Swedish Data Inspection Board has relaxed some of these restrictions because there has been quite extensive criticism against PDA.

The creation of the Bulletin Board Systems Act was due to a need to prevent the dissemination of child pornography and racial discriminating material. This act regulates services, which the service provider have control over, for instance a web based chat site. A normal web site however is not covered by the act. The act states that the service provider is responsible for keeping a reasonable watch over the content.

The Protection of Business Secrets Act regulates the secrecy regarding business secrets. The Public Secrecy Act regulates the secrecy regarding public authority secrets. This act is quite extensive.

A criminal investigation of a suspected criminal activity can only be initiated when a formal police report has been filed. In order to file a report the victim must, in a legal sense, state what kind of offence that is at hand. This is something the police usually help the victim with.

The terms IT crime and IT-related crime do not have a legal meaning in the Swedish justice system. These terms just denotes crimes that are related to information technology. The actual offence sorts under different acts of the Swedish law, which are neutral to how the crime was committed, be it with or without assistance of information technology. An attempt to classify computer related crimes and their relation to the Swedish law could be found in Appendix 1.

There are some laws though which aims at specific IT-related crimes, e.g. computer related fraud and computer intrusions.

In Sweden the courts use two concepts that could be translated into the concepts of *free submission of evidence* and *free interpretation of evidence.*

The telecommunications act of 1993[11] regulates the activities of the telecommunication providers. The most important parts are the section 44-49, which regulates confidentiality in relations to telecommunication subscriptions, traffic data and contents of messages. For the purpose of this report these sections and some related sections of the Telecommunication Act are reproduced in appendix 2.

In 1999 the Swedish parliament made an alteration to the Telecommunication Act that telecommunication providers should be called upon to destroy telecommunication specifications after they have received payment from the subscriber. Normally these specifications contain information about who is calling who and the start and end times of the call. The change to the act makes it practically impossible to trace a perpetrator. Due to the long handling times of incident investigations, at present[12] twelve to eighteen months, the legal authorities is not able to make tracing requests during the short period of time when the traffic data would be available. The victims usually do not discover the crime/incident in time before the specifications are erased. The increased use of the flat rate service accentuates this problem.

2.5 Legislative Update 2003

During 2003 the electronic communications act (SFS 2003:389) have replaced the telecommunications act of 1993 (SFS1993:597). The new act regulates the technical infrastructure but not the contents of the information services. The purpose is to establish a regulation that is unitary and neutral concerning different technical solutions.

The starting-point for the new legislation is that the regulation process should be more flexible. The new legislation therefore contains fewer general obligations for electronic communication providers than the former legislation. The new legislation contains tools for the Swedish national regulatory authority (the Swedish National Post and Telecom Agency) to decide on specific obligations for electronic communication providers. This will make the regulation more flexible because it is easier for the regulatory authority to decide upon a decree than the Swedish parliament to change the legislation.

In addition to this it can be noted that the Commission on Vulnerability and Security concluded in its final report that there is a need for legislative amendments in order to support the commission's proposals with respect to IT-security and the protection against information operations. A need for legislative amendments is particularly seen in the following areas[13]:

- Statutory and administrative provisions relating to the activities of local authorities and country administrative boards during major crises,
- The possibility of reallocating resources in the health services during major crises,

[11] Note that the Telecommunication Act of 1993 have been replaced by the Electronic Communications Act of 2003. Due to the fact that the main part of this study was done in early 2001 it was important to include the text on the Telecommunication Act in order to maintain consistency between different parts of this report.

[12] Early 2001.

[13] Swedish Commission on Vulnerability and Security, Vulnerability and Security, 20-21.

- The need for stricter safety regulations and for more effective supervision of the power suppliers.

The government has decided to review the legislation relevant to CIIP and Emergency Management.

3 CIIP Organisations and Protective Mechanisms

In general, there is a wide spread awareness among both private and public organisations of the importance of good IT-security practises. In the private sector there are several organisations promoting risk management and the adherence to different standards, e.g. BS7799 (in Sweden SS627799). The proportion of companies that have adopted preventive measures against computer intrusions from outsiders has increased from 40 per cent to just over 65 per cent in the span of just a few years. Though, the private sector lags behind the public sector in preventing external computer intrusions. When it comes to reporting information theft nearly half of all companies, public authorities, municipalities and county councils lack appropriate routines.[14]

This chapter contains a general overview of the organisational structure and some of the protective mechanisms that are established in Sweden for information assurance and the management of network mediated attacks. The focus of the presentation is on legal and organisational aspects. Mechanisms that primarily are of a technical nature are not included in this report. The different governmental agencies and organisations that have responsibilities in the area of critical information infrastructure protection are presented below under the heading of the ministry that they are affiliated to.[15] The newly assigned and specific responsibilities for CIIP at the Swedish Emergency Management Agency, the Swedish Defence Material Administration, the Swedish National Defence Radio Establishment and the Swedish National Post and Telecom Agency are presented in some depth. To provide insights into some of the protective mechanisms a major Swedish telecommunication provider has implemented a short presentation is given on Telia[16].

This chapter also includes information on organisational structures and protective mechanisms that are established on an international level, to which Swedish actors have some connections. To conclude this chapter some notes are made on Swedish CIIP research and development.

3.1 Ministry of Defence

3.1.1 The Swedish Emergency Management Agency (SEMA)

The Swedish Emergency Management Agency[17] was established on 1 July 2002, with the purpose of coordinating work on the civil preparedness to manage major societal crises, enhanced preparedness and war. When it was formed, SEMA took over some of the tasks from the Swedish Agency for Civil Emergency Planning and the National Board of Psychological Defence. SEMA presents proposals to the Government on the allocation of resources and then distributes funds to authorities with emergency management responsibilities. This includes directing, coordinating and evaluating measures taken.

[14] *IT-relaterad brottslighet* (“IT-related crime”), BRÅ-report 2000:2.

[15] The issue of responsibilities of the Swedish Government is somewhat complex due to the fact that the constitution is based on small ministries and strong, independent agencies. The government agencies are formally subordinated only to collective Cabinet decisions (where at least five ministers must be present) - not to the minister concerned or the Cabinet Department. This is important to have in mind when reviewing the organisational structure in Sweden.

[16] The presentation is based on a study made in early 2001, since then Telia and the Finish company Sonera have formed TeliaSonera.

[17] http://www.krisberedskapsmyndigheten.se/english/index.jsp

SEMA analyses the development of society, and the interdependency of critical societal functions. In order to ensure that emergency management takes this interdependency into account, planning and resource allocation for peacetime emergency preparedness and civil defence are organised in six areas of coordination:

- Technical infrastructure,
- Transport,
- Spreading of dangerous infectious substances, toxic chemicals, and radioactive materials,
- Economic security,
- Overall coordination, cooperation and information,
- Protection, rescue, and care.

In each area, a number of public authorities are represented and they coordinate their activities to reduce vulnerabilities and to enhance emergency management capabilities. SEMA also promotes cooperation between the public and private sectors.

The agency also coordinates and initiates research and development within the field of emergency management and has the overall governmental responsibility for information assurance in Sweden. Within SEMA the Information Assurance Department mainly manages the latter task and the Research and Analysis Department handles the former task.

SEMA/The Information Assurance Department

Some of the main activities of the Information Assurance Department can be summarised as follows:

- Annually prepare an overall assessment of the information assurance status in Sweden,
- Initiate and contribute to cooperation between governmental organisations, private companies and other important actors within the area,
- Gather, analyse and disseminate open source information related to information assurance,
- Develop preventive IT-security recommendations (consistent with ISO/IEC 17799) that will support other organisations IT-security activities
- Initiate research and development in the area and summarise risk and vulnerability assessments of different important societal systems,
- Managing the Board of Information Assurance (see below).

The Information Assurance Department is continuously developing these and other activities.

SEMA/The Board of Information Assurance

The Board of Information Assurance has been established to support SEMA's activities in the information assurance area. This board will establish a network of skilled experts from a variety of important organisations within the area. The board is replacing the former Cabinet

Office Working Group on Information Operations.[18] The board's primary task is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the information assurance area,
- Suggestions and viewpoints concerning direction, prioritising and realisation of SEMA's activities in the information assurance area.

Additionally, the members of the board are encouraged to disseminate information about SEMA's activities in the area.

3.1.2 The Swedish Defence Material Administration (FMV)

The Swedish Defence Material Administration[19] is the Swedish procurement agency for the armed forces. FMV has been involved in the area of IT-security Evaluations since 1989, performing in-house evaluations of equipment that are intended to be used by the armed forces.

FMV Certification Body for IT-security (FMV CB)

In the summer of 2002 FMV was tasked by the Government to establish a Swedish scheme for evaluation and certification of IT-security products intended for use within Swedish governmental organisations. The establishment of the Certification Body at FMV[20] is planned for the period 2003-2004. The first trial certification is planned to take place during 2003.

Evaluations will be performed according to the international standard ISO/IEC 15408 Evaluation Criteria for IT-security, a.k.a. Common Criteria (CC).

FMV CB is promoting increased understanding and competence in CC Evaluations and organises CC training events. Currently FMV has initiated preparatory licensing for two Swedish companies that are starting up IT-security Evaluation Facilities.

In connection with this it is important to mention the Swedish Board for Accreditation and Conformity Assessment (SWEDAC), affiliated to the Ministry of Foreign Affairs. SWEDAC is the Swedish signatory of the agreement of mutual recognition of conformity assessment of certification according to 'Common Criteria'. The division of responsibilities between FMV CB and SWEDAC is at present not established.

3.1.3 The Swedish National Defence Radio Establishment (FRA)

The Swedish National Defence Radio Establishment[21] is the Swedish signal intelligence organisation. It is a civil agency directly subordinated to the ministry of defence. The Information Security Technical Support Team is associated with FRA.

[18] SEMA document 0160/2003: Account of what measures that have been accomplished to take over the responsibilities from the working group on Information Operations (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

[19] http://www.fmv.se

[20] http://www.fmv.se/cb/index.asp?K=016&L=UK

[21] http://www.fra.se/english.shtml

FRA/The Information Security Technical Support Team

The Information Security Technical Support Team consists of twenty experts in the field of IT-security. Roughly half of the group is engaged in research and development; and supporting activities in the event of an IT-related emergency.

The team is specifically intended to support:

- Crisis management in situations of national crises when IT-security qualifications is needed,
- Identification of persons and organisations that are involved in IT-related threats against critical systems.

On request, the team supports Swedish authorities, agencies and state-owned corporations, which are responsible for critical functions in the Swedish society, with IT-security expertise and services. The customised services consist of penetration tests, computer forensic investigations, source code analysis, IT-audits, risk analysis etc. The team cooperates on regular basis with organisations within the national and international IT-security community.

3.1.4 The Swedish Armed Forces

The Armed Forces[22] must be able to quickly respond to different types of threats and risks. The Swedish Parliament has therefore decided that the Armed Forces are to be developed according to the concept of Network Based Defence. This places a great demand on the information infrastructure concerning availability and security. The Armed forces are therefore pursuing a considerable amount of work through for instance research and development in such areas as IT-security and information infrastructure.

The Swedish Military Intelligence and Security Service handle matters concerning the peacetime operational work related to IT-security in the armed forces. In addition, there is a group, the National Communications Security Group (TSA), which offers advice and control of cryptographic systems in Swedish defence organisations and industries.

3.2 Ministry of Industry, Employment and Communications

3.2.1 The Swedish National Post and Telecom Agency (PTS)

The Swedish National Post and Telecom Agency is the governmental authority that monitors all issues relating to the Information Communication Technology (ICT) and postal services. One of their key tasks is to ensure the development of functioning postal and telecom markets. The Department of Internet and Security within PTS is responsible for security issues concerning ICT.

PTS/Department of Network Security

The department of Network Security is tasked with monitoring developments concerning security issues and implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned following consultation with the ICT operators, the Swedish Armed Forces and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for managing the .se-domain

[22] http://www.mil.se/

autonomously have been installed within the Swedish borders. Associated with this department is the Swedish IT Incident Centre.

PTS/The Swedish IT Incident Centre (SITIC)

In May 2002 the Swedish Government tasked PTS to establish the Swedish IT Incident Centre.[23] The Centre was officially opened on 1 January 2003. SITIC supports national activities for the protection against IT-incidents by:

- Operating a system for information exchange on IT-incidents between both public and private organisation and SITIC,
- Rapidly communicating information to society on new problems that can disrupt IT-systems,
- Providing information and advice on preventive measures,
- Compiling and publishing incident statistics as an input to the continuing improvements of preventive measures.

3.3 Department of Justice

3.3.1 The Swedish National Police Board (NPB)

In organisational terms, the Swedish police sorts under the Ministry of Justice. The National Police Board[24] (NPB) is the central administrative authority of the police service and supervises the police service. The National Criminal Investigation Department (NCID) and the Swedish Security Service come under the National Police Board.

[23] http://www.sitic.se/index.html

[24] http://www.polisen.se

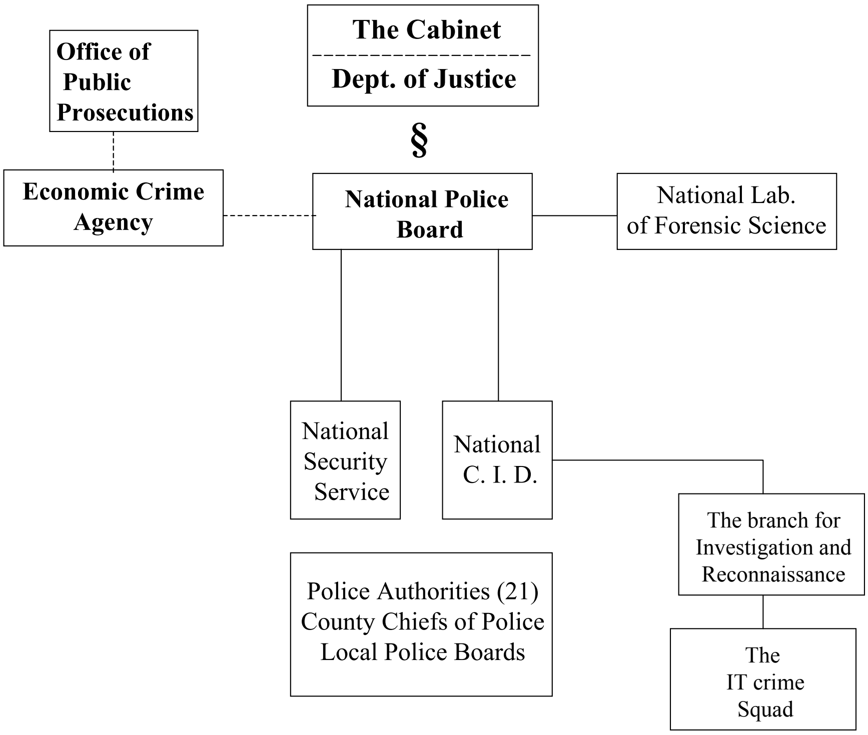


Figure 5: Parts in the Swedish police organisation related to investigations of IT crimes

The NPB is the supervisory authority of the National Laboratory of Forensic Science. The laboratory carries out forensic analyses primarily for the police service, but also undertakes assignments for other authorities and organisations. The laboratory conducts research and methodological development work, arranges training in forensic techniques and develops forensic methods of work. Cooperation with forensic laboratories in other countries, mainly in Europe, has been developed and intensified in recent years.

NPB/National Criminal Investigation Department (NCID)

Within the NPB, the National Criminal Investigation Department is responsible for the operational functions of surveillance, investigation and criminal intelligence work that are not the responsibility of the Swedish Security Service or the Economic Crime Agency.

The National Criminal Investigation Department consists of four branches, the secretariat, crime intelligence service, investigation and reconnaissance, and the branch for public order.

The unit for investigation and reconnaissance shall support NCID, foreign and international crime preventing organisations and local Swedish police departments with advanced investigation, reconnaissance and identification recourses. The IT crime squad is a part the branch for investigation and reconnaissance. This squad has specialist knowledge for investigating IT criminality. This squad shall develop the national support to the local Swedish police departments when it comes to investigation of IT criminality, participate in education of parts of the judicial system, assemble and communicate information about IT criminality. The Internet reconnaissance unit is linked to this squad.

In 1985 the US Federal Bureau of Investigation (FBI) trained the first Swedish police officer in IT crime investigations. The first organisational IT crime unit within the Swedish police was established 1986, the so-called computer crime unit. In 1993 Interpol appointed this unit as the national central reference point (NCRP) in Sweden, a so-called Interpol NCRP. In 1998 this unit was converted to a detached squad within NCID. The squad is a part of the G 8 network of 24/7 contact points since 1999. The composition of the squad staff is for the moment, one squad chief, one operational chief, eight detective investigators, two field technicians and one administrator. There are also project activities with time-limited employment and also part-time employees.

The IT crime squad has been training police officers from local police departments for some time now, to become specially qualified to perform IT crime investigations. The main education consists of twelve plus three weeks of training concerning tools and methods in IT crime investigations. Approximately 60 police officers have participated in this training. In addition 15 prosecutors have attended the training. The IT crime squad is of the opinion that it is essential that all parts of the judicial system understand the features of an IT crime investigation.

In 1999 there were approximately 320 investigations of which 160 where preliminary investigations. In 2000 there were 333 investigations. The most frequent IT crime up to 1998 was related to serious narcotic crimes. The most frequent IT crime 1999 was related to crimes of violence. The most common setting was the Internet.

The IT crime squad has participated since 1993 in the *Interpol European Working Group on Information Technology and Crime*. They cooperate with international and national organisations such as *Interpol* and *G 8, Europol, the International Organisation on Computer Evidence (IOCE)* and *US Federal Bureau of Investigation (FBI).* There is a special cooperation with the other Nordic countries.

The IT crime squad performs reconnaissance on the Internet only in connection with specific operations.

The IT crime squad participates in the tracing and identification of the perpetrator, searches of premises, forensic investigations and interrogations. They are acting as a bureau for advice and they support activities with their technical skills.

3.3.2 NPB/The Swedish Security Service (SÄPO)

The fundamental responsibility of the Swedish Security Service (SÄPO) is to prevent and detect crimes against the security of the Realm. Its prime task is crime prevention. This means that a very large part of SÄPO's resources are allocated to protective security, the aim of which is to create the necessary conditions for a high level of protection and to make intervention possible at an early stage when matters threatening the security of the Realm are discovered. This covers advisory and training activities but also other measures such as technical support and protective surveillance. SÄPO is engaged in four main fields of activity: *protective security* (including personal protection*), counter-espionage, counter-terrorism and protection of the constitution*. Whenever IT criminal activity touches upon those fields the Swedish security service is involved.

3.4 The Government Office

3.4.1 The Swedish Agency for Public Management

The Swedish Agency for Public Management[25] conducts studies and evaluations at the request of the government and modernises the public administration with the application of ICT. The agency helps to develop the Swedish administrative policy and also ensures that the electronic infrastructure in the public sector is open and secure.

The report *The 24/7 Agency - Criteria for 24/7 Agencies in the Networked Public Administration* proposes a four-stage agency development plan towards fulfilling the aim of enhancing accessibility and providing service round the clock, seven days a week. The criteria recommended by the agency focus primarily on government agencies' capacity to provide interactive services for the public and businesses. Specifically related to IT-security, the agency has compiled a strategy for the society's information assurance[26] and produced a publication on secure authentication[27]. During the year 2003 the agency is carrying out the project "Information Security at authorities". This project aims at supporting other authorities with methods and tools to implement analysis of threats and risks according to ISO 17799.

3.5 Public and Private Cooperation

3.5.1 The Swedish Emergency Management Agency approach

SEMA promotes interaction between the public sector and the business sector, and works to ensure that the expertise possessed by non-governmental organisations is taken into account in emergency management.

There are two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and the aforementioned Board of Information Assurance. However, it has not yet been established how the CIIP public-private partnership will be institutionalised.

3.5.2 The Industry Security Delegation (NSD)

The Industry Security Delegation[28] is a delegation within the Confederation of Swedish Enterprise (Svenskt Näringsliv) whose objective is to increase cooperation between companies, organisations and authorities; and promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness within the general public and the companies. To help their members with security issues the NSD is arranging courses in information assurance, crisis and risk management.

[25] http://www.statskontoret.se

[26] *Coherent strategy for the society's information assurance* (Sammanhållen strategi för samhällets IT-säkerhet, rapport Statskontoret rapportserie, 1998:18).

[27] *Security related to electronic identification* (Säkerhet med elektronisk identifiering, rapport i Statskontorets rapportserie 1999:30).

[28] http://www.svensktnaringsliv.se/index.asp?pn=155246

3.5.3 The Swedish Information Processing Society (DFS)

The Swedish Information Processing Society[29] is an independent organisation for IT professionals with 32 000 members. DFS owns the product family SBA[30] for information security, which are products focusing on risk analysis and information security. SBA is said to be a Swedish de facto standard.

3.6 Domestic Telecommunication Providers

In Sweden there are more than fifty Internet service providers (ISP). Among them there is great variety in size, experience and competence in IT-security. Therefore, it is difficult to give a general description of the protective mechanisms within a Swedish ISP. In his section the major Swedish telecommunication provider Telia[31] is presented with its protective mechanisms regarding information assurance. This should serve as a description of an organisation with great experience in incident handling.

In the 1990's the Swedish publicly owned and managed telecommunication provider Televerket, was converted to a public limited company, Telia AB, with the Swedish government as the major shareholder.

In Sweden, Telia provide data, voice, Internet, intranet, extranet, and a broad range of other services to 4.3 million residential, business and public sector subscribers. Telia have extended their services to markets all over the world, with activities in approximately thirty countries.

Telia have a 30,000-kilometer IP network, covering 15 European countries and have access to 18,000 kilometres of infrastructure in North America.

One unit is responsible for handling computer/network security, which is managed by Telias Computer Emergency Response Team Co-ordination Centre (Telia-CERT CC) in Stockholm. This group co-ordinates subCERT's which are distributed throughout the company.

The history of Telia-CERT CC starts in 1983 when the first security manager in automatic data processing was hired. From 1986 to 1998 the computer security activities in the company continuously grew, but under different names. In 1998 the Telia-CERT CC was constituted in its present form. In 1999 they joined the *Task Force of Computer Security Incident Response Teams* (TF-CSIRT) – former EuroCERT, and in 2000 they became a full member of the *Forum of Incident Response and Security Teams* (FIRST).

Telia-CERT CC activities are divided into three categories, *preventive actions, operational actions* and *co-ordinating activities*.

Preventive actions consist of for instance; gathering intelligence and statistics, identifying flaws in operating systems, dissemination of information about protective measures, lecturing, consultations and the organisation of sub-CERT's.

Operational actions include research on intrusion techniques, execution of penetration tests, actively tracing intrusions, and developing computer forensics and consulting services such as creating incident handling and response units.

[29] http://www.dfs.se/

[30] SBA is an abbreviation for the Swedish word SårBarhetsAnalys, which stands for vulnerability assessment.

[31] The presentation is based on a study made in early 2001, since then Telia and the Finish company Sonera have formed the TeliaSonera corporation.

Coordinating activities within Telia consists of, for instance, supervision of incident response organisations and subCERTs. The Telia CERT CC also coordinates the reporting to the police on IT-related incidents and they testify in court, if necessary. This naturally leads to contacts with the Swedish National Police Board (NPB) and the Swedish Security Service. Finally, Telia CERT CC coordinate their activities with national and international organisations, such as the *Federal Bureau of Investigation* (FBI), the *Forum of International Irregular Network Access* (FIINA), the *Forum for Incident and Response Security Teams* (FIRST), the *National Criminal Intelligence Service* (NCIS), and the *National Aeronautic Space Administration* (NASA).

Telia-CERT CC handles approximately five hundred security incidents every year. In these security incidents Telia is the victim or the origin of the security incident could be from some point within Telias network. Abuse of Telias Internet services is handled by the appropriate subCERT. They handle incidents where a subscriber to Telia's Internet services is abused or causes abuse. The range and scope of the incidents are wide.

The handling of an incident within Telia is guided by written plans of action, such as a modified version of the document *Computer Security Incident Handling Procedure 1996 NSWC Dahlgren* (Naval Surface Warfare Center, Dahlgren), and the Carnegie Mellons CERT CC instructions. There are also special plans for specific sub-networks.

Telia CERT CC is working in three steps to achieve a high level of technical security within their systems. The first step is to configure systems according to specified checklists. The second step is to verify the security level in the systems. The third and final step is to perform penetration tests. In addition to this there are controls of organisational/administrative and physical security.

3.7 International Support

This chapter contains information on protective mechanisms that are established on the international level. The focus of the presentation is on legal and organisational aspects. Mechanisms that primarily are of a technical nature are not included in this report.

3.7.1 Supporting Organisations for Law Enforcement

The international participation of the Swedish police is mainly done through the UN, Interpol, Europol (which acts within the framework for the transnational work within the EU, Schengen) and the Baltic Sea cooperation, as well as in the Nordic police and customs coordination (PTN). In addition, the Swedish police have bilateral contacts with several countries, e.g. Estonia, Latvia, Lithuania, Russia, Poland, Ukraine and Hungary.

The overall responsibility for Sweden's international police cooperation lies on the National Criminal Investigation Department, where coordination and communication are conducted at the National Liaison Office.

Interpol

The International Criminal Police Organisation, Interpol, has long been an important cooperation organisation for the Swedish police. Interpol's global police work began in 1923 and now includes 178 countries. A code that means that the member countries cooperate within the criminal police area and mainly crime that falls under general criminal law regulate

Interpol's activities. The police in Sweden have access to database registers containing information on crimes and criminals throughout the world. A Swedish police officer works at Interpol's headquarters in Lyon, France. The police work through Interpol permits access to cooperation partners in countries inside and outside the European Union (EU).

Europol

The Europol Convention came into force on 1 October 1998, and in connection with this the European Police Office, Europol, was established. The objectives are to fight and prevent drug crime, terrorism; illegal trading in nuclear and radioactive substances, illegal immigration networks, trafficking, trading in stolen vehicles, and money laundering that is connected with these types of crime, or crimes that are associated with these crimes.

Europol's main task is to function as a centre for exchange of information between member states in the EU on issues concerning drug crime in particular. Europol is therefore building its own criminal intelligence database and special analysis files. The handling of personal data is closely regulated in the convention and in special rules. There are joint and national bodies for data security.

Europol works in such a way that the member states provide information from their national databases. This information is compiled and processed, and when necessary, supplemented with information from other sources. The information is then analysed at Europol, after which the intelligence is returned to the police authorities in the member states to be used there.

Europol can be called upon when the actual circumstance shows an existence of a criminal organisation or structure that involves two or more member states. Depending on the crime's seriousness and consequences, joint action might be necessary.

Within each country there shall be a national single point of contact between Europol and the Member State. In Sweden this responsibility lies with the National Criminal Investigation Department (National Liaison Office). Sweden has two liaison officers stationed at Europol's headquarters in The Hague – one from the police and one from the Swedish customs authorities.

Liaison officers

One form of international cooperation that has proved very effective in combating crime is the stationing of liaison officers in countries with which there is a particularly large need for cooperation. This creates a platform for personal and direct contacts with the police forces in other countries, which experience shows, are very important for the success of the cooperation.

For many years there has been well-developed cooperation between police and customs, particularly with regard to combating drug trafficking, the so-called PTN cooperation. Within the framework of PTN the Nordic countries currently have a total of 34 police and customs officers stationed as liaison officers in 18 countries. Swedish police officers are today stationed in Athens, Bangkok, Budapest, The Hague, Moscow, St. Petersburg, Tallinn and Warsaw. In addition to this, Sweden has seconded staff at Interpol's headquarters in Lyon and at Europol in The Hague. The PTN cooperation changed a few years ago so that the liaison officers no longer act solely as drug liaison officers do but also as generalists, combating serious, cross-border international crime.

3.7.2 Supporting organisations for Telecommunication Providers

FIRST

To address the ever-increasing problem of security-related incidents that affect thousands of computer systems and networks throughout the world, a growing number of government and private sector organisations around the globe have established a coalition to exchange information and co-ordinate response activities.

This coalition, the Forum of Incident Response and Security Teams (FIRST), brings together a variety of computer security incident response teams from government, commercial, and academic organisations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has nearly 80 members. The only full member of FIRST in Sweden is the Telia-CERT CC.

FIINA

The *Forum for International Irregular Network Access* (FIINA) is comprised of 76 telecom administrations, representing 53 countries worldwide. It is an international organisation responsible for the dissemination of information required for the prevention of international illicit network access and fraud.

FIINA's primary task is to provide a forum for the exchange of ideas and information, sharing concerns of the telecommunication administrations on fraudulent use of telecommunication. Seminars are held for the development and understanding of international network fraud and abuse, to discuss necessary measures to combat fraud and network abuse by means of detection and to investigate the use of preventative technical features.

TF-CSIRT

Under the auspices of the TERENA[32] Technical Programme a task force has been established to promote the collaboration between *Computer Security Incident Response Teams (CSIRTs)* in Europe. The aims of the task force (TF-CSIRT) are:

- To provide a forum for exchanging experiences and knowledge;
- To establish pilot services for the European CSIRTs community;
- To promote common standards and procedures for responding to security incidents;
- To assist the establishment of new CSIRTs and the training of CSIRTs staff;
- To co-ordinate other joint initiatives.

The TF-CSIRT focuses its activities on Europe and neighbouring countries and on (potential) CSIRTs operated by (national and international) research and education networks, commercial Internet Service Providers (ISPs), major companies and governmental institutions as well as vendor-product teams and major commercial CSIRTs. The task force collaborates with other teams and with organisations outside the geographical area whenever such collaboration will assist in achieving the aims of TF-CSIRT.

[32] TERENA - Trans-European Research and Education Networking Association - was formed in October 1994. TERENA carries out technical activities and provides a platform for discussion to encourage the development of a high-quality computer network infrastructure for the European research community.

3.8 Notes on Swedish CIIP Research and Development

CIIP-related research and development (R&D) in Sweden is mainly conducted in the area of academic research, corporate research, and research at different defence institutions. The Commission on Vulnerability and Security concluded that there is a need for more R&D to improve the capacity for managing major crises. The efforts in R&D have to be made in an inter-disciplinary manner. The Commission made several proposals as how to best promote R&D:

- A broad cross-section of research groups should be encouraged,
- Public bodies should be encouraged to commission and purchase R&D,
- Purchasers and providers should be linked in subject- or problem-oriented networks that include public authorities and research groups.

SEMA has a leading role in coordinating Swedish CIIP research and development and has developed a number of R&D programs in that area. SEMA is also the contributing partner to the Swiss-Swedish CRN initiative[33].

The Swedish Defence Research Agency[34] (FOI) is an assignment-based authority under the Ministry of Defence. The R&D efforts within FOI spans a wide range of academic disciplines, from the entire field of applied natural sciences such as physics and chemistry, to political science, such as national security policy analysis. The Critical Infrastructure Studies Unit (CISU) at the division of Defence Analysis is a research group primarily focused on infrastructure related research. Currently the unit is working on a long-term research program on CIP sponsored by SEMA. Within this research program CIIP-issues has been one of the focal points. The department of Systems Analysis and IT-security at FOI are working with both civilian and military related research on IT-systems, primarily on a technical level. This department has acquired deep knowledge on commercial and military IT-systems and applications.

The National Centre for Information Operation/Critical Infrastructure Protection Studies (CIOS) is located at the Swedish National Defence College (SNDC). The task of the SNDC[35] is to contribute to national and international security through research and education. CIOS conducts research and policy development in the fields of information operations and critical infrastructure protection (IO, CIP). The Ministry of Defence and SEMA finances the research at CIOS. CIOS is also responsible for the basic and advanced courses at SNDC's advanced Officers Program concerning IO/CIP. These courses are funded by the Swedish Armed Forces.

SEMA is also sponsoring research at the Computer Security Research Group[36] at the Chalmers University of Technology in Gothenburg. The overall research goal of the group is to model security within the dependability framework, and in particular to find quantitative measures of IT-security that could be used for predictive purposes. One research area is the design and evaluation of reliable intrusion detection systems.

[33] http://www.isn.ethz.ch/crn/

[34] http://www.foi.se/

[35] http://www.fhs.se/

[36] http://www.ce.chalmers.se/research/Security/

Other important actors involved in CIP/CIIP research and development are The National Centre for IO/CIP studies, the Linköping Institute of Technology, The Royal Institute of Technology (KTH), Stockholm University, Karlstad University, and the Swedish Institute of Computer Science (SICS).

4 Procedures for Tracing Network-Mediated Attacks

In this chapter a description is given on the procedures involved in handling network-mediated incidents in Sweden. Depending on which network resources that has been utilised and from where the attack emanates the procedures of handling an incident varies. To illustrate these procedures the presentation is based on three different scenarios. These scenarios are schematically outlined in figure 1 below.

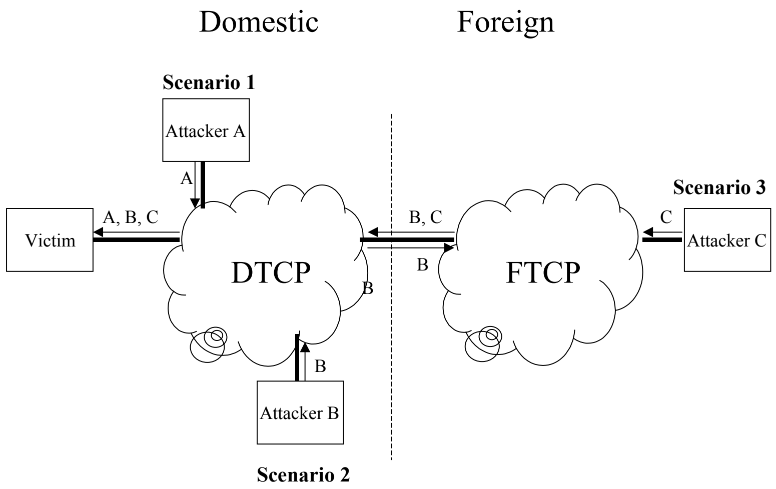


Figure 1. Scenarios used in this report

The basis for all three scenarios is that the victim is located in Sweden, and is connected to the Internet through Domestic Telecommunication Providers (DTCP), which for convenience also include operators that only provides Internet services, so called Internet Service Providers (ISPs). Foreign Telecommunication providers (FTCP) relay a connection to parts of the Internet that is located outside Sweden. The three scenarios are as follows:

1. In the first scenario (scenario 1) the attacker A is only using network resources in Sweden.
2. In the second scenario (scenario 2) the attacker B uses network resources in both Sweden and other countries. In this scenario the attacker B is also located in Sweden.
3. In the third scenario (scenario 3) the attacker C is located outside Sweden and uses network resources in Sweden and in other countries.

In the following sections 4.1 through 4.3 descriptions are given of the procedures that are involved in tracing and identifying an attacker in the different scenarios. In the scenarios the following categories of actors are at some stage involved in handling an incident:

- Supporting Organisations for Telecommunication Providers (SoTCP),
- Foreign Telecommunication Providers (FTCP),
- Domestic Telecommunication Providers (DTCP),
- Domestic Law Enforcement (DLE),
- Supporting Organisations for Law Enforcement (SoLE),
- Foreign Law Enforcement (FLE).

In the presentation the focus will be on the interactions *between* these actors. Detailed information on the units or departments that are involved within specific organisations in handling incidents and capacities they have at their disposal is given in chapter 3, *CIIP Organisations and Protective Mechanisms.*

In addition to the general categories of actors the procedures are, from the victim's point of view, divided into the following four stages:

1. Detection of an incident,
2. Assessment 1 and First-aid,
3. Assessment 2
4. Information handling and Law Enforcement support.

This division is a crude reflection of reality and does not necessarily reflect how actual incidents are handled. The activities described in the different scenarios should be considered as typical procedures. The purpose of the descriptions is to illustrate the main characteristics of the procedures involved in handling an incident, not to give detailed accounts of specific events.

The first scenario, where the attacker only uses network resources within Sweden, forms the basis for the other two scenarios. The victim's contacts with its telecommunication provider and with the domestic law enforcement are very similar in the early stages in the handling of an incident, regardless of what kind of scenario that is at hand.

4.1 Scenario 1: Attacker using network resources only in Sweden

In the first scenario the attacker is only using network resources in Sweden. The actors involved in scenario 1 are outlined in figure 2 below.

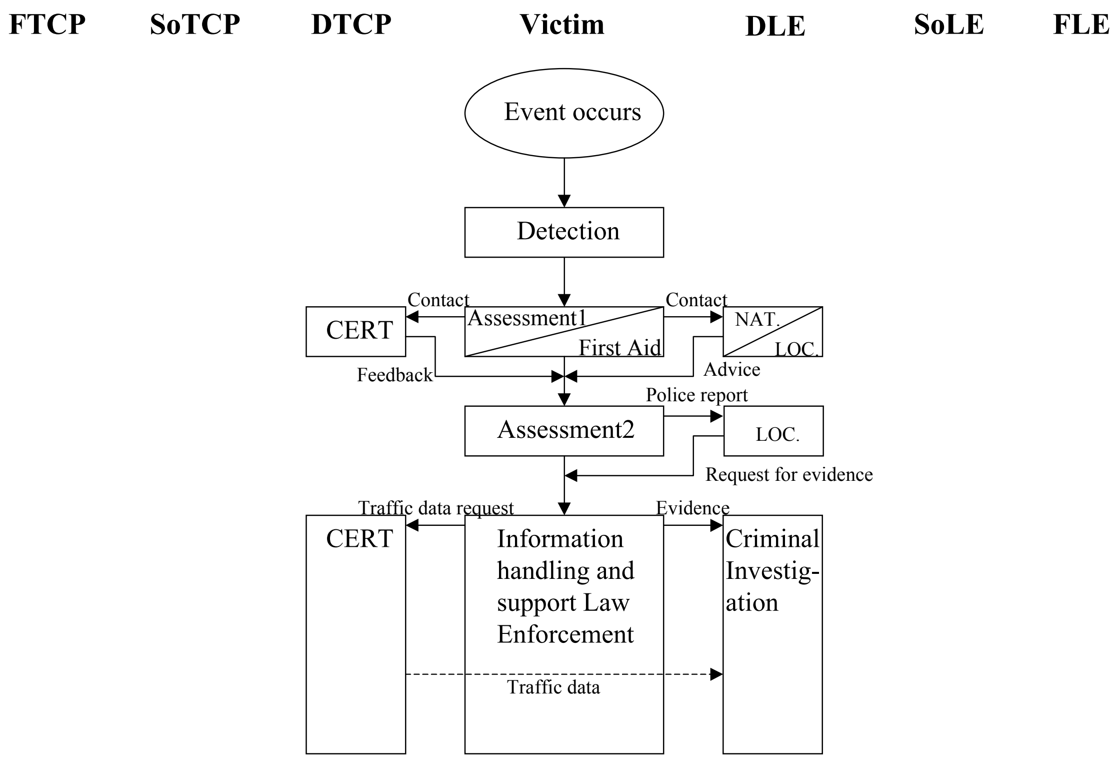


Figure 2: Incident handling procedures in scenario 1

The meaning of the boxes and the interactions in figure 2 will be outlined and explained in the following subsections.

4.1.1 Detection

In general three different parties can detect an incident, firstly by the victim himself, secondly by the domestic telecommunication provider (DTCP) to which the victim is connected, or thirdly by an external party that has identified that the victim’s problem originates from the DTCP´s network. An example of the latter would be a DTCP Network Management Centre that logs network activities detects irregularities that are interpreted as a denial-of-service attack. The origin of the attack is traced to a computer within their network. This situation would typically lead to that a caution message is sent to the owner of the specific computer. Another detection mechanism would be that a third party, for instance a university or other organisation, reports that someone from within the DTCP network is trying to do something malicious.

It is apparent from the examples above that if an incident is not too serious and it is easy to identify the perpetrator, it is often sufficient just to warn the perpetrator. If the incident were serious, the next step for the victim would be to do an initial assessment of the effects and if necessary initiate first aid operations in the affected systems.

4.1.2 Assessment 1 and First Aid

After the detection of an incident there would normally be an *initial assessment*[37] of the event, probably stipulated by the victimised organisation's security policy. The assessment establishes, among other things, the seriousness of the incident.

The extent and quality of this assessment depends on the qualifications of the victim and what resources that are available. A victim, who is highly qualified in the IT-security area, for instance a large or middle-sized telecommunication provider, would probably have access to a Computer Emergency Response Team (CERT) within the organisation. Such a team would take responsibility of the handling of the incident and manage contacts with law enforcement and other relevant actors.

The *first aid* would consist of an initial damage assessment, a consequence analysis and an assessment of possible measures to stop the incident and mitigate the damage.

An affected organisation, which does not have a CERT or similar function, would probably contact the police at this stage. The victimised organisation gets in contact with the police, either at the local or the national level, which is indicated by *Nat./Loc* under DLE (Domestic Law Enforcement) in figure 2.

For the IT crime squad at the Swedish National Police Board (NPB, see subsection 3.3.1) most incidents begins when someone, a private person or a representative of the victimised organisation, makes a telephone call to the squad. Usually it is a technician, systems administrator or the Chief Security Officer that calls. According to the working procedures of the Swedish police the correct way for the victim would be to contact the IT crime unit at a local police department.

The handling of the incident proceeds with a discussion between a police officer at the IT crime squad and the victim. In this discussion the police act as an adviser. The owner of the attacked system decides how to respond to the incident. In the contact between the victim and the police one obvious subject that is discussed is the possibility to log the perpetrator's activities.

Notably, telecommunication providers and Internet service providers (ISP) does not always report attacks. This usually depends on how likely it is that the perpetrator actually can be identified, prosecuted and convicted. If they decide to report attacks they always proceed to file a formal police report.

According to the NPB IT crime squad, most of the Swedish ISP's has been reluctant to participate in IT crime investigations. In most cases the victim decides to shut down their systems and patch the vulnerabilities without further legal actions.

The IT crime squad may *advise* the victim to contact the next node in the incident chain, often the DTCP that is responsible for the server from where the attack seems to emanate. Another advice could be that the victim should contact the IT crime unit at a local police department.

One part of the first assessment would be that the victim contacts the DTCP, see the first CERT-box in figure 2. Note, that it is not always the case that the DTCP have an actual CERT, but for convenience the term is used because it is probable that the inquiry ends up at

[37] As an example of local incident handling, the following can be noted. The Swedish telecommunication service provider Telia and the Bank of Sweden, have decided to establish virtual Security Incident Response Teams in their organisations according to the method presented in a master thesis by Jimmy Arvidsson; *Incident organisation and incident handling*, 2000 (in Swedish). The book Computer Security Handling inspires some parts of this thesis – *Step by step*, SANS Institute (System Administration, Networking, and Security), NSWC, 1998.

a CERT unit or similar function. The task for the CERT-function will be to help the victim as far as possible in tracing the perpetrator. According to Swedish law the telecommunication subscriber/customer is always entitled to obtain information about his or her own telecommunication messages, see also section 2.4.

Some DTCP's assist their customers as far as possible in the tracing illicit activities, e.g. with contacting other DTCP's. Large DTCP's do this, regardless from where the attack emanates, as part of their ambition to keep the Internet and other information systems free from malicious activities.

Some DTCP's have fraud units, which handles problems that customers are affected by, such as abuse, intrusions and fraud. These units help customers to trace perpetrators. The tracing of perpetrators is usually done in collaboration with other DTCP's, often without formal agreements. If the attack does not originate from the DTCP's network, they may provide the victim with relevant incident information, e.g. traffic data. The victim is then responsible to pursue the incident investigation, either by contacting the next DTCP in the incident chain or by contacting the police.

In the tracing procedure it is likely that non-DTCP organisations will be nodes in the incident chain, for instance a Swedish University could have been exploited as a node in an attack. This is usually handled through informal contacts with these organisations.

The range of activities in the first CERT box, in figure 2 above, therefore depends of what kind of primary DTCP the victim is connected to. In a worst-case scenario, the victim receives information from each DTCP separately and the victim has to be the link between the different DTCPs. In a best case scenario the tracing of a perpetrator is done by a single DTCP.

The *feedback* that the victim receives from the DTCP/CERT and from the police is an input to the second incident assessment.

In the handling of an incident most communications are done by email, some contacts are taken by telephone. One experience from incident handling and tracing activities is that it usually is difficult to get in touch with the right people within the different organisations.

The experience of some Swedish DTCP's is that it is much easier to get in touch with the right people in an organisation if contacts have previously been established. The concept of *web of trust* is important in the contacts between the nodes in an incident chain.

4.1.3 Assessment 2

After the initial assessment and contacts with the DTCP and law enforcement the victim usually performs a *second assessment*. In this assessment the *feedback* information from the DTCP and the *advice* from the police are evaluated. The objective of this is to decide on what further actions should be taken and, in particular, if any legal actions are necessary.

The second assessment could lead to that the victim files a report to the police (this is indicated as *police report* in figure 2). This is done at the local police department. If there is an IT crime unit at the department, this unit will handle the report.

The local IT crime unit has to establish if a crime has been committed and what type of offence that is at hand. To be able to establish this, the police will have to make requests for evidence from the victim, e.g. technical information from log files etc. This activity will continue during the criminal investigation. If there is no local IT crime police unit the IT crime squad at the NPB will pursue the investigation.

4.1.4 Information handling and Law Enforcement support

The victim has to provide *evidence* to the law enforcement that gives a good description of how the systems have been affected. It is only the victim that has the legal right to access traffic data from his DTCP's. The victim has to provide this information to the police. The actual procedure for this can either be that the victim receives the information from the DTCP and then hands it over to the police or that the police are authorised by the victim to receive the information directly from the DTCP.

The DTCP have the right to hold technical information about incidents for only a finite time. To be able to use the information at later stages, the CERT has to save the information. The Swedish law regulates this in the Swedish Telecommunication Act, see section 2.4. Though, it is not strictly regulated to what extent the DTCP is allowed to save traffic data or when it is proper to use this information. It is possible to extend this law if the DTCP considers it necessary to save the information for future business related activities.

Some DTCP has a handful of employees working fulltime to support the police with incident related information. Some companies have also configured their incident handling system to match the information needs of the National Criminal Investigation Department.

Before the police can take any further actions in relation to an incident there must be a well-founded suspicion of a crime that could lead to a minimum of two years of imprisonment.

If the suspected perpetrator lives in Sweden and in the same police district as the victim the local police department will be in charge of the investigation. In this situation the national IT crime squad only acts as an adviser. If the suspected perpetrator and the victim are living in different police districts, then the national IT crime squad co-ordinates and guides the local police departments in their investigations.

If the prosecutor finds it suitable, a search of premises and an interrogation is executed. This could take place as soon as the suspected perpetrator is identified. The prosecutor brings in an indictment against the suspect. The prosecution usually takes some time, some times due to time-consuming forensic work on confiscated computer hardware and other physical evidence.

It is difficult to estimate how long each stage will take in the procedure outlined above. The technical aspects of tracing an attack can be quite rapid, ranging from just a few minutes to hours and days. The criminal investigation of an attack is always more time consuming and can take several days and sometimes months. When there is an international component in the attack, as in scenario 2 and 3, the investigations often take months to complete.

4.2 Scenario 2: Domestic attacker using network resources outside of Sweden

In the second scenario the perpetrator uses network resources in both Sweden and foreign countries. The perpetrator is located in Sweden. The actors involved in scenario 2 are outlined in figure 3 below.

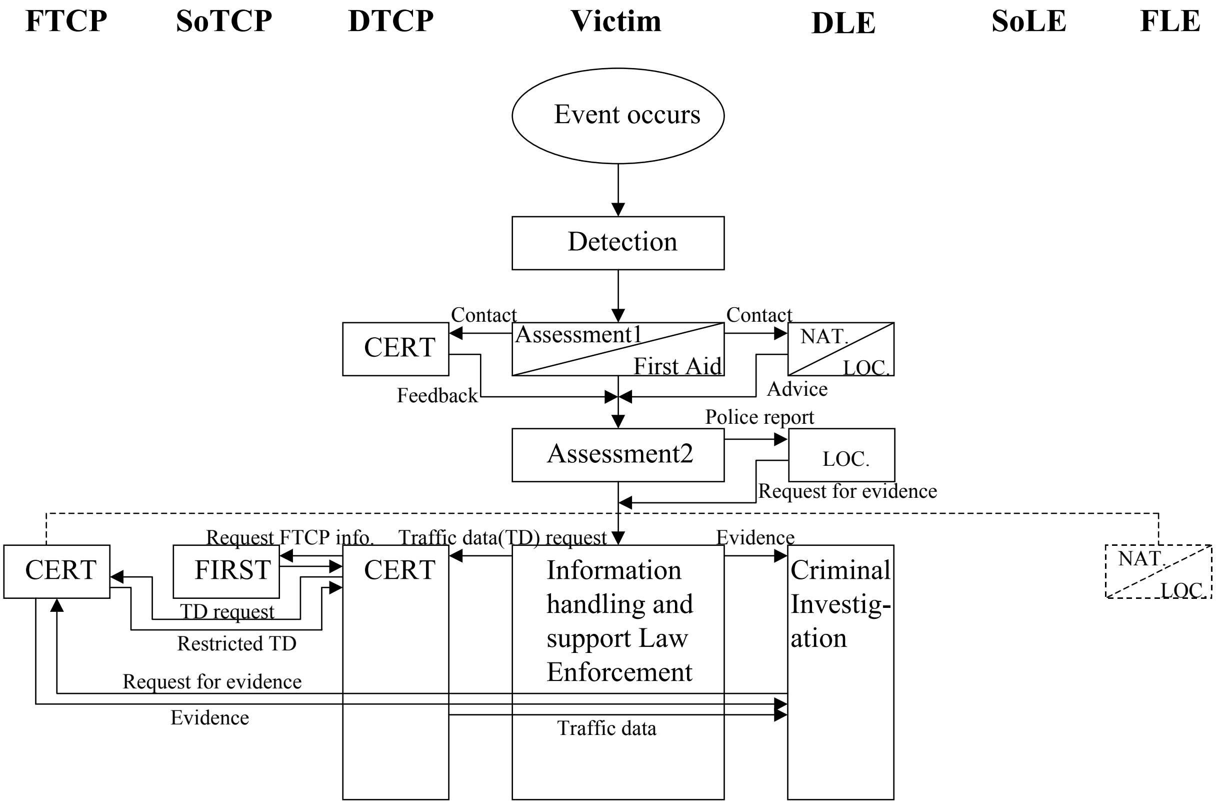


Figure 3: Incident handling procedures in scenario 2

The meaning of the boxes and the interactions in figure 3 will be outlined and explained in the following subsections.

4.2.1 Detection

The *detection* of the incident in scenario 2 follows the description made in subsection 4.1.1.

4.2.2 Assessment 1 and First Aid

The *initial assessment* and *first aid* of the incident at the victimised organisation closely follows the description made in subsection 4.1.2. The *contact* with the police in the initial assessment and the *advice* obtained from the police at this stage is independent of the fact that some of the nodes in the attack are located in foreign countries.

The next step is that the victim contacts the DTCP to which the victim is connected. This is indicated in figure 3 with the term *CERT* (the first box). Aspects of the procedures at the CERT closely follow the procedures outlined in section 4.1.2. The task for the CERT will be to help the victim as far as possible in tracing the perpetrator. At this stage it is possible that the DTCP take informal contacts with foreign telecommunication providers (FTCP), which is described in the fourth stage of the incident handling, see section 4.2.4.

The *feedback* the victim receives from the DTCP/CERT and from the police is an input to the second assessment.

4.2.3 Assessment 2

In the *second assessment* of the incident the victim is trying to verify conclusions made in the first assessment. With the additional information from DTCP and the police the victim establishes what legal actions should be taken. This second assessment of the incident follows the description made in section 4.1.3.

4.2.4 Information handling and Law Enforcement support

The interaction between the victim and the Swedish police follows the description made in section 4.1.4.

According to Swedish law there are no restrictions for DTCP's to contact any other domestic or Foreign Tele Communication Provider (FTCP) to request information in order to trace and identify a perpetrator. The result of the request depends on the policies of the contacted organisation and on the laws that are applicable to the request. It is a Swedish experience that it is often difficult to get in touch with the right person that could be of assistance in handling a tracing request. If the contact points already are established it is usually much easier to get in touch with the relevant people in an organisation. For example, some Swedish telecommunication providers CERT's have had very good experience working with the British Telecom CERT CC.

If there is no established contact with a FTCP, the DTCP can often turn to a *Supporting organisation for Tele Communication Provider* (SoTCP) to obtain relevant contact information. Examples of SoTCPs are the *Forum for Incident and Resonse Teams* (FIRST), *Forum of International Irregular Network Access* (FIINA) and *Task Force – Computer Security and Incident Response Teams* (TF-CSIRT), see section 3.7.2 for additional information on these organisations.

In figure 3, FIRST has been used as an example of a SoTCP. FIRST consists of 80 incident response and security teams from 19 different countries, and provides a closed forum for these teams to share experiences and information related to incidents, and to promote preventive measures. Additionally, FIRST as it exists today is a voluntary organisation with no operational element. As such, it provides an introduction service and meeting place for teams to establish trusted interactions.

With the exception of specific information on telecommunication subscribers the DTCP usually obtain the requested traffic data in an informal way from the contacted FTCP/CERTs.

If the information regarding a specific telecommunication subscriber would be of vital importance to the tracing of an incident, the next step for the DTCP would be to file a police report in the respective country. In scenario 2 the perpetrator is not located in a foreign country, so the last piece of information is not essential to the investigation. Though, it should be noted that it might be quite difficult to arrive at this conclusion just from the obtained traffic data.

According to some DTCP's, obtaining *evidence* from a FTCP always involves *Foreign Law Enforcement* (FLE), even if the perpetrator is located in Sweden and only uses network resources in a foreign country to attack targets in Sweden. The general impression is that the FTCP handles the contacts with FLE without involvement of *Supporting organisations for Law Enforcement* (SoLE) because it does not concern citizens of the foreign country.

The victim has to provide the DLE with *evidence* from affected systems. The primary DTCP has to supply evidence (e.g. traffic data) to the DLE from other DTCP and FTCP and organisations that has been used as nodes in the incident chain.

4.3 Scenario 3: Foreign attack on Swedish target

In the third scenario the perpetrator uses network resources in both Sweden and foreign countries. The perpetrator is located in a foreign country. The actors involved in scenario 3 are outlined in figure 4 below.

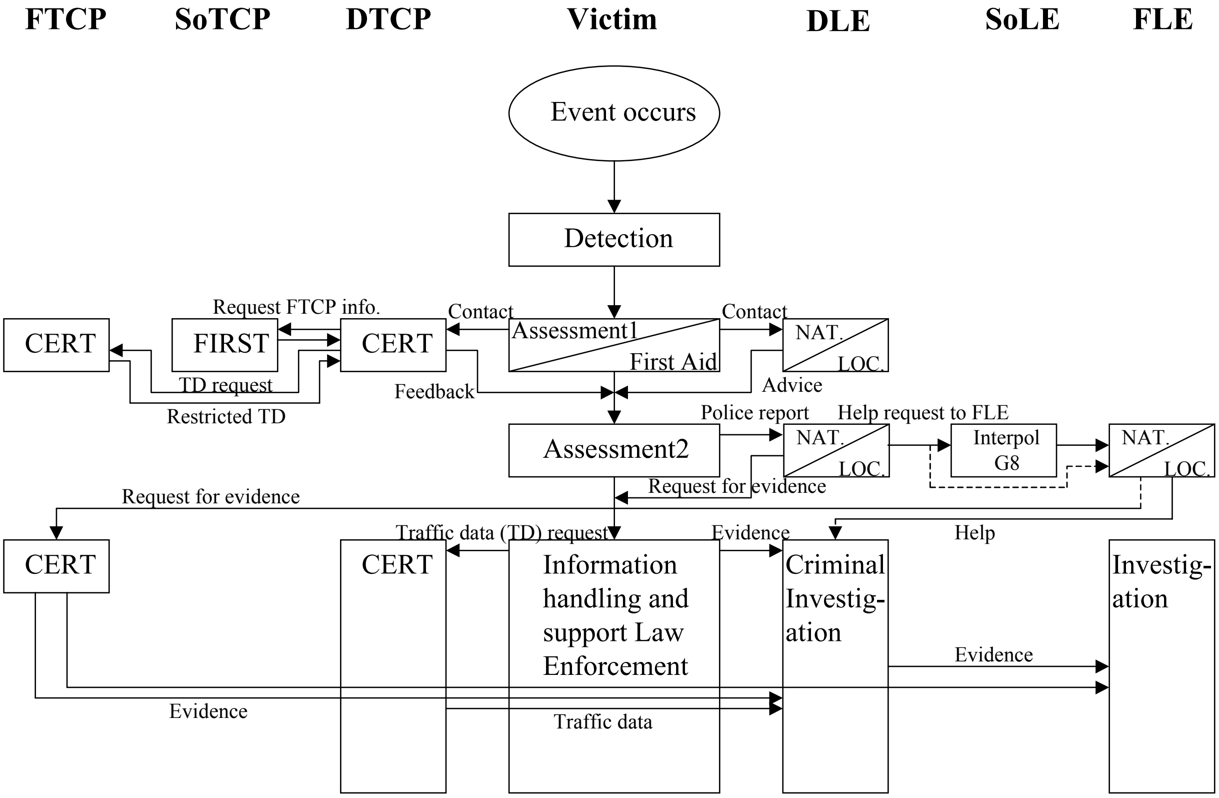


Figure 4: Incident handling procedures in scenario 3

The meaning of the boxes and the interactions in figure 4 will be outlined and explained in the following subsections.

4.3.1 Detection

The detection of the incident in scenario 3 follows the description made in section 4.1.1.

4.3.2 Assessment 1 and First Aid

To make this description transparent, we assume that the *feedback* from DTCP makes it clear that the perpetrator is located in a foreign country. With this assumption follows that the second assessment will contain a police report that will be sent to the foreign country through supporting organisations for Law Enforcement (SoLE).

The result of this assumption is that the initial assessment of the incident in scenario 3 follows the descriptions made in sections 4.2.2 and 4.2.4.

4.3.3 Assessment 2

The second assessment of the incident follows the description made in section 4.1.3 to the point where a foreign police force is contacted. Then the procedures are as follow.

When the Swedish police or prosecution authorities wish to *request* assistance in a foreign country they have in principle two possible options. One is a letter of request (letter rogatory) which is normally sent by the Swedish prosecutor through official channels to the country in question, i.e. via the Ministry of Justice or, in the EU Member States directly to the opposite competent prosecution authority. Such a letter may include a request for coercive measures such as search of premises, etc.

The second alternative is the ICPO-Interpol. Such requests are channelled through the Swedish police or prosecution authority via the International Liaison Office/Interpol Stockholm to the relevant foreign authority for execution of the requested action. Uncomplicated requests for record information etc. are usually processed directly at the respective Interpol offices. These types of inquiries are mostly dealt with on a bilateral basis without engaging the Interpol General Secretariat. The laws and regulations of the recipient country determine what measures should be taken as each State is sovereign in this regard. If Interpol Stockholm sends a request for assistance relating to a crime, which is not punishable in the requested country, that country will not take action.

4.3.4 Information handling and Law enforcement support

The main rule in these cases is to investigate, prosecute and pass judgement in the country where the criminal act was committed. If located in another country, the suspected perpetrator may then be extradited to the country where the crime was committed. As Sweden does not normally extradite its own citizens, the alternative is to transfer prosecution and sentence to Sweden. For those countries that normally do not extradite its own citizens, the evidence obtained in Sweden will be transferred to the country where the prosecution will take place.

Appendix 1 Swedish law relevant to IT-related crime

The Swedish layer Thomas Carlén-Welders has attempted to classify computer related crimes, where computers are used as tools, into five general categories and then identify which parts of the Swedish law that is applicable[38]. The relevant parts of the Swedish law are the Swedish Penal Code (SPC), the Swedish Data Protection Act (SDPA, abolished through the Personal Data Act) and the Law of Protection of Business Secrets (LPBS). The classification is given below.

Crime category	**Relevant part of the Swedish law**
Crimes Against Public Order	
Inciting rebellion	SPC 16:5
Racial agitation	SPC 16:8
Child pornography	SPC 16:10a
Unlawful depiction of violence	SPC 16:10b
Defamation	
Defamation	SPC 5:1
Insulting behaviour	SPC 5:3
Unlawful threat	SPC 4:5
Molestation	SPC 4:7
Theft of identity	SPC 9:1
E-mail bombing	SPC 4:7
Spamming[39]	SPC 4:7
Swamping	SPC 4:7
Economic Crimes	
Extortion	SPC 9:4
Fraud	SPC 9:1
Swindling	SPC 9:9
Crimes of Information	
Computer intrusion (breach of data secrecy)	SPC 4:9c (SDPA 21 §)
Computer sabotage	SPC 4:9c (SDPA 21 §), SPC 12:1-3
Computer fraud	SPC 4:9c (SDPA 21 §), SPC 9:1, SPC9:9
Computer espionage	SPC 4:9c (SDPA 21 §), LPBS 3 §
Computer manipulation	SPC 4:9c (SDPA 21 §)
Business espionage	LPBS 3 §
Computer time theft	SPC 4:9c (SDPA 21 §)
Attempt/preparation of crime	SPC 9:11, SPC 23
Crimes Against the Security of the Realm	
Unauthorised possession of secret information	SPC 19:5, SPC 19:7
Careless handling of secret information	SPC 19:9

Swedish law relevant to IT-related crimes

[38] Nätjuridik. Lag och rätt på Internet (*Network law. Law and order on the Internet*), Carlén-Wendels, Thomas, Norstedts Juridik AB, 1998.

[39] This concerns crime against a person. If the crime is directed against an organisation, the crime is classified as damage or sabotage.

Appendix 2 The Swedish telecommunications act (1993:597)

The following text is quoted from the translation of the Swedish Telecommunication Act (as stated in July 1999) obtained from the Swedish National Post and Telecom Agency.

Mandatory notification
Section 5
Within a public telecommunications network, the following services may only be provided following notification to the authority appointed by the Government (the supervisory authority)

1. Telephony services to a fixed termination point,
2. Mobile telecommunications services,
3. Other telecommunications services requiring allocation of capacity from the numbering plan for telephony determined by the supervisory authority, and
4. Network capacity.

The Government or, if authorised by the Government, the supervisory authority may issue regulations concerning exemptions from mandatory notification.

Mandatory licence, etc.
Section 7
In addition to what follows from Section 5, a licence under this Act is required in order to be entitled to provide within a public telecommunications network:

- Telephony service to a fixed termination point,
- Mobile telecommunications service or
- Network capacity,

If the activity is of an extent which is considerable with regard to area covered, the number of users or other comparable circumstances. A licence may relate to a specific area or to the whole of Sweden.

Secret telecommunications interception, etc.
(The Code of Judicial Procedure contains rules restricting such surveillance)
Section 17
A party granted a licence under Section 7 shall pursue the telecommunications activities so that decisions concerning secret telecommunications interception and secret telecommunications monitoring may be executed and without the execution is revealed. The content of and information about the telecommunications messages subject to interception or monitoring shall be made available so that information may be easily dealt with.

The obligation of confidentiality, etc.
Section 44
A telecommunications message may be monitored in telecommunications activity only to the extent that this is necessary in order to carry on the activity.

Section 45
A party who in telecommunications activities has become cognisant of or obtained access to:

1. Information on a telecommunications subscription,

2. The contents of a telecommunications message, or
3. Other information relating to any specific telecommunications message

Must not without authorisation forward or utilise what he/she has become cognisant of or obtained access to.
The obligation of confidentiality, as defined in the first paragraph, does not apply in relation to a party who has participated in the exchange of a telecommunications message or who has in some other way dispatched or received such a message. The obligation of confidentiality with regard to information as referred to in the first paragraph items 1 and 3 does not apply in relation to a holder of a subscription used to convey a telecommunications message.

Section 46
The obligation of confidentiality as referred to in Section 45; first paragraph applies also to information relating to:

1. Measures to retain dispatches as referred to in Chapter 27, Section 9 of the Code of Judicial Procedure,
2. Any matter relating to the use of secret telecommunications interception or secret telecommunications monitoring according to Chapter 27, Section 18 or 19 of the Code of Judicial Procedure.

Section 47
A party pursuing telecommunications activities and who has in so doing become cognisant of or obtained access to information as referred to in Section 45, first paragraph, shall upon request render:

1. Information as referred to in Section 45, first paragraph, item 1, to a public authority which in an individual case is in need of such information for service pursuant to the Service of Documents Act (1970:428) if the said authority considers that it may be assumed that the party sought in order to be served is keeping himself/herself unavailable or that there are otherwise extraordinary reasons,
2. Information as referred to in Section 45, first paragraph, item 1, which concerns suspicion of a crime, to the public prosecution authority, police authority or any other public authority whose task it is to intervene against such an offence, if the penalty prescribed for the offence is imprisonment and if it may, in the view of the authority, entail a sanction other than fines,
3. Information as referred to in Section 45, first paragraph, item 3, which concerns suspicion of crime, to the public prosecution authority, police authority or any other public authority whose task it is to intervene against such offence, unless a less severe sanction than two years imprisonment is prescribed for the offence,
4. Information as referred to in Section 45, first paragraph, item 1, to an enforcement service in need of the information in enforcement operations, if the authority considers that the information is of considerable importance for dealing with a matter,
5. Information as referred to in Section 45, first paragraph, item 1, to a tax authority in need of the information for operations relating to the checking of tax or charges or in investigations concerning the correct population registration district under the Population Registration Act (1991:481), if the authority considers that the information is of considerable importance for dealing with the matter,
6. Information as referred to in Section 45, first paragraph, item 1, to a police authority, if the authority considers that the information is required in connection with providing

notification, tracing or identification in the event of accident or fatality or in order for the authority to perform information referred to in Section 12 of the Police Act (1984:387),

7. Information as referred to in Section 45, first paragraph, item 1, to a police authority or public prosecution authority, if the authority considers that the information is needed in a special case in order that the authority may fulfil obligations to provide information in accordance with Section 31, third paragraph of the Act with Special Provisions concerning Young Offenders (1964:167),
8. Information as referred to in Section 45, first paragraph, items 1 and 3, to the regional alarm centre referred to in the Operations at certain Regional Alarm Centres Act (1981:1104).

Section 48 (omitted in this text)

Section 49
A person who in telecommunication activities has become cognisant of information that relates to a particular telecommunications message shall destroy the information or prevent it from being identifiable at the end of the call or when the message has reached the recipient. However, information that is necessary for billing subscribers and for payment of interconnection charges may be processed until the debt is paid or time-barred. Such information may also be processed for the marketing of telecommunications services in their own activities if the subscriber has provided his or her consent to the processing. The provisions of the Personal Data Act (1998:204) on rectification shall also apply to processing of personal data under this Act.

Section 50
What is stated in Section 49, first paragraph, does not apply:

1. To telecommunications messages that have been conveyed or dispatched or ordered to or from a particular telecommunications address that is subject to a decision on secret telecommunication interception or secret telecommunication surveillance,
2. To the extent that it is necessary to prevent and expose unauthorised use of the telecommunications network, and
3. If the subscriber, in order to be able to identify disturbing telecommunications messages, requests that information about the telecommunications addresses from which telecommunications messages emanate shall be stored for a specified period. Information referred to in the first paragraph, item 3, and shall be made available to the subscriber upon request.

[Authors note: Rendering information about telecommunication messages, Internet connections, and telephone subscribers requires that the victim/subscribe contacts the telecommunication provider or the ISP and requests the information. The telecommunication provider/ISP then has to present the information to the victim, who in turn can provide the information to the police/law enforcement.]

Section 51
Information referred to in Section 49, first and second paragraphs, may only be processed in telecommunications activities by authorised persons. This processing shall be restricted to such information as is necessary for the activity.

Telecommunications activities in war, etc.

Section 65

If Sweden is at war or in danger of war or should such exceptional circumstances prevail which are entailed by war outside Sweden’s borders or by Sweden having been at war or in danger of war, the Government may issue the regulations on telecommunications activities necessary having regard to the defence of the country or its security in other respects.

The Government, or the public authority appointed by the Government, may issue regulations governing the peacetime planning for meeting the needs of the Total Defence system for telecommunications under such conditions as are specified in the first paragraph.