



Large scale Internet attacks

The Internet attacks on Estonia

Sweden's emergency preparedness for Internet attacks

SEMA's Educational Series 2008:2



SWEDISH EMERGENCY
MANAGEMENT AGENCY

Large scale Internet attacks

Title: Sweden's emergency preparedness for Internet attacks
Published by the Swedish Emergency Management Agency (SEMA)
Number of copies: 400 ex
Text: Omvärldsanalysgruppen på Informationssäkerhetsenheten, KBM
Cover photo: Keystone

ISBN: 978-91-85797-14-1
ISSN: 1652-3539
Design: Jupiter Reklam AB
Print: NRS Tryckeri, Huskvarna, 2008

The publication can also be downloaded from SEMA's website:
www.krisberedskapsmyndigheten.se

Table of Contents

Foreword	4
Part 1 – The Internet attacks on Estonia	7
Summary	8
Background and development of events	9
The Internet attacks	11
Scope of the attacks, traffic measurements	17
Official Estonian reactions	18
Russian activism as an influencing factor	19
Conclusions – the events in Estonia	20
Part 2 – Sweden's emergency preparedness for Internet attacks	21
Introduction	22
Possible threats and threat levels	23
The Internet in Sweden	27
Structure and dissemination	28
Public distribution of responsibility	31
Distribution of responsibility at departmental level	32
Distribution of responsibility amongst the Swedish authorities	33
The Police	33
Swedish Armed Forces	33
The Swedish Defence Materiel Administration and CSEC	34
Swedish National Defence Radio Establishment	34
Swedish National Post and Telecom Agency and Sitic	35
Swedish Emergency Management Agency	36
Collaboration	37
SAMFI	37
Other collaborative fora	38

Vulnerabilities of the Swedish branch of the Internet	39
Internet infrastructure	40
Authority networks and public websites	43
Other societally important information infrastructure	46
Swedish mass media	46
Digital control systems (SCADA)	47
Swedish incident management	49
Attack scenarios	50
National CERT operations in Sweden	51
Summary of national emergency management	53

Foreword

In spring 2007 Estonia was subjected to an Internet blockade lasting several weeks. During this time the net did not work normally. It became hard to reach authorities and the mass media via the Internet, for a brief period Internet banks had to interrupt their business, and for several extended periods it was hard to communicate with the rest of the world via the Internet.

How would Sweden cope with a similar situation? This is one of the questions we had in mind when we drew up this report, which is divided into two sections. The first part charts the events in Estonia, including the special circumstances that led to the country being subjected to extensive Internet attacks. In the second part we look at how Sweden is equipped for similar events, i.e. what it would do if the country were subjected to more or less organised attacks.

The review of the situation in Sweden has been based on an assumption of three levels of antagonistic threat. The first level, involving limited blockage and minor manipulation of the content of certain websites, does not normally constitute a serious threat to society and can usually be handled by the organisations and Internet operators affected. The other two levels, however, constitute threats the creation of which generally requires advanced knowledge and which aim, for example, to affect communications, distort official information or sabotage critical infrastructure such as electricity or water supplies. The experiences of Estonia also show that attacks will affect several players and sectors simultaneously.

The review reveals worrying current vulnerabilities in Swedish society regarding serious Level Two and Level Three threats.

Firstly, both the Swedish National Audit Office's reviews and SEMA's own investigations have revealed marked

shortcomings in the authorities' handling of their own information security. Amongst other things, important procedures are missing, authorities' websites can be hijacked – and insufficient attention has been drawn to problems at management level.

Secondly, the Swedish administrative tradition with its independent authorities means that it would probably be far harder in Sweden than in Estonia to maintain a picture of the current situation when Swedish networks are being attacked on a broad front. Above all there is no possibility of rapidly detecting many simultaneous attacks on Swedish authorities if they are not part of a major traffic flow that is visible at backbone network level.

Thirdly, there are only a limited number of people in Sweden with operational experience of handling extended large-scale Internet incidents. In the event of such an attack there may be a need for more experts than are currently available.

Fourthly, the increasing number of high-capacity household broadband connections may escalate the threat from a coordinated attack. A botnet of infected home computers with high-speed connections could become a powerful weapon against society's information systems. Authorities' computers might also be taken over and used in such attacks. This was shown in a recently published investigation of DNS use in Sweden.


Otherwise, backbone-network infrastructure in Sweden has a very high capacity, and the risk of total blockage of the Swedish branch of the Internet is relatively small.

The present document constitutes a partial report in the Swedish Emergency Management Agency's ongoing work of studying the field of cyber defence. The partial report constitutes data for the annual situation assessment regarding society's information security that the authority prepares on behalf of the government. It is thus not an investigation in the normal sense, but rather a charting of

the area and an attempt to analyse the possible consequences of experiences of the Estonian Internet attack regarding protection of Swedish societal functions. It does not aim to provide concrete proposals for measures, but restricts itself to focusing on crucial problem areas that should be the topic of a broader discussion. It is planned that the resultant proposals should form part of the plan of action for the field of information security which the Swedish Emergency Management Agency will be submitting to the government in March 2008.

The partial report has been drawn up by the Information Assurance Unit's Strategic Analysis Group. The work has been made much easier by the generous help received from the Estonian authorities and from people with special insight into the way handling of Internet incidents works.

Stockholm, 28.11.2007



Ingvar Hellquist

Part 1

**The Internet attacks
on Estonia**



Summary

From the end of April until the middle of May 2007 there was an extensive attack on the Estonian branch of the Internet. It seems the event was directly connected with disturbances in Estonia in conjunction with the moving of a Russian war memorial.

The attacks followed a pattern whereby simple access attacks were gradually followed by intelligence gathering and focused, well coordinated attacks involving major botnets.

Several Internet banks were blocked during the attacks, but it proved possible to protect the central networks and computer systems of the Estonian authorities. Neither were there any successful attacks on electricity networks or any other critical infrastructure in the country. The attacks mainly comprised access attacks of various kinds and hacking into websites – so-called defacements.

The attacks show that attacks on informational resources can be used to create attention, interrupt the business of authorities and commerce and act as a method of exerting pressure, e.g. combined with financial sanctions. They show that attackers now have the possibility of carrying out Internet attacks and simultaneously concealing their own actions.

The events in Estonia also show that the effects of similar Internet attacks can be limited by preventive measures and by unified action during the actual crisis. The preventive measures chiefly include preparedness to monitor patterns and deviations in Internet traffic, being prepared to quickly introduce protective measures in one's own networks, and efficient international collaboration in the field of incident management. During the actual attack the work was made easier by the quick convening of a team including representatives of different sectors of society. These experiences should also have consequences for Swedish emergency management.

Background and development of events

Estonia has a population of about 1.4 million. Of them, about 400,000 are Russian speakers, mainly of Russian-Estonian origin. Within this group of 'Russians' there are various groups which to varying degrees have been integrated into Estonian society. A large number of them speak Estonian and accept Estonia as a state, whilst others do not do so and are of the opinion that Russia is their state and that Estonia will again come under Russian control.

In 1947 Stalin's regime erected a bronze statue representing a Red Army soldier. For parts of the Russian minority in Estonia this statue symbolises the Soviet Union's victory over Nazi Germany. The statue has long stood in central Tallinn, and is now honoured every year on 9 May – the Russian day of commemoration of victory in WW2 and the country's great war against Nazism. For many Estonians, however, the statue is a reminder of Soviet occupation and a symbol of oppression. It is one of the few symbols of the Soviet era remaining in Estonia after the country's independence in 1991. The statue did not formerly have any major polarising effect. People who wanted to honour the memory of the soldiers who took part in the war against Germany came and placed flowers on the site – without any provocative intentions – and those who were reminded of the problems of the Soviet era were able to ignore the statue.

But the situation changed on 9 May 2006, when the police intervened to try and resolve a disturbance which had arisen between different groups carrying Soviet and Estonian flags respectively. This event created internal conflicts, and the Estonian government thus decided to move the statue plus a number of graves of Soviet soldiers. This was not, however, something that the politicians in the Estonian parliament were in agreement on, and the issue was debated. It was decided that the move should take place after 9 May 2007.

On Thursday 26 April the Estonian authorities erected a large tent on the site and surrounded it with fencing, in order to start excavation of soldiers' graves in the ground around the monument. This directly led to a demonstration, which initially went quietly. But when things suddenly got out of hand in the evening and extensive riots broke out, a quick decision was made during the night to 27 April to move the bronze statue to a secret location. The move took place early the very next morning.

The riots led to extensive devastation in central Tallinn, resulting in broken shop windows, plundered shops and fires. It was mostly drunken youths who took part. A large number of people are arrested, fifty or so were injured and a young man of Russian-Estonian origin also lost his life. After the first night of rioting the authorities made the decision to prohibit all sale of alcohol and decided that the prohibition should last until 2 May. The riots continued the next day, Friday 27 April, and during the following weekend. The first Internet attacks started late on Friday evening.

On Sunday 29 April Estonia's Minister of Defence Jaak Aaviksoo announced that the bronze statue would be officially re-inaugurated on 8 May. This indeed took place, and the statue and its stone wall are now to be found in a military cemetery in Tallinn.

The Internet attacks were not the only events occurring in conjunction with the disturbances on the streets of Tallinn. During the period from the end of April until the middle of May Estonia was also affected by a number of sanctions on the part of the Russians. Unannounced repairs to rail connections between Estonia and Russia were carried out, handling of papers at border crossings suddenly became abnormally extensive, transit traffic was severely restricted and major Russian product orders were cancelled.

The Internet attacks

The first wave of Internet attacks started on the evening of 27 April, less than 24 hours after the moving of the bronze statue and at a time of violent insurgency in central Tallinn.

This first wave of attacks consisted almost exclusively of simple access attacks and junk mail. The access attacks above all targeted web servers with a high public profile, the aim being to severely restrict access to them.

Those affected included several political parties, the president's and parliament's websites, the Estonian police, several central authorities and some Estonian legations abroad.

One of the results was that the Estonian government's public briefing room (www.valitsus.ee/brf) was temporarily blocked to access from abroad. Hackers also succeeded in breaking into the governing Reform Party's website, where they placed a false official apology for moving the bronze statue, signed by the Prime Minister Andrus Ansip. The picture of the Prime Minister was also given a Hitler moustache.



An example of a Russian-language website (zyklonteam.org) offering attack tools specially adapted for targeting attacks at Estonian websites.

In conjunction with the spread of the disturbances around Tallinn, detailed attack instructions had also rapidly spread on a number of Russian-language websites and discussion fora for hackers – often coupled with exhortations to run these command sequences in order to damage Estonia. Express commands were posted, and ready-made attack tools were provided that were specially adapted for attacking websites in Estonia.

The instructions which have been documented (and which in numerous instances can still be read on the Internet) typically exhort to so-called ping-flooding of named Estonian websites. This is a method whereby large amounts of abnormal test signals are sent to an Internet-connected computer with the aim of flooding it with data bits. Other similar methods also occurred during this first wave of attacks. One example is SYN-flooding. Several variants of this type of attack occurred.

```
последовательности команд есть, то есть сначала первый адрес проверить, потом следующий и т.д. , а можно несколько раз
выполнить команду ping и превратить все сразу:
```

```
ping -n 5000 -l 1000 www.rbc.ru -t
ping -n 5000 -l 1000 www.rferl.ru -t
ping -n 5000 -l 1000 www.haifa.ru -t
ping -n 5000 -l 1000 www.aab.ru -t
ping -n 5000 -l 1000 www.camp.ee -t
ping -n 5000 -l 1000 www.tandipark.ee -t
ping -n 5000 -l 1000 www.tbb.ee -t
ping -n 5000 -l 1000 pol.ee -t
ping -n 5000 -l 1000 www.polizei.ee -t
ping -n 5000 -l 1000 tavata.polizei.ee -t
```

После этого вы увидите доступен этот сайт или нет. Имена сайтов можно менять, достаточно не чаще 10 минут. Или создать файл с расширением bat. Что для этого нужно сделать? Откройте Блокнот (появил его в директории Windows) и например вставьте этот текст:

```
@echo off
SET PING_COUNT=50
SET PING_TIMEOUT=1000
```

In conjunction with the disturbances, attack instructions and exhortations to attack Estonian web servers began to spread to many Russian discussion fora for hackers. In the above example readers are exhorted to ping-flood a number of named Estonian websites.

During Friday evening and the night to Saturday 28 April the situation was fairly chaotic at the Estonian end. It did not take long to conclude that the greatly increased traffic towards the Estonian branches of the Internet was linked to the disturbances in the country and the moving of the bronze statue, but the motives for this were not entirely clear.

Subjecting of authorities and political websites to attacks was something that was to be expected. Some of the mass media were also attacked, including the daily newspaper Postimees. A direct motive was to be found here, by virtue of the fact that these media had reported directly from the insurgency in Tallinn – and in some instances had even exhorted people to send the police their digital and mobile photos in order to help identify the insurgents.

But in addition large traffic flows were simultaneously directed at the websites of small municipalities and schools in rural parts of Estonia. This initially created the impression that this wave of attacks was not particularly well coordinated, and was rather the result of a large number of attacks from many individual players who had been exhorted to take joint action. There were, however, indicators that use of large coordinated botnets had already begun.

Over the following days filtering and other protective measures were introduced at the Estonian end. Thus in a renewed wave of access attacks after the weekend it was possible to markedly reduce the effects.

At this juncture, however, people had started noticing several changes. Various types of intelligence gathering were detected in the Estonian networks, plus attempts to hack into and take over equipment in the actual network infrastructure. Bandwidth tests were carried out to measure capacity ceilings in the Estonian networks.

People now noticed that big botnets were beginning to be used, and the attacks were becoming increasingly sophisticated. Parliament was forced to close down its e-mail system for 12 hours, the Estonian mass media stopped answering foreign calls and on one occasion on 1 May several Internet operators in Estonia were forced to break all customer connections for 20 seconds in order to restart their equipment.

A mere 24 hours or so after the first wave of attacks the Estonian authorities had organised a team to create a collected picture of the situation and coordinate work. It met every day at the Ministry of Defence in Tallinn, and collaboration was made much easier by the fact that the ministries are within walking distance of each other. The practical work was led by the incident-management body CERT Eesti (CERT-EE) at the nearby Centre for Information Technology (RIA).

Initial information was sent out to foreign CERT organisations as early as on 28 April, after the first night of Internet attacks. Just before lunch on the Monday (30 April) more detailed information on the target systems in Estonia was then disseminated to CERT-EE's foreign collaborating partners, thus facilitating creation of signatures and filtering of traffic close to the sources of the attacks.

When the next major wave of attacks started a few days later, on 4 May, the state of emergency preparedness was thus relatively good. For nearly 24 hours very large traffic



Traffic statistics collected at a measuring point in Estonia. Here one can see the sudden flow of ping packets which late in the evening of Friday 27 April began to be sent to Estonian computers. The attack lasted nearly 24 hours. The diagram then shows how a renewed major wave of attacks hits the Internet on the night to Monday, but it is held in check relatively quickly, and in this instance people also stopped replying to ping calls so as not to place an unnecessary load on their own network.

flows were directed at the servers and networks of Estonian authorities. These attacks were far more organised than what had been seen previously, and were like a deluge of Internet traffic over the Estonian networks – or sustained and coordinated hammering of the networks using many different tools and weapons.

The degree of coordination of the attacks could be concluded by virtue of their involvement of big botnets which were in close succession directed at carefully selected targets using various tools of attack. Large, parallel attack flows were visible whose individual components/tools and launch ramps were exchanged at intervals of only a few seconds.

It was also clear that the attackers had regrouped their botnets. After the first wave of attacks incident-management organisations all over the world had been involved, and had helped put attacking computers out of action within their respective nearby operator networks. The number of botnet attacks now increased from jurisdictions without any incident-management organisation (CERT) or with a very weak incident management capacity.

But the attacks did not just come from abroad. Right from the very first wave of attacks a large number of attacking computers inside Estonia had been noticed. In parallel with the incident-management work, the Estonian police thus worked on trying to trace the perpetrators. According to information provided, several people were identified. After over a week a young man was arrested who had published instructions and attack targets on Estonian discussion fora and had exhorted others to help in the attacks. The man was shown on Estonian television – something which immediately had a deterrent effect on other Internet activists in Estonia. In the course of a single night the number of domestic attacks plunged to a very low level.

During the period 6–8 May hostile activity decreased somewhat. Then what was probably intended to be the

big main attack commenced. It happened late in the evening of 8 May Estonian time, or midnight to 9 May Moscow time, i.e. at the precise time when the Russian day to commemorate the WW2 victory began.

The main attack meant an extremely intensive blast of coordinated Internet attacks on Estonian servers. The approach was like that already seen a few days earlier, the difference being that the botnets now involved were far bigger. It is estimated that botnets with way over a million slave computers took part in the main attack. As always in such contexts, however, the estimate of the number of participating computers is relatively rough. It is based on traffic flows and is affected by the bandwidths the attacking computers have at their disposal.

Since special protective measures were undertaken during the main attack, its effect was reduced to a level far lower than was measured at the time of the first coordinated wave of attacks on 4 May.

Between 10 and 15 May two Estonian banks were also attacked: Hansapank and SEB Eesti Uhisbank. This happened through extensive access attacks which for a limited period of time completely stopped their Internet business and blocked their contact with foreign countries for a long time. On 15 May there were further focused attacks on the networks of Estonian authorities.

There have also been reports in the mass media of attacks on the Estonian telephone system, also stating that at least one public telephone exchange was put out of action. During the initial days in April there were extensive attacks on telephony – attempts to block Estonian authorities through phone calls. No successful technical attacks were reported, however. But there were attempts to attack mobile-phone networks in Estonia and systems used by the Estonian rescue service – which might have had major consequences.

Neither has any information come to light on attacks against SCADA (Supervisory Control and Data Acquisition) systems or other systems for control or monitoring of critical infrastructure in Estonia, e.g. the electricity network.

Scope of the attacks, traffic measurements

It has not yet been possible to completely clarify the total scope of the attacks. The results of traffic measurements are greatly dependent on the location of the measurement points, and the measurements carried out in Estonia are for natural reasons the truest ones. A number of such measurement graphs have been published, and we have had access to further information. The material does not, however, suffice to provide a full picture of the scope, but it is clear that the biggest attacks created traffic flows of around 1 Gbps (Gigabits per second) in the target networks.

People with a background in international operating business have stated that attacks of several Gigabits a second are not now uncommon. The same sources state that the attacks on Estonia did not contain anything technically new, but that the situation was exacerbated by the fact that the Internet connections in the country were unable to cope with really big sustained traffic flows.

The fact that there had historically been bigger attacks was not of that great a significance from the Estonian standpoint. For Estonia the attacks were massive, and constituted a huge burden on international connections and internal Internet resources. During the biggest waves of attacks traffic filtering and other measures were undertaken. But it was also necessary to seek outside help to cut off the flows as close as possible to the sources (the attacking computers).

In the middle of May the company Arbor Networks published on a blog a number of details of the attacks. Arbor Networks runs a traffic-monitoring tool with measurement points positioned all over the Internet. On the blog it was reported that a total of 128 unique DDoS attacks on Estonian websites had been detected. Of those, 115 attacks comprised ping-flooding, four SYN flooding and nine other types of attack. Most affected were the websites of parliament and the Prime Minister (36 attacks), the Estonian police (35 attacks) and the Estonian Ministry of Finance (35 attacks). The predominant proportion of attacks seen by the company lasted for under an hour and generated maximum traffic flows of 30 Mbps, though a quarter of the attacks were bigger, and the ten very biggest attacks were estimated at 90 Mbps and lasted up to 10 hours.

Official Estonian reactions

The Internet attacks led to extensive articles in the mass media and the specialist press all over the world. Estonia initially pointed the finger at Russia, but quickly withdrew the accusation when it proved very hard to point out any particular attacker. In as far as the origin could be traced, these traces pointed to computers spread all over the world.

The attacks also led to Estonia taking measures with regard to NATO, whereby they sought to put the issue of Internet attacks (cyber attacks) onto the security-policy agenda by asserting that such attacks should be inserted into NATO's agreement texts on mutual military aid. This was also taken up at NATO meetings in June, and the discussion is continuing within the organisation.

In a speech to the UN's general assembly at the end of September, Estonia's president Hendrik Ilves also appealed for a UN convention on cyber-warfare and cyber terrorism.

Russian activism as an influencing factor

Over the past two years several new political movements have changed the domestic-policy schedule in Russia. The radical Nasji ('we''us') movement faithful to Putin is of particular interest, as its members have been linked to several events connected with the Internet attacks on Estonia.

It was Nasji activists who subjected Estonia's embassy in Moscow to a blockade in conjunction with the riots in Tallinn. The activists stretched out a big streamer representing the bronze statue in front of the embassy building, tore down the Estonian flag and got into a scuffle with the Estonian ambassador's bodyguards. In conjunction with the blockade the Swedish ambassador was also mobbed as he left the Estonian embassy building in a car, and for a short while got stuck in the crowd.

A Nasji commissioner stated that he met a leading Russian-Estonian opposition politician in Tallin on 20 April – exactly a week before the riots broke out and the Internet attacks began.

A Nasji representative appeared in the media on 2 May and said that he had personally taken part in the Internet attacks on Estonia, and that they had taken place from a site in the breakaway region of Transdnier in Moldavia. He simultaneously denied that the Russian administration had been involved.

Immediately adjacent to the bronze statue the Estonian authorities have repeatedly arrested (and subsequently deported) young Russians who as a silent protest had positioned themselves by the statue in old Russian uniforms. For a period of two months such arrests took place on at least seven different occasions.

Conclusions – the events in Estonia

The events in Estonia clearly show that coordinated Internet attacks are no longer a remote vision but can already be used as an active means of exerting political influence. An attacker or group of attackers can without any major problems implement attacks that interrupt the normal business of authorities and commerce in another country – and furthermore conceal their own involvement in the attack.

The events in Estonia have also shown that it is possible to defend yourself against Internet attacks, though it is important to acquire the capacity for manoeuvre by quickly getting organised and preparing countermeasures that can limit the effects.

A critical factor in this context proved to be the capacity to quickly produce a reliable function for creating a picture of the situation by setting up a national team involving the participation of many sectors of society. Even though the attacks took place through the Internet they affected businesses in many areas of society, ranging from schools in areas of low population to nationally disseminated mass media, banks and central authorities.

Technically it was also essential to have access to traffic measurements in strategically selected locations in one's own networks, to which access was gained from the unified Internet environment used by Estonia's authorities and from domestic Internet operators.

Another critical factor was international collaboration. The incident management body CERT-EE had an international contact network and quickly contacted its collaborating partners in other countries for assistance in the work of cutting off the traffic from computers used in the attacks. Within a mere few days the outside world had been made aware, and a few days later more detailed information was disseminated that helped operators all over the world to filter abnormally large traffic flows directed at target systems in Estonia.

Part 2

Sweden's emergency preparedness for Internet attacks



Introduction

The Internet attacks on Estonia have given Estonian authorities and private players practical experience in handling a large-scale Internet attack. The media's diligent reporting of the events also contributed to an increased awareness in the outside world that coordinated Internet attacks were no longer science fiction. We have taken the Estonian experiences as a point of departure for analysis of Swedish vulnerabilities and the possible consequences if Sweden were to suffer a similar attack.

To facilitate reading comprehension and so as to achieve a clearer link between the Estonian partial report and the Swedish part of the report we have listed the prominent features of the Estonian partial report:

Prominent features of the events in Estonia:

Background – Even before the Internet attacks in Estonia some form of aggression had built up in society.

Objective – There was probably no underlying financial reason for the attacks. They have instead been explained as being politically ideological and to some extent sort of 'cyber riots', i.e. demonstrations starting on the street and transferring to the Internet.

Course of events – An introductory stage primarily involved simple access attacks, which then gave way to more sophisticated and better coordinated attacks involving large botnets.

Aim – Authorities, political websites and the media were attacked, plus banks, small municipalities and rural schools. The media also spoke of attacks on the Estonian telephone system, though there were no reports of successful attempts. Attempts were also made to attack the mobile network and the system used by the Estonian rescue service.

Exacerbating factor – The situation was probably exacerbated by the fact that the Estonian Internet connections were unable to cope with really large, sustained traffic flows.

Key factors for efficient handling:

Organisation of countermeasures – The capacity to quickly get organised has proven to be very important in the planning of countermeasures to limit the effects of a possible attack.

Establishing a team – In order to form an overall picture of the situation as soon as possible it is necessary for representatives from the various parts of society affected to quickly gather in team-like groupings.

Technical data – Handling of a major attack requires access to traffic measurements from strategically selected locations in one's own networks. In Estonia this was facilitated by the authorities' joint Internet environment and close collaboration with domestic Internet operators.

International collaboration – Good contacts with other players, including players abroad, have proven necessary to facilitate cut off of the traffic close to computers used in attacks.

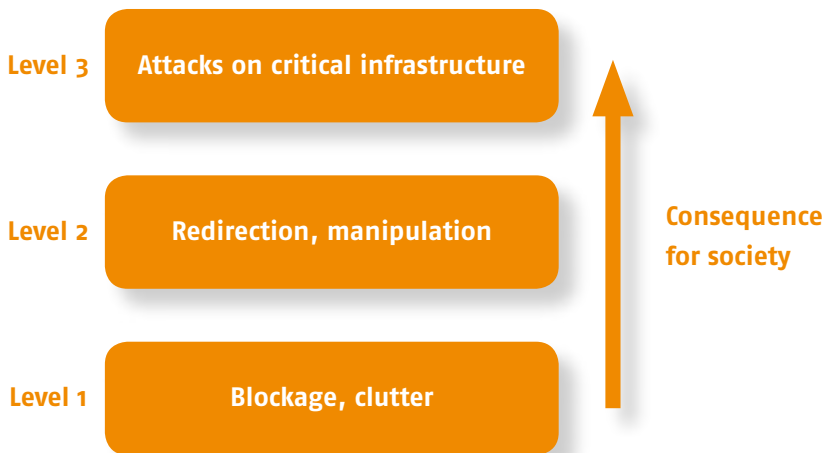
Possible threats and threat levels

Internet attacks of the extensive kind that affected Estonia in spring 2007 have not hitherto occurred in Sweden. The answer to the question as to whether anything similar could happen here is simple. The two countries have different overall security policy situations, and likewise different potential threats. The events equally give reason to consider the possible consequences of one or more similar Internet attacks if they were directed at societal functions in Sweden.

This presentation is entirely based on large-scale antagonistic threats, i.e. attacks staged by one or more players who intend and are able to damage vital societal functions in the country. We ignore criminal attacks of a limited scope and operational stability – matters handled entirely within the parameters of police work and the authorities' responsibility for Internet security.

Internet attacks can be staged in a number of different ways. One possibility is access attacks with the aim of limiting access to computer resources, e.g. e-mail systems and websites. Hacking can aim to interrupt operation, change information or completely take over an information system. There is also a category of Internet attack that aims to disrupt or stop socially important infrastructure of a kind completely different from information systems per se, e.g. telephone networks, electricity networks, water purification and process industries.

The forms of attack can be graded in accordance with a successful attack's potential consequences for society, and then categorised according to distinct threat levels. It is essential to bear these levels in mind when considering society's capacity to handle Internet attacks.



Level 1 – Blockage and clutter

This level firstly involves attacks with the aim of blocking access to information resources, i.e. so-called access attacks (denial of service), and secondly limited hacking of websites with the aim of demonstrating the target objects' lack of security (defacements). The latter usually occurs in combination with publication of clear signatures (tags) and disparaging or hostile comments.

Attacks at this level are often relatively easy to carry out, and when the reasons involve activism the target object is often of a symbolically important nature. Defacements are sometimes carried out in large numbers – not least in conjunction with conflicts between hackers or hacker groups. When information is manipulated at this level it is relatively easy to detect

Level 1

Level 2 – Redirection, manipulation

This level firstly involves attacks whereby Internet calls, references or signatures are manipulated in such a way that traffic is discarded or incorrectly routed or information is incorrectly assessed as being reliable, and secondly more advanced hacking with the purpose of taking over target systems and manipulating information with a fraudulent aim.

Attacks at this level have a higher aim than demonstration of the attacker's ability. They involve manipulation of information, e.g. by publishing false official messages, false news, rerouting traffic to a falsified website or Internet bank, conning users into revealing log on details, announcing false routes in networks or completely taking over one or more authority computers.

Attackers at this level require far greater ability than for Level 1. The methods are often closely linked to those used in advanced Internet crime, e.g. targeted dissemination of malicious code (malware) using trojans or manipulated websites, use of botnets or advanced exploitation of security gaps through so-called 'exploits'.

Level 2

The methods of attack at this level can give attackers the opportunity to carry out regular psychological information operations (psyops, perception management), whereby false or partially falsified information helps attackers achieve their aims

Level 3

Level 3 – Attacks targeting critical social infrastructure
This level involves attacks on information systems that control facilities of vital importance to society, e.g. electricity networks, nuclear power, water supply, rail networks, road signalling etc. These systems are often given the collective name of SCADA (Supervisory Control and Data Acquisition) process-control systems.

Attacks at this level normally demand much greater ability of the attacker, but the effect of a successful attack on an information system of this type can have very serious consequences for society.

As far as society is concerned, it is of course important to apply well considered prioritisation when handling incidents of the above nature. To simplify things slightly, it can be said that Level 1 attacks are indubitably irritating and create a temporary absence of Internet resources, loss of prestige and maybe loss of income, but that they do not need to entail a threat to society more serious than a mere temporary operational disturbance. It is not until Level 2 and Level 3 that attacks can have more serious consequences for society.

Level 3 attacks can have major consequences and sometimes cause practically irreparable damage to critical infrastructure. In many countries protective measures at this level have been given a high priority. Of the Swedish the authorities it is above all the Security Police and the Swedish Emergency Management Agency who are studying this type of threat.

The Internet in Sweden



Structure and dissemination

The Internet in Sweden is based on a number of major and physically separate backbone networks handled by private Internet operators. Several of them have their own international ramifications and their own connections with other operators. In part the Internet operators directly exchange traffic with each other, and in part they do so on nodes located in Sweden or abroad.

In Sweden there are several nodes that convey large amounts of traffic. They are run by the company Netnod, which is owned by the Foundation for Internet Infrastructure. The aim of the nodes is to facilitate exchange of traffic and create a stable and robust infrastructure in the central parts of the Internet in Sweden. This is reinforced by the nodes being in protected operating locations. Exchange of Internet traffic takes place at five locations: Stockholm, Gothenburg, Malmö, Sundsvall and Luleå. Exchanges of traffic in the different cities/towns are interdependent.

Netnod works in close collaboration with the Swedish Internet Operators' Forum (SOF), which principally gathers operators with a direct link to the national Internet nodes. SOF also works on matters regarding joint traffic and other functions and operational issues necessary for optimum functioning of the Internet in Sweden¹. In 2000 Netnod created the operating company Autonomica, which in addition to operation of the Internet nodes in Sweden also looks after one of the 13 root-name servers in the Internet's DNS (Domain Name System) cataloguing system. The root name server is divided amongst 26 locations worldwide but is controlled from Stockholm².

¹ <http://www.isoc.se/sajt/bilder/pdf/vem%20og%C3%B6r%20vad.pdf>

² <http://www.netnod.se/>

There is no unified network infrastructure for authority networks in Sweden. The Swedish authorities themselves are responsible for their IT systems and connections with the outside world. The way in which Estonia gathered its authority networks in a homogeneous and well-protected Internet environment has no counterpart in Sweden.

In Sweden there are currently about 2.5 million broadband subscriptions, which is equivalent to about half of all households. In December 2006 the number of subscribers with an Internet connection capable of handling at least 2 Mbit/s downstream (in a direction towards the subscriber) was over 1.5 million, which is equivalent to two thirds of all fixed connection subscriptions.

There has also been an increase in the number of Internet accesses with far higher speeds than 2 Mbit/s. The proportion of subscriptions comprising fixed connection to the Internet has been concentrated on six major Internet suppliers, who have nearly 90 per cent of the market (2007). There are a total of over 170³ companies offering broadband subscriptions.

75 per cent of the basic public services in Sweden can currently be carried out electronically, i.e. electronic case handling is available via the Internet. Sweden has invested in high-quality services from the major authorities, rather than local and regional services⁴.

There is currently one national top domain for Sweden: .se. The Foundation for Internet Infrastructure (the II Foundation) has the responsibility and the remit of developing and managing operation of the top domain. There are currently over 676,000⁵ active .se domains

³ http://www.pts.se/Archive/Documents/SE/Bredband_in_Sweden_2007.pdf

⁴ <http://www.capgemini.com>

⁵ <http://www.iis.se>

Most operators' networks are monitored from their own centres, where they have dedicated incident-management functions and abuse departments that operate 24 hours a day. There are also functions for detection of hacking that operate 24 hours a day, plus logical agents in the network – so-called probes or sensors – that can issue alarms regarding abnormal traffic flows, e.g. in the event of access attacks. In such an event there will be an attempt to trace the disturbing source and filter away its traffic. Some operators have contacts with external incident management functions, including equivalent groups of other domestic operators, so as to obtain early warning of ongoing attacks and detect security gaps⁶.



⁶ <http://www.pts.se/Archive/Documents/SE/Ar%20Internet%20i%20Sverige%20robust.pdf>

**Public distribution
of responsibility**



Distribution of responsibility at departmental level

Work on information security in Sweden is governed by the responsibility principle, which means that authorities, companies and organisations with normal operational responsibility are also responsible for informational security.⁷ The principle also applies at departmental level, which means that handling agents in the authorities' various departments look after information-security issues for the authority in question. However, information security is one of many areas the handling agents have to deal with.⁸ There is thus no special department with responsibility for information-security issues, though some departments have been given coordinating responsibility for specific matters, one example being electronic communications, for which the Swedish Ministry for Industry, Employment and Communications is responsible. A number of expert authorities (the Swedish National Defence Radio Establishment, the Swedish Emergency Management Agency, the Swedish Administrative Development Agency, the Swedish National Post and Telecom Agency, the Swedish Defence Materiel Administration, the Swedish Police and the Swedish Armed Forces) have also been given special responsibility in various segments of the field of information security.

Hitherto, however, the government has not coordinated information security issues within the Swedish Government Offices so that all departments receive the same information/descriptions regarding threats, risks, vulnerabilities and the need for measures in the area (see section p. 26 on the Swedish National Audit Office's audit of governmental control). In such work more stringent demands could be made of the expert authorities in the area regarding production of relevant and practical information that can form a basis for decision-making.

⁷ Government bill 1999/2000:30, The new armed forces

⁸ 'Governmental control of information-security work in state administration', Swedish National Audit Office Report RIR 2007:10, p 47

Distribution of responsibility amongst the Swedish authorities

As mentioned before, all the authorities are obliged to ensure sufficient information security within their own operations, but some authorities work more directly on information security than others.

The Police

Through the National Swedish Criminal Investigation Department (RKP), the Swedish National Police Board (RPS) has created an IT crime unit comprising four groups. They form part of networks of IT experts both internationally, at Interpol and on the G8's contact list, and nationally, with contacts within the field. In the Swedish Security Service (Säpo) the Security Protection Unit has special supervisory responsibility in accordance with the security protection legislation regarding important societal functions' protection against IT attacks, and they continuously analyse IT-related incidents, threats and vulnerabilities.

Regarding creation of an overall picture in connection with incidents, together with Säpo, RKP has formed a coordinating function for crime related IT incidents (S-BIT). It is a way in for anyone needing to contact the police in the event of suspicion of a crime-related IT incident. S BIT also acts as an interface with other players in society who hold information in the field of information security.

Swedish Armed Forces

The Swedish Armed Forces (FM) have supervisory responsibility in accordance with the Security Protection Ordinance, which covers the Swedish National Defence College, the Swedish Defence Materiel Administration, the Swedish Defence Research Agency, the Swedish National Defence Radio Establishment, the Swedish National Fortifications Administration and the Swedish National Service Administration.

Monitoring of the Swedish Armed Forces' own networks is carried out by the Swedish Armed Forces Computer Emergency Response Team (CERT). The aim of monitoring is to ensure confidentiality, availability, correctness and traceability in the network. The remit of the Swedish Armed Forces Joint Communication Agency (FMTM) is to look after system operation and system-operation management of the Swedish Armed Forces' joint telecommunications infrastructure.

In practice the Swedish Armed Forces has the role of National Communications Security Authority (NCSA) and National Distribution Authority (NDA) through the security offices of the Swedish Military Intelligence and Security Service (MUST). The threats faced by the Swedish Armed Forces and their supervisory authorities in the field of information security include foreign countries' intelligence and signal-tracing services.

The Swedish Defence Materiel Administration and CSEC

At the Swedish Defence Materiel Administration is the Swedish Certification Body for IT Security (CSEC), which uses the certification standard Common Criteria (CC). Even though CSEC has no specified operational role in the event of an Internet attack, its work may be of importance in incident management. All the certifying bodies using Common Criteria do have extensive documentation on product properties and vulnerabilities in areas such as program code. In certain instances CSEC would be able to gain access through its contact network to information that can facilitate troubleshooting and rectification of critical errors.

Swedish National Defence Radio Establishment

The Swedish National Defence Radio Establishment (FRA) must support measures with IT contributions in the event of national emergencies, participate in identification of players involved in the event of IT-related threats to

socially important systems, carry out IT-security analyses, give authorities and state-owned companies technical support, provide signal protection operations with cryptological authorisation and maintain a high level of technical expertise in the field of information security.

On request FRA must assist authorities and state-owned companies who manage information deemed sensitive with regard to vulnerability or to security policy or defence policy. The assignment is limited, however, to state-owned companies who carry out socially important business. FRA has the remit of ensuring that expertise is available at national level. FRA assists Säpo in the supervision in accordance with security-protection legislation.

Swedish National Post and Telecom Agency and Sitic

In the field of information security the Swedish National Post and Telecom Agency (PTS) bears responsibility pursuant to the Electronic Communications Act (2003:389). This includes requirements regarding good function, technical security and integrity protection in electronic communication such as telephony, mobile telephony and the Internet. PTS strives to attain more robust and more reliable networks and to prevent networks being put out of action during disturbances. The authority also carries out investigations and provides information in the field of Internet security.

The Swedish IT Incident Centre (Sitic) is part of PTS. Sitic's remit is to act as a national centre for reporting of IT incidents and a resource for the support of society's protection against IT incidents. Sitic disseminates information on new problems that may interrupt IT activities, at the same time as providing advice on preventive measures and compiling statistics.

Sitic collaborates with a number of national and international organisations in order to be able to operate in the event of an incident. Sitic is a member of FIRST, an international forum for trusted CSIRTs that jointly handle IT security incidents and encourage preventive measures in

this field by developing and exchanging technical information, tools, methods, processes and best practices.⁹

Sitic is also a member of EGC, an informal group comprising European sister organisations. Its aim is to develop efficient collaboration in the field of information security by preparing measures to handle major IT security incidents that may have effects across national borders, to exchange information and technology related to IT-security incidents, harmful code and vulnerabilities, and to identify skills and expertise that can be called on within the group.¹⁰

Swedish Emergency Management Agency

The Swedish Emergency Management Agency (SEMA) has overall official responsibility for questions concerning society's information security, which also includes more extensive Internet incidents that may affect the stability of Swedish society.

Neither SEMA nor any other authority has any specific responsibility for national management of the work on information-security issues. However, SEMA manages the authority collaboration SAMFI (Joint Action Group on Information Security) which includes the Swedish National Post and Telecom Agency/Sitic, the Swedish Armed Forces, VERVA, the Swedish National Police Board and the Swedish Defence Materiel Administration.

SEMA also works actively on projects involving collaboration between the state and commerce, including in the field of SCADA. Internationally SEMA is also Sweden's national point of contact regarding information-security matters.

In 2006 SEMA together with the Swedish Rescue Services Agency was assigned with preparing and starting the establishment of a situation presentation function with the aim of rapidly detecting serious events, notifying affected players and providing an overall national picture of the situation and cross-sector analysis.

⁹ www.sitic.se

¹⁰ <http://www.egc-group.org>

In the event of a comprehensive threat to technical infrastructure, e.g. in the form of an extensive Internet attack, SEMA has the role of convening strategic players to form a team. These players are primarily the authorities who form part of the collaborative body SAMFI (see below). Should this scenario develop, SEMA's situation centre will be activated so it can follow the situation and compile a picture of the current situation. SEMA's remit also includes analysing the consequences of the event in question, both in the short and the long term, and proposing possible measures. SEMA must also notify the department and other affected players of the current situation. When there is a threat to technical infrastructure it is natural that the situation centre should be manned both with support staff from SEMA and with other supporting players, e.g. Sitic and FRA.

Collaboration

SAMFI

The Collaborative Group for Information Security (SAMFI) is a collaborative body for authorities with information security-related operations. It was formed in 2003 against the backdrop of the government's then new strategy for information security in society that had been proposed in the government bill Civic Safety and Emergency Preparedness (2001/02: 158). SAMFI comprises the Swedish Emergency Management Agency, the Swedish National Post and Telecom Agency, the Swedish National Defence Radio Establishment, the Swedish Defence Materiel Administration, the Police/Swedish Security Service (via S-BIT), the Swedish Armed Forces and VERVA. The Swedish Emergency Management Agency is the convening authority.

Through exchange of information and collaboration SAMFI supports the work of the participating authorities. Usually the body acts in the main in fields such as strategy and regulatory frameworks, technical matters, standardisation issues and national and international action, as well as

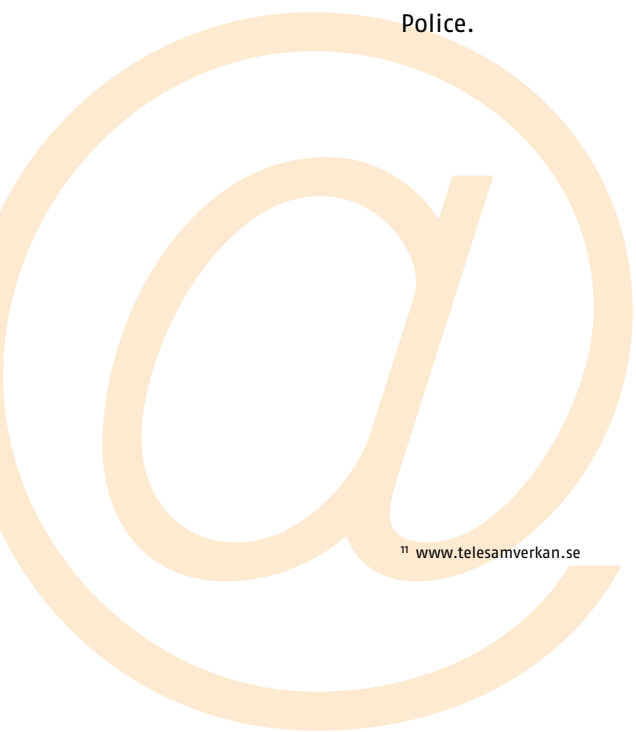
through awareness raising measures. If there is an event of major social significance SAMFI has the potential to act by way of national strategic management support for the individual authorities.

Other collaborative fora

There are a number of voluntary formal and informal collaborative fora for information–security matters. These fora have in many cases been formed on the basis of joint interest and are thus subdivided by sectors. One example of this is the National Telecommunications Coordination Group (NTSG), which was formed in August 2005 and is a voluntary collaborative forum for telecom operators or other organisations with their own technical equipment. The aim is to support restoration of the national infrastructure for electronic communications in the event of extraordinary events in society. By virtue of their role these operators/organisations have the possibility of major influence on the critical national infrastructure for electronic communication.¹¹

Collaboration also takes place between Swedish intelligence authorities regarding assessments of threats and events in the outside world. This circle also includes MUST, the Swedish National Defence Radio Establishment and the Police.

¹¹ www.telesamverkan.se



**Vulnerabilities of
the Swedish branch
of the Internet**



Internet infrastructure

Backbone network infrastructure in Sweden is characterised by high capacity and operator networks which in numerous instances extend beyond the country's borders and have many connections with the outside world. The risk of the Swedish branch of the Internet being completely blocked by access attacks must thus be described as relatively small.

But the international interweaving that has taken place simultaneously decreases the possibility of isolating 'Sweden' from the rest of the Internet, which might be desirable in the event of extensive global disturbances on the Internet, or in a security-policy situation in which we for some reason wish to limit the exchange of traffic with the outside world, or at least increase control of traffic flows into and out of the country. It is currently very hard to precisely determine which backbone-network connections pass through borders. The same applies to the total amount of traffic that these connections manage to convey.

The Swedish access networks are also generally characterised by high individual capacity of the broadband connections to our households, which is a natural consequence of rapid technological development. This gives us access to a number of new services, but also increases vulnerability. When data, telephony and radio/TV are transmitted via the same connection a disturbance can have more serious consequences than with separate connections.

The high bandwidth of household Internet connections also entails a new potential threat to important societal functions. The impact of a botnet of infected home computers can be huge if all systems run on high capacity broadband connections. Gathered in a single botnet, Sweden's 2.5 million broadband-connected households

¹² We are reckoning here on each broadband connection coping with at least 200 kbit per second 'upstream' (going out onto the Internet from households) and on there not being any bottlenecks in the operators' backbone networks that limit the total traffic flow. The latter should in practice limit the effect

would in theory be capable of a total capacity at least 500 to 1,000 times bigger than was the case with the biggest wave of attacks observed in Estonia.¹²

One factor that reinforces this threat is the fact that privately owned computers are often far less well protected against harmful code and regular hacking than computers of companies and authorities. Private individuals usually lack the expertise and the procedures required to maintain a high level of security, e.g. by frequently upgrading software, sealing all security gaps and avoiding pre-installed passwords.

The backbone-network infrastructure can be subjected to traffic congestion in conjunction with access attacks. E-mail servers positioned at the operators can also be overloaded, even though this problem has radically decreased in recent years. Internet equipment can be disturbed and in certain instances even put out of action or taken over as a result of targeted hacking. These effects are well known amongst those working in the field of Internet security, and within the standardisation body IETF active work on coping with both existing and potential problems has long been in progress. Two of the basic functions deemed critical on the Internet are the catalogue service DNS and Border Gateway Protocol (BGP) routing.

The global DNS system has hitherto suffered two extensive attempted attacks that have seriously disrupted parts of the system but not succeeded in putting it out of action. During 2002 a number of the 13 so called root server systems suffered serious disturbances. The attacks led to reinforcement of the DNS system, and in a renewed attempted attack in February 2007 the attackers only succeeded in seriously disrupting the operation of three root-server systems. The systems distributing their operation to many servers worldwide generally coped well.

The DNS system is now said to be very robust. This also applies to the DNS infrastructure in Sweden, including the Swedish top domain .se, which is managed by the Foundation for Internet Infrastructure. The vulnerabilities

of the Swedish part of the DNS system are not currently at operator level, but lie mainly with those domain-name owners who manage their domains themselves.

More extensive attacks on GBP routing have not hitherto occurred, either abroad or in Sweden. Alongside commercial agreements on traffic exchange the system is largely based on trust in the international collaboration between operators. Within IETF there has been a start on taking stock of the existing attack options and safeguarding the present exchange of messages, but much remains to be done.

But what constitutes a clear vulnerability is the limited number of people in Sweden who have the requisite operational experience for handling of extensive and extended Internet incidents. These people are mainly to be found amongst the Internet operators and in the node company. The situation is the same in many parts of the world.

In everyday operation the Swedish Internet infrastructure works well, and limited incidents can be handled by the Internet operators themselves and the independent node company without any further state support. But in the event of very extensive incidents that threaten society it is possible that more manpower will be needed – chiefly people with experience of the special tasks that may be needed, e.g. analysis of traffic data. Ensuring that this expertise is maintained and is available amongst a sufficiently wide circle of people would constitute a contribution from society to an otherwise well functioning Internet infrastructure.

Authority networks and public websites

Nearly all Swedish authorities currently are connected to the Internet. A large number of them provide services for private individuals, companies and other interested parties in society. The scope of this business will probably increase in the coming years, not least bearing in mind the initiative involving the so-called 24-hour authority, the aim of which is to get authorities to provide people with 24-hour e-services.

Authorities' networks can suffer attacks at several different levels. Websites can be affected by access attacks and defacements, and e-mail servers can be blocked. The information in the DNS system that indicates where the authorities' services are to be found can under certain conditions be manipulated. Computers inside the authorities' internal networks can also suffer targeted attacks, e.g. using previously unknown harmful code and thus undetectable. Swedish companies have already suffered such attacks, and it is not improbable that a wider, planned Level 2 attack will be accompanied by such targeted attacks.

The vulnerability of an authority network in part depends on how it is connected to the Internet and how various resources (e.g. website or e mail servers) are advertised on the Internet. An introductory inventory of how authorities use the Internet's catalogue system DNS has recently been carried out. It will probably be supplemented with a review of how more important authorities can be reached, by investigating operators and more important Internet connections.

In September 2007 SEMA and the Foundation for Internet Infrastructure (.SE) carried out a joint investigation of how DNS is used by Swedish authorities and other socially important organisations. The investigation covered over 800 different players and resulted in a number of very interesting observations, which are recorded in a report.

The investigation shows a large number of direct errors and defects in the players' handling with regard to DNS systems. The results probably show that more knowledge of the DNS system is needed on the part of the players.¹³

One of the most prominent defects proved to be the fact that over 10 per cent of name servers are run on old software, making it easy to break into the computer and re route web traffic and e-mail to false addresses. 40 per cent of the name servers also permitted a function called open recursion, which means they can be used in access attacks. Many businesses also had too few name servers, or name servers that were too concentrated or incorrectly set.

It is also worth noting that few Swedish authorities currently use the option of verifying e-mail using functions such as SPF (Sender Policy Framework) or the option of safeguarding information on their Internet domain by means of digital source protection (signing). The latter means that in the event of an emergency it can be hard to verify whether the information a authority is disseminating on the Internet really comes from the authority or from a false sender.

Signing of domains in the domain system DNS is achieved using the technology DNSSEC (DNS Security Extensions), though very few Swedish players have hitherto started using this technology. The Swedish National Post and Telecom Agency and the Foundation for Internet Infrastructure are actively working on increasing use, and this can be seen as very important work on reinforcing the integrity of Swedish Internet domains. Recently the Foundation also requested that the international domain body ICANN sign the top so-called root zone in the DNS system.

In 2005 and 2006 the Swedish National Audit Office audited the way authorities manage their internal information security, and this was summarised in a report earlier this year. There is still no complete inventory of the Swedish

¹³ 'Nåbarhet på nätet, hälsoläget i .SE 2007' [Accessibility on the Internet, the state of health of .SE 2007] .SE, SEMA

authorities' Internet services – a prioritisation that shows which services can be deemed to be of particular social importance and a survey of how they are protected against Level 1 and Level 2 Internet attacks.

The Swedish Security Service is the supervisory authority for authorities to whom special requirements apply in accordance with security-protection legislation. They carry out regular reviews, and also have excellently functioning operational collaboration with the open police. The Swedish Security Service is also actively working on an investigation of the systems that may be vulnerable to Level 3 attacks.

An evident defect, however, is the fact that there have hitherto been no uniform security requirements regarding the authorities' Internet services in the form of regulations – especially requirements reinforcing the authorities' capacity to oppose external attacks at various levels. As from 1 January 2008, however, a new information security regulation from VERVA will be coming into force. VERVA has decreed that the standards Management Systems for Information Security (SS ISO/IEC 27001) and Guidelines for Control of Information Security (SS ISO/IEC 27002) shall apply throughout the field of state administration.

The responsibility principle in the field of information security does not relieve the state of the responsibility of guaranteeing that the state authorities' IT use meets security requirements. It is a matter of trust with regard to both the general public and companies.¹⁴ As a result of this the Swedish National Audit Office has audited the government's control of information security work in state administration. An overall problem arising in connection with the audit is the lack of control over the authorities' information security work.

There are also major deficiencies in the authorities' information-security work, and it has been stated that this is largely because management does not assume sufficient

¹⁴ 'Governmental control of information-security work in state administration', Swedish National Audit Office Report RIR 2007:10, p. 13

responsibility for information security matters. There is often a lack of information on the authority's information assets that are worth protecting. There are also no continuity plans, and it has been reported that the staff often lack training in the area. It is thus no surprise that the Swedish National Audit Office's audit reports that managements have an unclear picture of the risks faced by the authorities in question.¹⁵

Another problem is lack of clarity and lack of knowledge regarding how security incidents should be handled. Which incidents should be reported? How should they be documented and how should shortcomings be remedied?

In the event of a major Internet attack the authorities' shortcomings would probably lead to difficulties handling the emergency situation arising.

Other societally important information infrastructure

Swedish mass media

Alongside the Internet operators, the mass media are probably the social sector in Sweden that has now managed to acquire the most extensive experience of major traffic deviations in their Internet connections. It is a matter firstly of handling the abnormally heavy traffic load arising in the event of major news events, and secondly regular Internet attacks when an individual or social group has got worked up about what has been published.

The mass media's existence is reliant on constant accessibility. Major resources have thus been invested – above all in the national media's news webs. It is highly probable that in the event of an emergency they will prove to be at least as robust as many of the websites run by the authorities – if not more so.

¹⁵ 'Governmental control of information-security work in state administration', Swedish National Audit Office Report RiR 2007:10

Despite this it cannot be excluded that the Swedish mass media will be particularly affected in conjunction with a major Internet attack on Sweden. In Estonia the national press was already affected in the initial wave of attacks. No centralised websites can currently be completely protected against targeted access attacks if the traffic volumes targeted at the website are big enough to overload available Internet connections. Admittedly capacity is constantly being expanded, but media content is simultaneously requiring greater resources – likewise the number of users with broadband connections.

Digital control systems (SCADA)

According to all the available information the access attacks on Estonia did not affect any computer-based systems for control or monitoring of critical infrastructure (digital control systems). More detailed studies are required for a qualified assessment of how the Swedish control systems would have coped with an attack similar to that on Estonia. The aim of this report, however, is primarily to clarify the consequences regarding Internet infrastructure, thus the problems regarding security in digital control systems are only being discussed from a more general standpoint.

The digital control systems have traditionally been based on proprietary protocols and technologies, and have been both physically and logically isolated from other networks. Control systems are increasingly being made available via public networks, are increasingly using the same technologies as ordinary IT systems (Ethernet, TCP/IP and databases and OS), and are to a certain extent being integrated with administrative information systems. To sum up, this is leading to a radically changed threat. Security in digital control systems is thus an area that has received great attention in recent years, and these matters are being studied by both industry and the state.

There is a need for an increased social preparedness to handle security in digital control systems, especially with regard to qualified antagonistic IT attacks targeting important societal functions. The fundamental security problems can largely be attributed to dependencies between IT systems and physical supply systems. Questions thus include both what is usually called CIIP (Critical Information Infrastructure Protection) and CIP (Critical Infrastructure Protection). There are currently very few Swedish players with specialised technical skill in the area. Particularly small and medium sized operators of socially critical infrastructures lack both the resources and the expertise to maintain expert security work. Since the area includes aspects vital to national security it is also more important to ensure the existence of state expertise in the field.

Because of the above, since 2004 SEMA has been doing work on security in digital control systems, and the authority intends to make this work permanent and expand it as from 2008. SEMA intends to manage and has financed a coordinated state initiative regarding security in digital control systems. Further information is available firstly in the plan of action for information security that the authority is currently preparing and secondly in the separate report (Roadmap) describing plans for the practical implementation of the work.



Swedish incident management



Attack scenarios

How an incident will be handled depends in all likelihood on its nature and how serious it is deemed to be. It can be assumed that handling of Level 1 attacks on individual socially important websites and authority networks will normally be performed internally by the organisation affected, if necessary by seeking support from the Internet operator(s) used by the organisation, from the police, regarding investigation of the crime, and if necessary from Sitic, for additional advice.

Access attacks may require rapid measures in one or more operator networks. In this context it is primarily Internet operators who are expected to become involved. There is also a possibility of seeking support from Sitic, but its ability to actively influence traffic flows is limited.

The same situation applies to Level 2 and Level 3 attacks on societally important information systems. When one's own organisation cannot handle the event it is principally one's own security consultants who will be called in, and then the Internet operator. This will often involve advanced hacking with potentially enormous consequences, and the police will usually quickly be involved.

No really extensive attacks on important Swedish societal functions or on the Swedish branch of the Internet have hitherto taken place. It is highly probably that at least during the initial phase such an attack would be handled as several separate incidents. In the event of attacks that affect several Swedish authorities or other socially important organisations in parallel it will of course not be possible to maintain a collected picture of the state of affairs in the independently managed authority networks and on the authorities' websites. Such a picture will firstly involve detection of real or potential hacking and secondly studying of traffic patterns. All the individual Internet operators have part of this overview at their disposal, but none of them can currently see the entirety.

There is thus currently no possibility of detecting and following extensive and wide-ranging Internet attacks that affect many Swedish societal functions in parallel, possibly with the exception of major access attacks, which are quickly detected at backbone-network level.

National CERT operations in Sweden

Internationally, numerous organisations have been created in recent years for handling of IT incidents, usually under the designation CERT (Computer Emergency Response Team). As far as society is concerned it is currently Sitic (Swedish IT Incident Centre) that has the express assignment of handling IT-related incidents in Sweden, including disruption of the Swedish branch of the Internet. Sitic is a member of several international collaborative bodies. Operations recently received increased funding, which now makes it possible to maintain 24-hour operation in the same way as the incident organisations of the major Internet operators.

Sitic's remit is largely provision of advice and dissemination and exchange of information concerning IT incidents. All the major operators in Sweden now have their own emergency preparedness for incidents and manage most matters independently, including incidents requiring international cooperation in order to trace traffic or stop attack flows close to the source. Sitic's activities are operational in the sense that the organisation is handling incident alarms issued through the international collaboration between CERT organisations. However, network operators have repeatedly pointed out that they would prefer to see Sitic's operations not being carried out at the supervisory authority in the field of telecommunications.

The mutual collaboration between the Internet operators in Sweden seems to work well in normal circumstances, though the jury is still out regarding the way incident

work would be organised in the event of a large-scale Internet attack on Swedish social interests. Sitic's role in such a situation is unclear.

Sitic has built a system (Honeynet) with sensors that detect attempted attacks. In a pilot project anonymised traffic data from Internet operators is also being collected, though there is currently no function that collected traffic data from the authorities' Internet connections and creates an overall picture of their traffic patterns.

It is easy to state that the Swedish administrative tradition with its independent authorities has made it hard to get a well-functioning picture of the way societally critical infrastructures would be affected in a situation in which Sweden suffered an extensive Internet attack or faced the impending threat of such an attack. Maintaining a true picture of the situation is a critical function in the event of an emergency. In this context Sitic could have a far bigger role to play than at present.

A further factor complicates the situation, however. In the event of extensive access attacks blocking all backbone-network connections it does not suffice to put your own traffic out of action. The network affected must quickly seek outside help, and hostile traffic flows must be put out of action as close to the source as possible, which often means in networks at completely different locations in the world.

Since many attack flows are currently very short, an incident-management organisation faces stringent requirements regarding the ability to work on incidents operationally. Excellent personal contacts with other backbone network operators worldwide are required to facilitate sufficiently quick cut-off of such flows. This is actually a sphere which is currently way beyond state control. The matter has recently become discernible in newspaper reportage, and has long been generally known amongst those working in the field of backbone-network operation. This is also the experience of Estonia.

Summary of national emergency management

Sweden's Internet operators would probably cope with Level 1 attacks independently without state involvement. It is only at the other two levels that more organised national emergency management is necessary. In a comparison with Estonia there are then a number of factors that could be both advantageous and disadvantageous as far as Sweden is concerned.

Looking at the characteristics of the attacks in Estonia, we have already observed that they were preceded by a form of aggression. In the event of more serious events that spread agitation on the streets in the form of demonstrations, we can thus expect that the threat on the Internet will also increase. Which players are the target of a prospective attack will probably depend on a number of different circumstances. But we have learnt from Estonia that it is unlikely that only one sector or player will be attacked. Attacks will rather affect several players simultaneously. In Estonia the massive attacks were a problem because the Internet connections were not really able to cope with large sustained traffic flows. The Swedish backbone networks have much greater capacity, but this does not actually mean any protection against attacks that target individual websites.

If we take a further look at the factors that have proved important to efficient handling, we have already observed that it is essential to quickly organise countermeasures, establish a team, gain access to technical data and commence international cooperation.

The clearest vulnerabilities of Swedish Internet infrastructure are deficiencies in the Swedish authorities' handling of their own security, the lack of an overall picture of the traffic in the Swedish authority networks and the high degree of personal dependence. There are relatively few people in Sweden with the relevant experience to handle

traffic flows at operator level, and only a small group of them have the extensive contact network that would be required in the event of really extensive attacks.

It is very possible that Sitic would act as a body for operational cooperation in conjunction with a major Internet attack on Sweden, together with a more strategically targeted authority team including representatives of the police, intelligence authorities etc. The experiences of Estonia show that such a form of organisation worked well. Alongside the joint authority team that met daily under the management of the Ministry of Defence, all the operators in the country gathered at CERT-EE to discuss the problems mutually, create a joint operational picture of the situation and coordinate their work.

It should simultaneously be borne in mind that right from the very start CERT-EE was closely linked to the joint authority environment that is to be found in Estonia and that goes under the name of X-Road. This Internet environment, like the many authority servers in the country, was one of the targets for the Internet attacks. CERT-EE had access to traffic data – and gained access to further traffic data from the operators.

There is no equivalent access to one's own traffic data from the authorities in Sweden. The structure of the Swedish authorities means it would be far harder to quickly get a corresponding picture of when and how the public information resources have been affected in the event of a large-scale Internet attack.

SEMA's Educational Series in English

- 2008:2 Large scale Internet attacks
- 2006:1 International CEP Handbook 2006 – Civil Emergency Planning
in the NATO/EAPC Countries
- 2003:4 Crisis Journalism – A guidance for government agencies
- 2003:2 International CEP Handbook 2003 – Civil Emergency Planning
in the NATO/EAPC Countries
- 2003:1 Crisis Communication Handbook

ISBN 978-91-85797-14-1
ISSN 1652-3539

Swedish Emergency
Management Agency

P.O. Box 599
SE-101 31 Stockholm

Tel +46 (0)8 593 710 00
Fax +46 (0)8 593 710 01

kbm@kbm-sema.se

[www.krisberedskaps
myndigheten.se](http://www.krisberedskapsmyndigheten.se)