Independent degree project – second cycle

Master's thesis AV, 30 higher credits

Master of Science in Engineering:
Computer Engineering
Industrial Engineering and Management

Vulnerability in a cyberattack
How DoS affects Swedish government authorities

Peter Burgos
Julia Storsten

Mittuniversitetet
MID SWEDEN UNIVERSITY

Vulnerability in a cyberattack –
How DoS affects Swedish government authorities
Peter Burgos, Julia Storsten 2014-11-12

MID SWEDEN UNIVERSITY
Department of Information and Communication Systems (IKS)

Examiner: Tingting Zhang, Prof., tingting.zhang@miun.se
Examiner: Aron Larsson, aron.larsson@miun.se
Internal Supervisor: Daniel Bosk, daniel.bosk@miun.se
External Supervisor: Ross Tsagalidis, MSc.
Author: Peter Burgos, peter.burgos@miun.se
Author: Julia Storsten, just0900@student.miun.se
Degree programme: Master of Science in Engineering: Computer Engineering and Industrial Engineering and Management, 300 higher credits
Main field of study: Information Security
Semester, year: Spring, 2014

Abstract

With a growing development of technologies and the fact that many companies implements online services, an interruption in such service could cause problems for any kind of user by exploiting the vulnerabilities in these systems. The Swedish Armed Forces (SwAF) indicates that the development of the defensive ability must continue, since the vulnerability of the cyberenvironment becomes a greater interest for adversaries. A denial of service can create panic by e.g. force resources to look into the ongoing attack minimizing the awareness of the protection of other systems. Known attacking tools and statistics are presented in this thesis, but the scope is to generate a framework. The main aim is to look into the Swedish government authorities and give an insight of how a possible path for an increased resilience against a modern distributed denial of service attack could be and at the same time expand the knowledge and give a base for developing more secure systems. This thesis consists of a survey and simulations of network traffic behaviors in order to categorize and give a framework for a small, middle and large sized authority. The result shows that a small sized authority has a risk of 47% in not being able to survive an attack, while a middle sized authority only would have 17% as dangerous risk, since that is the risk of having attacks exceeding 60 Gbit/s. A large sized authority is defined by having a capacity of 100 Gbit/s. Therefore, an increased resilience is by exceeding 60 Gbit/s showing that 60% of the authorities within this thesis are prepared against a modern distributed denial of service attack. If an attack succeeds, the authorities are at greater risk to not be able to communicate externally and reach out to the society as impact.

Keywords: DoS, DDoS, resilience, cyberattacks, cyberdefence, attacking tools.

Sammanfattning

Med en snabb teknikutveckling och det faktum att många företag genomför online-tjänster, kan ett avbrott i en sådan tjänst orsaka problem för alla typer av användare genom att utnyttja sårbarheter i dessa system. Försvarsmakten antyder att utvecklingen av den defensiva förmågan måste fortsätta, eftersom sårbarheten i cybermiljön blir ett större intresse för motståndare. En överbelastningsattack kan skapa panik genom att t.ex. tvinga resurser att undersöka en pågående attack vilket minimerar medvetenheten för skydd av andra system. Kända attackverktyg och statistik presenteras i denna studie men avgränsningen är att skapa ett ramverk. Det främsta syftet är att undersöka svenska myndigheter och ge en mall för en ökad motståndskraft mot överbelastningsattacker och att även öka kunskapen och ge en bas för att utveckla säkrare system. Studien består av en enkätundersökning och simuleringar om beteendet av nätverkstrafik för att kategorisera och ge en ram för en liten, medel och stor myndighet. Resultatet av denna studie visar att en liten myndighet har en risk på 47% att inte överleva en attack, medan en medelstor myndighet endast skulle ha en risk på 17% att inte överleva, eftersom det är risken för attacker som överstiger 60 Gbit/s. En stor myndighet definieras genom att ha en kapacitet på 100 Gbit/s. Ett ökat motstånd är därmed en kapacitet på över 60 Gbit/s som visar att 60% av myndigheterna inom denna studie är förberedda inför en överbelastningsattack. Om en attack lyckas, löper myndigheterna större risk att inte kunna kommunicera externt och nå ut till samhället som påverkan.

Nyckelord: DoS, DDoS, motstånd, cyberattacker, cyberförsvar, attackverktyg.

Acknowledgements

This thesis has been conducted as the last examination of the Master of Science program in both computer engineering and industrial engineering and management at Mid Sweden University. There have been a lot of friendly people included as support within this thesis which we would like to thank.

First of all, we would like to express our appreciation to our supervisors at the University, Dr. Aron Larsson and Mr. Daniel Bosk, for all the necessary guidance, the support in achieving our goals and the patience you have had during our meetings.

Secondly, we would like to thank Prof. Cornelia Schiebold and Mr. Sam Lodin for guidance in mathematics, Prof. Tingting Zhang and Mr. Filip Barac for assistance with computer science, and externally Mr. Per-Anders Borgström for helping us establishing valuable contacts.

We would also like to give thanks to our families that we love and cherish. You have supported us during this long journey making it possible to fulfill our dreams.

Last but not least, we would like to thank Mr. Ross W. Tsagalidis at the Swedish Armed Forces and Prof. Mikael Gidlund at Mid Sweden University for believing in us and giving us the opportunity to realize this thesis.

Peter Burgos, M.Sc student
Computer Engineering,
Mid Sweden University

Julia Storsten, M.Sc student
Industrial Engineering and management, Mid Sweden University

FÖRSVARSMAKTEN

Mittuniversitetet
MID SWEDEN UNIVERSITY

Table of Contents

Abbreviations

ACK	Acknowledge, referred to acknowledge packet in computer communication.
CERT/CC	Computer Emergency Response Team Coordination Center.
CERT-SE	Swedish National Computer Emergency Response Team.
CIDR	Classless Interdomain Routing.
CPU	Central Processing Unit.
CSIS	Center for Strategic and International Studies.
DDoS	Distributed Denial of Service, special case of DoS.
DDOSIM	Distributed Denial of Service Simulator.
DoS	Denial of Service.
ENISA	The European Union Agency for Network and Information Security.
FBI	Federal Bureau of Investigation.
FOI	Swedish Defense Research Agency (sv, Total-försvarets forskningsinstitut).
FTP	File Transfer Protocol.
Gbit/s	Gigabit per seconds (measure unit for data transfer).
HOIC	High Orbit Ion Cannon.
HTA	HTML application.

HTML	Hyper Text Markup Language.
HTTP	Hyper Text Transfer Protocol.
ICMP	Internet Control Message Protocol.
IEC	International Electrotechnical Commission.
IGMP	Internet Group Management Protocol.
IMAP	Internet Message Access Protocol.
IIS	Internet Information Service.
IP	Internet Protocol.
IRC	Internet Relay Chat.
ISMS	Information Security Management System.
ISO	International Organization for Standardization.
ISP	Internet service provider.
LOIC	Low Orbit Ion Cannon.
Mbit/s	Megabit per seconds (measure unit for data transfer).
MSB	Swedish Civil Contingencies Agency (sv, Myndigheten för samhällsskydd och beredskap).
Mstream	Multiple Stream.
NATO	North Atlantic Treaty Organization.
Opnet	Optimized Network Engineering Tools.
OSI	Open Systems Interconnection (ISO/IEC 7498-1).

PPS	Packet per seconds (measure unit).
RSS	Rich Site Summary.
SMTP	Simple Mail Transfer Protocol.
SOCKS	Socket Secure.
SQL	Structured Query Language (designed for managing databases).
SSL	Secure Sockets Layer.
SwAF	Swedish Armed Forces (sv, Försvarsmakten).
SYN	Synchronization packet used in TCP containing a 32-bit sequence number.
TCP	Transmission Control Protocol.
TFN	Tribe Flood Network.
UDP	User Datagram Protocol.
XOIC	X Orbit Ion Cannon.

1 Introduction

According to the Swedish National Agency for Education there is a great access to computers among the students in the elementary school. There are around six students on one computer in public schools and around two students on one computer in private or independent schools, which leads to better self confidence in utilizing computers for both searching and creating [1]. It is also easier to obtain a personal computer with access to the Internet for residential use, where statistics [2] shows that the average number of people in a Swedish home is 2.5 persons while the average number of computers in a Swedish home is 2.8 computers, meaning that there are more computers in a Swedish home than actual individuals. It is also certain that the computer in a home is used mainly for Internet access [2]. Maybe this explains the reason why newspapers are writing about young people solving [3] and creating problems [4, 5] for large companies and important parts of the government. The development of computer capacities started to be studied at the end of the 1960s [6] where it indicated that the capacity increases to the double every 12 months and is expected to continue identically if the development adapts to necessary changes [7]. This may be both for the better or for the worse since computers could represent a major role as weapon in e.g. a distributed denial of service attack, causing problems for various important parts of a society, or as victims while being attacked.

With a growing development of technologies and the fact that more and more companies implements online services, e.g. Spotify [8] and Google Drive [9], to make them easily accessible, it generates a behaviour that spreads in the society. This may give a general desire of having similar services everywhere, including Swedish government authorities, e.g. the Swedish Tax Agency [10] and the Swedish Social Insurance Agency [11]. An interruption in the operation within the Internet could cause problems for any kind of user. By e.g. exploiting the vulnerabilities in a system, such as exploiting weaknesses in the design of online services [12], which can therefore be associated to a specific quote:

> *"The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."*
>
> — *Eric Schmidt [13]*

The Swedish Armed Forces (SwAF) indicates [14] that the development of the defensive ability must continue since the conclusion of the evaluation in the same document is that a cyberattack rarely aims to conquer territory, but rather to establish control over strategically important areas for a specific purpose. Since the use of today's technologies increases, the vulnerability of the cyberenvironment becomes a greater interest for potential adversaries. A denial of service (DoS), can create panic by e.g. force resources to look into the ongoing attack minimizing the awareness of the protection of other systems; where attackers could be implementing e.g. hidden attacks such as SQL injections or cross-site scripting [15] while the denial of service attack is keeping human resources occupied. A major problem arises if a Swedish government authority does not follow the development of technology rapidly enough, since prediction of the future is uncertain. Estimations of how long the growth rate of capacities of computers may continue and how it develops is difficult to anticipate. Even though there are some guidance [16] for secure information systems for Swedish government authorities, it is not necessarily certain that all authorities follow them correctly. Depending on how strict the guidance is being followed the level of resilience varies. The lower the resilience is the higher is the risk for an attack to succeed. It is therefore important to study the vulnerability in Swedish government authorities, by looking into the impact of a denial of service.

1.1 Background and problem motivation

> *"Distributed denial-of-service is a major threat that cannot be addressed through isolated action of sparsely deployed defense nodes." [17]*

A distributed denial of service can therefore be interpreted as an attack where defenders and victims have minimal control and power to avoid it, especially when it comes to large-scale attacks.

A distributed denial of service attack is a method used to achieve a denial of service and it may be considered as one of the hardest security problems on the Internet [18]. To understand the seriousness of a distributed denial of service attack against a Swedish government authority, it is important to first understand the vulnerabilities causing the problem and what effect it has.

In some cases there exists attacks that may not be intentional, e.g. when Swedish students applies online for university studies at the same time, shortly before deadline [19]. But if an attack is intended against a Swedish government authority, it can be considered very serious since it affects the whole society. An example is the three-week cyberattack against Estonia [20, 21] that was a total cyber take down of a country, where organizations worldwide reconsidered the importance of the security when it comes to network security.

In 2011 there was a study [22] indicating that a large-scale distributed denial of service attack aimed at core networks can be the choice of attacks in the future military cyberconflicts.

Previous studies in the area of distributed denial of service attacks suggest that a defence system will require the use of several defences, by having e.g. any form of alliance formation [17, 23]. Further there are indications of having organized distributed denial of service attacks in politics, where the blame can be put on opponents, enemies or adversaries of the state creating mass panic and in worst case a war [20, 21].

1.2 Aim

The main aim is to look into the Swedish government authorities and give an insight of how a possible path for an increasing resilience against a modern distributed denial of service attack should be. By having previous studies and historical events in mind, a good question to ask is whether Sweden has been attacked? The answer is yes, both unintentionally [19] and intentionally [24, 25]. The Swedish Armed Forces takes it seriously when Sweden is under attack [25], which leads to an importance of analysing the resilience of the Swedish government authorities'. The purpose is to expand the knowledge and give a base for developing more secure systems, considering that the technology develops fast [14]. By studying how the techniques become more easily accessible and what the reasons of cyberattacks may be, it could make it easier to understand how it comes that attacks increases to a larger scale.

This thesis aims to investigate whether Swedish government authorities are or are not prepared for a modern distributed denial of service attack on a large-scale by giving results of the current situation and estimating the coming five years.

1.3 Scope

The scope of this thesis is to give insight into modern distributed denial of service attacks and not to primary create an ultimate defence solution for vulnerable systems.

This study will only examine distributed denial of service attack as a cyberattack performed by cyberterrorists, looking into the behaviour of overloading the network traffic towards victims, excluding specific layer attacks such as e.g. distributed denial of service attacks targeting the application layer. Distributed denial of service is known for take downs and denying access; meaning that it is not aiming to immediately access sensitive information. Only the capacity and resistance that should attract attention for Swedish government authorities will be looked at and by that give a prediction of how the development could look like in the future.

Note that this thesis treats any kind of attack against a Swedish government authority as cyberterrorism, in order to give a full overview of the concept since the scale between cyberterrorism and cyberwar is an abstract line that cannot be discussed within the scope of this thesis.

1.4 Research questions

The following research questions are defined to achieve the purpose and aim for this thesis:

- What impact does a denial of service have on Swedish government authorities?
- What lower limits are needed in computer and bandwidth capacities for an increased resilience?
- Are Swedish government authorities prepared against a modern distributed denial of service attack?

Further, the following sub questions are taken into consideration in order to achieve the goals of this thesis:

- What does the development of computer and server capacity look like from a historical perspective until now?
- What does an estimation of computer capacities for a period of five years look like?
- What does it take for an attack to succeed and what are the consequences?
- How important is the bandwidth and data transfer rate for an attack to succeed?
- What is the current average bitrate used within Swedish borders according to known statistics?
- What computer and security capacities are being used among Swedish government authorities' at the moment?

1.5 Outline

The first chapter gives the reader an introduction and basic understanding for this thesis. Further on, chapter two describes necessarily knowledge for deeper understanding of this thesis. Chapter three explains the methodology and the approach to achieve the goals of this thesis. The construction design for applying parts of the methodology is presented in chapter four. All results are compiled and presented in chapter five. Finally, chapter six presents our conclusions and suggestions for future work.

1.6 Contributions

This study is a common thesis, where the authors' contribution is a combination from the majors of Industrial Engineering and Management and Computer Engineering. Some parts have been written separately but have been merged together into the chapters in order to keep sustainable flow in this thesis. By writing this thesis together with two different majors, it have provided a more sustainable and convincing conclusion to the reader as it has been seen from two different perspectives. We have learnt a lot from each other during the time and we highly recommend that students studying Master of Science with different majors write together because this is how we will work in the future; putting our knowledge together and create results.

2 Theory

This chapter presents relevant information for further understanding of this thesis.

2.1 Definition of information security

Information security is the need of protecting information and its critical elements from those who are willing to misuse it. Information security can be defined, as:

> *"Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction." [26, 27]*

Information security has become an important aspect since computers represents a great part of the daily activities, whether it is as working tools, for shopping online etc. While this leads to easier access of information it also leads to number of security issues. If the data in a system that is used in e.g. a bank gets exposed to an attacker, it could generate consequences that can be devastating for the users [27]. The most important factors when discussing security issues are confidentiality, integrity and availability, also known as the CIA triad, illustrated in Figure 1.

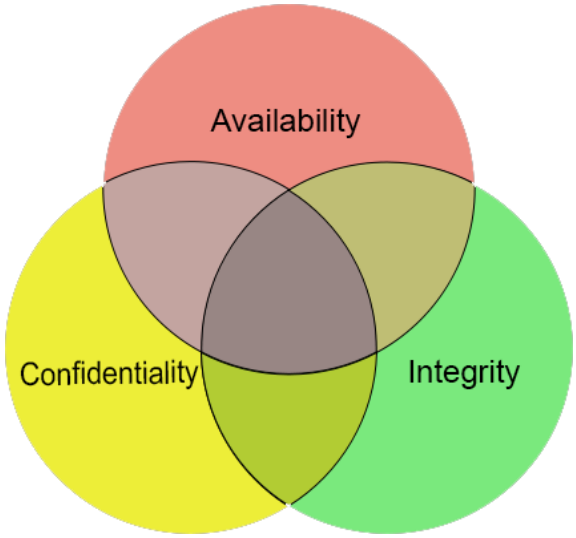


Figure 1: CIA triad.

Confidentiality is the ability to protect data from unauthorized disclosure and limit the data access to those who are authorized [27, 28]. The confidentiality fails if unauthorized users gains access to private information. Confidentiality is an important term when referring to personal information e.g. employees and customers private data. Users rely on the organization regarding their personal information and expect it to be confidential [26]. Integrity is a term used to describe the how data can be prevented from being changed in an unauthorized or undesirable manner. The last term within the CIA triad is availability which explains the ability to access data whenever a user needs it. This study focuses on availability.

2.2 Explanation of cyberterrorism

There are several interpretations of the word cyberterrorism, and there have been long ongoing studies [29, 30] about the definition where no international standard or law has been clarified yet. The explanation of the word cyberterrorism differs from person to person, independent of the level of expertise. Cyberterrorism is a word composed of two terms, those two terms will be defined separately to understand the overall concept. Note that this is a general term that describes illegally performed activities on the Internet, including e.g. cybercrime and cyberespionage.

The prefix cyber originates from the word cybernetic [31] and is often combined as cyberspace, which is a metaphorical expression for the abstract space where the work of computers is assumed to be performed. The word could theoretically be combined with any adverb or noun that can be accomplished by using or having computers, e.g. cyberchat, cybersociety, cybercrime etc.

The Swedish law (SFS 2003:148 2 §) defines a terrorist as

> *"a person that has intentions to commit a crime that has a purpose to seriously harm a state or a government authority with the impact to 1) create fear among the civilians, and habitants, 2) force government authorities or other public organizations to do or abstain from any act, or 3) seriously neutralise or destroy fundamental political, constitutional, economical or social structures of the state or other public organizations."* [32]

A cyberterrorist would thereby be an adversary that fulfills the above requirements by using computers as tools with the purpose to deliver an attack through the network to a specific victim, as confirmed by Lewis from the Center for Strategic and International Studies (CSIS):

> *"…the most likely use of the Internet for what would unquestionably be an act of terrorism would be in form of a 'hybrid attack', with a Denial of Service attack combined with a conventional attack…" [33]*

An act that is associated as an attack is according to the Swedish law (SFS 2007:213 4 kap 9c §):

> *"a person … that obtains resources to perform a task that is meant to automatically treat or illegally change, exterminate, blocks or in a register manipulate such task will be convicted for computer trespassing… The same applies to the person that illegally by using similar methods seriously interrupts or prevents such task." [34]*

Cyberterrorism is therefore defined as a combination of the actual act, through cyberattacks, combined with the purpose or reason for the attack. There are some statements made by international [33] and national agencies [35] that states cyberattacks as following definitions. The definition given by NATO [33]:

> *"A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal."*

The FBI's [33] definition:

> *"Any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."*

And the Swedish FOI's definition:

> *"Cyberterrorism is a general name for a serial of activities such as qualified computer attacks meant to destroy fundamental social infrastructures. In an expand definition it also includes telecommunication as electronic warfare."(Authors translation)* [35]

2.3 Cyberattacks

Within this thesis some examples of attacks will be mentioned, but the focus is on distributed denial of service attacks as a method to achieve denial of service and how it affects systems based on known statistics. Attacks can be divided into two major categories: passive attacks and active attacks, with several sub-categories [36]. Both passive and active attacks represent a major role as security threats, where all attacks can be categorized into one of the following types:

- Interception - is when an unauthorized user has gained access to data allowing e.g. leakage of private information.
- Interruption - is when information becomes unavailable or un-usable on a system.
- Modification - as interception, with addition of tampering with information.
- Fabrication - reminds of modification, with addition of forcing systems to strange behaviours e.g. revealing information from databases.

The methods are illustrated in Figure 2.

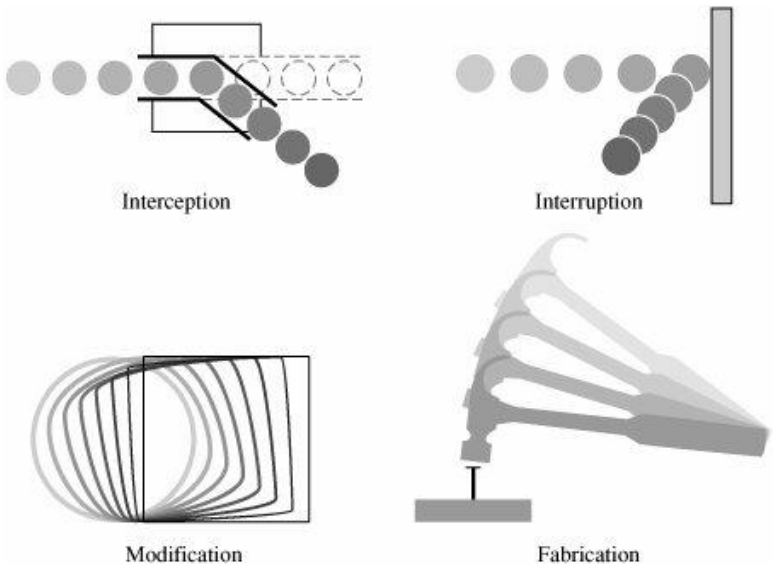


Figure 2. System Security Threats, image source: [37].

Passive attacks can be any action that compromises the security of information by e.g. eavesdropping or traffic analysis. While active attacks are acts that attempt to override the security of a service and in some way violate the security policy of a system, which can be done by e.g. masquerading or message tampering [37].

Denial of service is an active attack and a form of interruption [36] which is explained in the next section.

2.3.1 Attacking availability

Denial of service has become a way to make a statement, regardless of the purpose. Denial of service attacks are different kinds of interruptions [12] that obstructs operations in a system or a service by using an Internet connection, and thereby compromise the availability according to the CIA triad. Some assumptions are that the development of denial of service attacks originated from practical jokes, pranks or proofs of concept in the early days [38]. A practical example is, e.g. Internet relay chat (IRC) [39], where the owner of a channel is called an operator. The operator can allow or deny users to communicate and manipulate conversations by e.g. banning unwanted users. The operator is the owner of the channel as long as the computer is online and connected. Adversaries can exploit that vulnerability by forcing the operator's computer to lose connection with the channel through a denial of service attack, making it possible for other users to take control of the channel.

The same concept has later been applied against, e.g. companies and governments to show disagreement and opinions [38]. A denial of service attack can be difficult for a victim to avoid or control as well as to backtrace, especially if a large-scale attack is performed, which makes it technically possible for attackers to exert extortion attempts [17, 38].

The reasons and motives for a denial of service attack can vary, but the outcome of such an attack is to block a legitimate user from a service, where a service can be e.g. network bandwidth, central processing unit (CPU) calculation time or memory and disk space [38, 40, 41]. Two different ways are commonly used to achieve denial of service; either by using a single-sourced attack or by using a multi-sourced attack, where multi-sourced attacks are more difficult to backtrace and identify regarding the actual number of attackers [42].

According to the Computer Emergency Response Team [43], there are also two other ways to achieve a denial of service, where the first one is to manually change paths to a location or simply remove the destination of the service, which would require access to the current system. The second one is to physically break or interrupt the connection to a service by e.g. rejecting the cable to the power supply.

2.3.1.1 History of denial of service attacks 1980s to 2004

The Computer Emergency Response Team Coordination Center (CERT/CC) was established during the late 1980s [38] after a worm attack known as the Morris worm attack. The purpose with this team was to be one step ahead for possible attacks. A task they are assigned is to "develop advanced methods and technologies to counter large-scale, sophisticated cyber threats" [44].

According to the history of network-based denial of service written in *Internet Denial of Service: Attack and Defense Mechanisms* by Mirkovic et al. [38], denial of service attacks were first noticed as a problem in the mid 1990s where computers had software installed that could be remotely accessed. To be able to make maximal damage by using these computer programs, a requirement was a powerful computer and a fast network connection. Computers with those requirements were only located at the universities at that time, which required a student account to be accessed. Hijacking accounts was the solution to access these computers, which was possible due to the fact that FTP-services that were commonly used had clear-text password problems, which means that intercepting the communication could easily reveal the password.

Smaller groups discovered vulnerabilities in the TCP/IP-stack in 1996 that was used to generate an overload such that a server could not handle the requests. The vulnerability was that the protocol allowed the sending of packets with only the SYN bit set, a technique called SYN flood. A year later, this technique developed to useful tools against IRC networks as an effective method to disconnect a large number of users from the network (similar to the example in chapter 2.2.1).

At the same time a new kind of single-source attack was discovered, named smurf attacks. A smurf attack could reflect and increase the size of network traffic with a factor up to around 200 if bouncing through a misconfigured Class C network or with a factor up to around 60.000 if bouncing through a misconfigured Class B network (see Table 2).

Table 2. IPv4 Address Class Network and Range, compilation: [38].

IP Address Class	CIDR	Dotted-Decimal	Binary	Range (Block size)
B	/16	255.255.0.0	11111111 11111111 00000000 00000000	2^16 - 2 = 65.534 (65.536)
C	/24	255.255.255.0	11111111 11111111 11111111 00000000	2^8 - 2 = 254 (256)

The actual attack is when the source requests communication to all available computers in the network through a so called broadcast with the victims address as return address. This would generate large traffic as reply to the victim which would lead to an overload impossible to deal with.

The perpetrators continued to overload their victims by sending large amount of packets via university networks, with a capacity of 1 Mbit/s, having in mind that the victims network in that time barely could handle around 14 Kbit/s. Since the victims network already were slow relatively the attackers network, the attack made the victims network even slower and not far from useless.

Their bandwidth became more equal between victims and perpetrators after 1998, also the Internet service providers (ISP) learned how to deal with smurf attacks which together made it more difficult for perpetrators to use old techniques as attack method. As a result of this, perpetrators began to control individual computers around the world by remotely accessing them, which could generate large traffic that could be sent by all computers together towards a victim. It was not until after 1999 that this phenomenon started to be known as distributed computing. The first real distributed large-scale attack took place in the middle of 1999. Once again the Internet relay chat networks were the intended victims and since university computers often worked as servers for those networks, they were the actual victims. This attack took down several universities' servers for almost three days. The attacks continued in a great extent which forced the Computer Emergency Response Team to react and organize a workshop in November of 1999, where the situation was discussed.

Thirty experts were invited with the following announcement:

> *"...During the workshop, we hope to analyze these new attack tools; explore their possible evolution and kinds of impact we might see from their use; and outline techniques that can be used to detect, respond to, and recover from attacks." [45]*

Mirkovic et al. [38] continues that in January of 2000 there were some attacks that reminded of smurf attacks, but this time they were noticed to be directed both to the servers and the servers routers, which affected and reduced the network capacity of the region with about 70% [46].

Mirkovic et al. [38] continues that in February the attacks began to aim towards commercial sites where a lot of traffic and many users were assumed to be located at. But it was not only commercial sites that got attacked during this time, even American authorities' web sites, such as FBI's web site, was down for about three hours. In 2001 the network capacity among attackers began to increase gradually and took form as domain name system (DNS) attacks. Forged domain name system requests were invoked to several domain name servers that resulted in a large amount of traffic against what seemed to be the requester, but actually was the victim.

During 2003, distributed denial of service attacks started to be combined with worm events (form of malware), where the worm was spreading itself to infect computers and put them into botnets, as the purpose was to control the possibility to spread unwanted information, so called spam. During the war between America and Iraq the same year, this phenomenon was utilized in order to spread American arguments for the actions via non-American sites, e.g. Al-Jazeera (Arabic news channel); when visiting the web site users were welcomed by texts with arguments for invading Iraq. Since then, this phenomenon has mainly been a method to attack a victim because of financial motives as an example. Later on, during 2004, financial motives continued to be the reasons of the attacks. Those took place as worm attacks, where the possibility to infect thousands of hosts with malicious software was made. Those hosts were contaminated by using trojan horses in different programs fooling users to install the worms, which created a botnet. A botnet (see chapter 2.2.3) is a network where computers can be remotely controlled by perpetrators, and in some cases sold as service in the black market.

A reason for illegally selling a botnet on the black market is that minorities with enough money can rapidly become a majority in form of number of hosts that can attack a specific victim. An example of a multi-sourced attack is the attack that occurs by having a large number of hosts that instantly invokes a server or a network at the same time. This kind of attack is known as a distributed denial of service attack, and has the purpose to e.g. overload a cryptographical calculation at the server side to achieve a denial of service. Mirkovic et al. ends by explaining that an overload in this kind of services can rapidly become very expensive if they are misused.

2.3.1.2 Distributed denial of service

Distributed denial of service attacks is what is known as a multi-sourced attack, possible to do due to distributed computing [38, 42]. For an attack to be called a distributed denial of service attack is that computers must be involved in a botnet, which can be done by contaminating computers with malicious software that are brought together into a network (illustrated in Figure 3, where agents represents the infected computers, also known as zombies), making it possible to attack any victim on a single command [41]. Note that attackers rarely want to be seen, they are therefore often hidden behind handlers [38] that "distributes" the commands of the attacker.

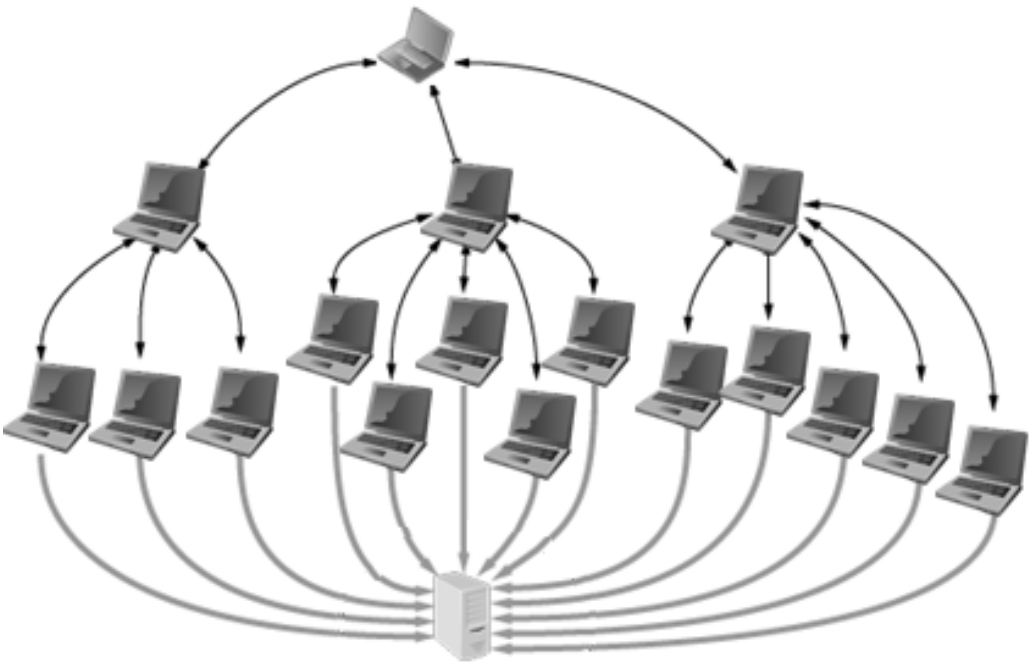


Figure 3. Handler and zombie architecture.

Distributed denial of service attacks that aims towards bandwidth with the purpose to create congestion in data traffic are categorized as volumetric attacks, which is the most commonly used category (61% of the cases) [47]. Further it is defined that attacks toward high-capacity devices that can maintain over millions of connections through e.g. a firewall, is categorized as a TCP state-exhaustion attack.

The third category that exists within distributed denial of service attacks is the so called application layer attack that aims toward safer systems, that could have existing defence mechanisms against commonly used attacks such as volumetric attacks, which requires more advanced and skilled methods. Application-layer attacks occurs via top layers (application layer, layer 7) in the OSI model [47], examples of such attacks are the Slowloris attack [48] and R-U-Dead-Yet attacks, also known as Rudy attacks [49].

Slowloris attacks aims to take down web servers by sending incomplete and divided handshake packets, forcing the server to request for the rest of the packet, which may be sent afterwards or not sent at all. Slowloris uses this technique several times in the same connection such that the maximum allowed processes for handshaking new connections is reached. Since new users will have to wait for the previous processes to end, this will generate a denial of service for legitimate users [50].

A similar technique used in application layer attacks is the R-U-Dead-Yet attack that sends a complete header packet, unlike Slowloris, fooling the web server to start further processes. The rest of the data packets are sent in smaller bits to extend the arrival time and in that way sustain the connection to the server, denying services for legitimate users. Some old tools used for attacks are mentioned in Table 3 and some modern tools used nowadays are mentioned in Table 4.

An application layer attack requires less network capacity [51] than other methods to make damage. The attacks are difficult to detect as they do not invoke with the same amount of data as traditional distributed denial of service attacks, it may therefore look like any ordinary data traffic.

Table 3. Enabling tools for distributed denial of service attacks, compilation of [52, 53].

Name	Description
Mstream	A powerful stream attack; sending TCP ACK packets by using random ports, randomizes 32 bits of the source IP address.
Omega	Attacks by TCP ACK packet flooding, UDP packet flooding, ICMP flooding, IGMP packet flooding and also a mix of these four floods. Randomizes 32 bit (like Mstream) but includes chat function allowing multiple attackers to communicate.
Plague	Similar to Omega. Attacks using TCP ACK and TCP SYN flooding tools.
Stacheldraht	Works incognito; communication by hidden channels (ICMP) and encprytion on the network. Provides ICMP flood, UDP flood, SYN flood and smurf attacks via TCP and ICMP connections.
Tribe Flood Network (TFN)	Similar to Stacheldraht. Performs attacks such as, UDP flood, ICMP flood, TCP SYN flood attacks and smurf attacks via ICMP connection. A later version is called TFN2K, which has additional features, e.g. encryption and ability to send shell commands.
Trinity	Used as SPAM distributor, redirects Internet Explorer Search queries and modifies the start page.
Trinoo (Trin00)	Generate attacks such as, UDP floods, TCP SYN flood, ICMP echo request flood and smurf attacks via TCP connection. Has the ability to generate spoofed source IP addresses.

Table 4. Modern tools for distributed denial of service attacks, compilation of [54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64].

Name	Description
Anonymous-DoS	A HTTP flood program written i HTML Application (HTA) and javascript which flood a chosen web server with HTTP connections.
DAVOSET	Uses the vulnerabilities in the HTTP on several sites to be able to attack other sites. The latest version is v.1.1.7 from February 2014.
DDOSIM	Simulates a zombie network, having random IP addresses. Supports both HTTP DDoS with valid requests, but also invalid requests, and SMTP DDoS. Supports TCP connection flood on random port. Aimed to be used locally for testing.
Dereil	Attacks via TCP, UDP and HTTP protocols.
HOIC (High Orbit Ion Cannon)	A program able to cause DoS by using HTTP floods, but has a built-in scripting system that can amplify the attack as additional feature.
Hive Mind LOIC (Low Orbit Ion Cannon)	A updated version of LOIC from April 2013, that aims to stress test servers against DDoS attacks, control bots via IRC channels, and as additional feature to control RSS servers.
Moihack Port-Flooder	A tool from 2012 to stress test network devices and measure routers or servers load. The program is a simple port flooder.
PyLoris	Utilizes SOCKS proxies and SSL connections to target protocols such as HTTP, FTP, SMTP, IMAP and Telnet to test a servers vulnerability to connection exhaustion attacks.
Tor Hammer	Runs within the Tor Network that allows attackers to be anonymized. The tool uses a SLOW POST request to the target and supports slow networks.
SSL-DOS	Exploits vulnerabilities in the Secure Sockets Layer (SSL) renegotiation protocol by sending multiple requests for secure connections, which requires 15x more processing power on the server than on the client. SSL renegotiation allows web sites to create a new security key over an already established SSL connection.
XOIC (X Orbit Ion Canon)	An updated and more powerful tool comparing to other Orbit Ion Cannon tools, supported on Windows 7 and 8. The attacker can choose different modes depending on the purpose; either requesting counter and TCP, HTTP, UDP and ICMP messages or skipping it for better performance.

2.3.2 Statistics on distributed denial of service attacks

This section includes statistical values over the past years regarding the network capacity within an attack. It also includes the dispersion rate of computers that become infected and the theory of combining these infected computers and the networks capacities that are constantly increasing.

There are several organizations, both from private and public sectors, which collects information regarding the amount of network traffic and behaviours in the traffic [65]. Some of the organizations choose to dive deeper into specific cyberattacks, to be able to give a more detailed description. These organizations analyse, for instance the development of the attacks on a global scale and states e.g. the most common motives of an attack. The outcome of such reports offers information of the current situation and gives a hint of how it could be further developed. Organizations that works with these kind of analysis are, according to the European Union Agency for Network and Information Security (ENISA) [65], e.g. Prolexic [66], Computer Emergency Response Team [44], Arbor Networks [67] and Akamai [68].

2.3.2.1 Sizes and types of cyberattacks

As mentioned earlier (section 2.3.1.2), large-scale distributed denial of service attacks were first seen in late 1999. According to Mirkovic et al [38], some of the first large-scale attacks were registered to be in a size of 60 Mbit/s to 90 Mbit/s. A year later, in 2002, serious measurements began to be registered [69] giving a statistical histogram of a typical size of a distributed denial of service attack. An overview of the largest registered size of an attack, starting from 2002, is illustrated in Figure 4, showing that the largest size of reported attacks reached 309 Gbit/s in 2013 while the second largest reached 100 Gbit/s in 2010.

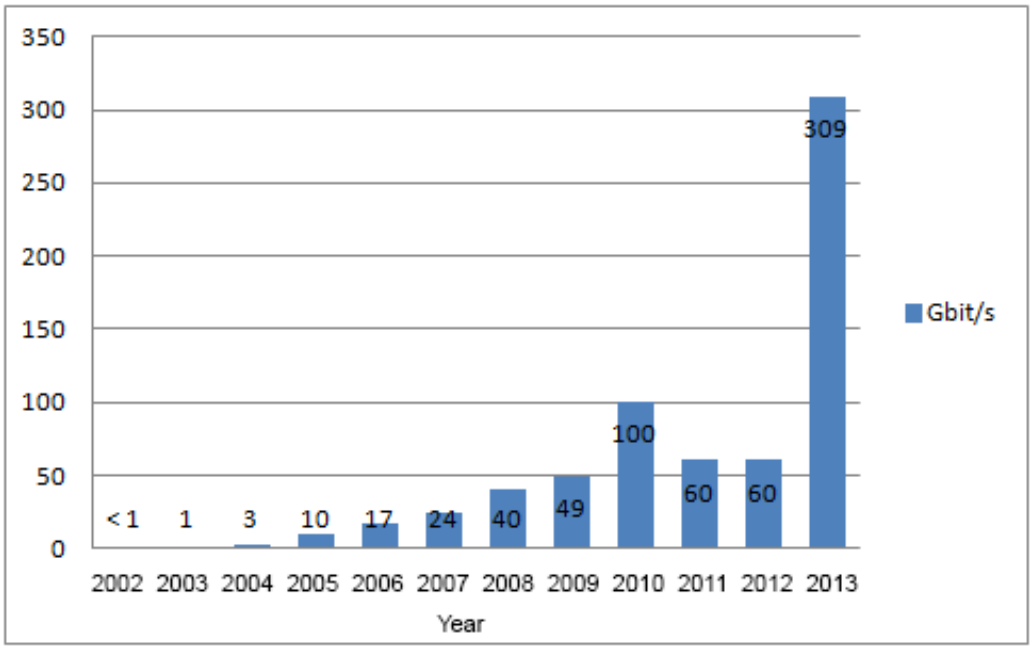


Figure 4. Size of largest reported DDoS attack.

It is however important to know the size of the average attacks and not only the size of the largest attack that has been registered. Studies [70, 71, 72, 73, 74, 75] that was made from late 2011 to the end of 2012 showed that the average attack bandwidth increased from 2.1 Gbit/s to 5.9 Gbit/s. In the first two quarters of 2013 there were some changes in the attack strategy [76, 77], where both Internet service providers and carrier router infrastructures were targeted. In that case the average attack bandwidth increased with 718 percentage points from previous quarter to an average attack bandwidth of 48.25 Gbit/s in the first quarter and another 2 percentage points, to an average attack speed of 49.24 Gbit/s in the second quarter of 2013 (see Figure 5). In quarter 3 of 2013, a decision [78] was made of using peak rates to measure the size and intensity of distributed denial of service attacks instead of average attack bandwidth. Peak rates are considered to be a better way of measuring network capacities.

By using peak rates as measurement, the average size of an attack in quarter 3 of 2013 was 3.06 Gbit/s, while the average size of an attack in quarter 4 of 2013 was 4.53 Gbit/s, meaning an increase of 48.04 percent. The statistical numbers from quarter 3 of 2011 to quarter 4 of 2013 are presented in Table 5.

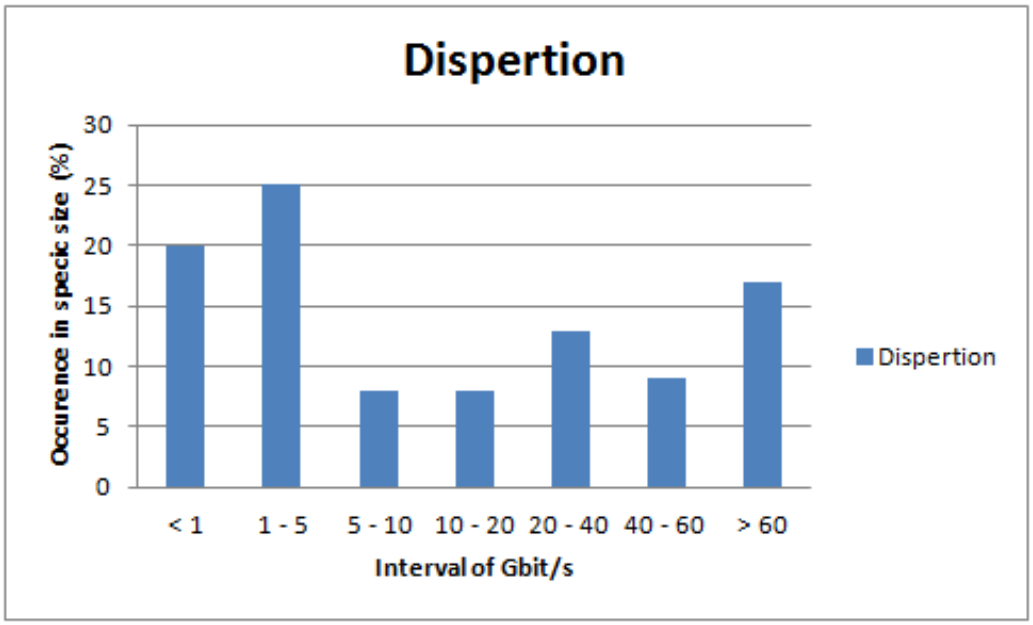


Figure 5. Average Gbit/s in quarter 2 of 2013.

Table 5. Compilation of average attack speed or peak rate, compilation of [70, 71, 72, 73, 74, 75, 76, 77, 78, 79].

Year	Quarter	Average attack speed or peak rate (Gbit/s)	Percentage of increasing (%)
2011	3	2.1	
2011	4	5.2	147.6
2012	1	6.1	17.3
2012	2	4.4	-28
2012	3	4.9	11.4
2012	4	5.9	20.4
2013	1	48.25	718
2013	2	49.24	2
2013	3	3.06	
2013	4	4.53	48.04

The duration of the largest distributed denial of service attacks are divided into different time intervals. The majority of the attacks, in 48 percent of the cases, the duration of the largest registration lasted between some minutes up to six hours, while 15 percent lasted between one to three days [69]. The duration of several weeks occurred only in 6 percent of the cases, and for a month only in 5 percent. Details of the average duration of the largest registered attacks are illustrated in Figure 6.

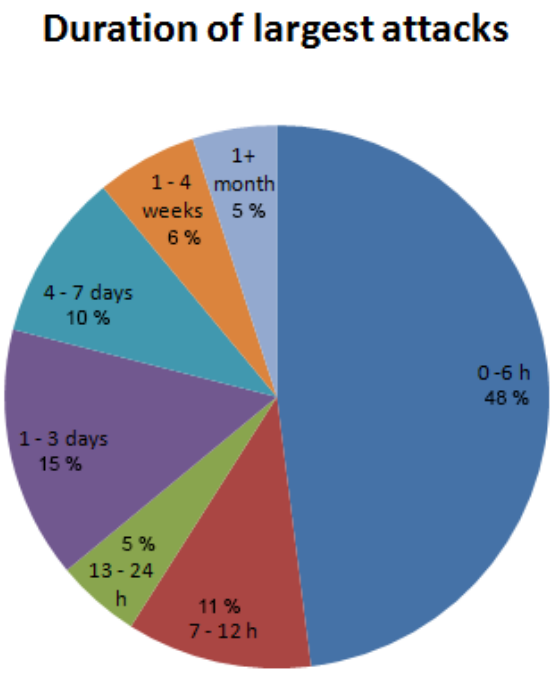


Figure 6. Duration of largest DDoS attack.

The average duration of each attack during 2013 was in the first two quarters over 30 hours, and where minimized to around 20 hours in the last two quarters [76, 77, 78, 79], due to the fact that distributed denial of service attacks became more efficient [79] and thereby less time consuming.

Different types of distributed denial of service attacks have been discovered over the past years. An overview of the most common types of attacks that occurred during 2011 and early 2012 is presented in Table 6. In the second quarter of 2012 some additions were made to the list of common types of attacks. Distribution of flood attacks in different protocols, from second quarter of 2012 until the end of 2013 is presented in Table 7.

The flood attacks in Table 6 represents different layer attacks in the OSI model [80], in layer 3 (network layer) and 4 (transport layer), but also in layer 7 (application layer). The total percentage of attacks in layer 7 is presented in Table 8.

As long as computer capacities are increasing, the evolution of distributed denial of service attacks are expected to continue evolving [76], since the concept of distributed computing depends on having networks of multiple hosts. The concept is explained in next section.

Table 6. Flood attacks in different protocols, in percent (%), from late 2011 to early 2012, compilation of [70, 71, 72].

	ACK	DNS	GET	ICMP	POST	PUSH	RESET	SSL GET	SSL POST	SYN	SYN PUSH	UDP	UDP Fragment
Q3(2011)	1.55	1.55	14.73	22.48	0	1.94	4.26	0	0	24.42	0	9.69	19.38
Q4(2011)	1.15	2.49	16.28	21.84	2.11	1.92	3.07	0.57	0	19.54	0	20.11	10.92
Q1(2012)	0.58	2.50	20.42	19.65	2.12	2.50	2.31	0.58	0.96	24.66	0.58	15.41	7.71

Table 7. Flood attacks in different protocols, in percent (%), from second quarter of 2012 to late 2013, compilation of [73, 74, 75, 76, 77, 78, 79].

	Q2 (2012)	Q3 (2012)	Q4 (2012)	Q1 (2013)	Q2 (2013)	Q3 (2013)	Q4 (2013)
ACK	2.47	1.43	0.48	1.74	0.53	1.69	2.81
CHARGEN	0	0	0	0	0	3.37	6.39
DNS	1.76	4.92	4.67	6.97	7.25	8.94	9.58
FIN PUSH	0	0.41	0	0.32	0	0.39	1.28
HEAD	0	0	0	0	0.13	0.13	0.64
HTTP GET	14.81	13.50	20.61	19.33	21.48	18.03	19.91
HTTP POST	1.94	3.07	3.22	1.43	2.50	3.37	1.53
ICMP	17.28	17.79	18.04	15.53	15.15	11.41	9.71
IGMP	0.18	0.20	0	0	0	0	0
NTP	0.18	0.20	0	0	0	0	0.26
PUSH	1.76	1.02	0.32	0.95	0.39	0.91	0.77
RESET	1.94	2.86	2.90	1.43	1.19	1.94	1.40
RIP	0	1.02	0	0	0	0.13	0
RP	0	0	0	0	0	0.39	0.26
SSL GET	0.18	0.61	0.64	1.43	0.53	0.78	0
SSL POST	0.18	0.20	0.16	0.32	0.26	0.26	0.13
SYN	26.63	23.53	24.0	25.83	31.22	18.16	14.56
SYN PUSH	0	0.41	0.48	0.63	0	0.13	0.38
TCP Fragment	0.18	0.20	0.32	0	0.26	0.65	0.13
UDP	23.10	19.63	15.46	16.32	10.41	14.66	13.15
UDP Fragment	7.41	9.00	8.70	7.77	8.70	14.66	17.11

Table 8. Total percentage (%), of Application Layer attacks (Layer 7), compilation of [73, 74, 75, 76, 77, 78, 79].

Q2 (2012)	Q3 (2012)	Q4 (2012)	Q1 (2013)	Q2 (2013)	Q3 (2012)	Q4 (2012)
19.05	18.60	24.95	23.46	25.29	23.48	23.24

2.3.3 How a botnet is built

The following section gives an overview on how a computer gets recruited into a botnet.

2.3.3.1 Dispersion of computer infection

There are great numbers of Internet users in the world and many of them have no secure system for their Internet usage [51], which is a vulnerability an attacker can use to execute a distributed denial of service attack. Attackers can use vulnerabilities in computers to infect them and gain total control for further usage of those computers. To be able to convert a computer to a zombie, the attackers installs a bot, a software with malicious code [81] via e.g. an e-mail attachment, infected Web site or by other procedures, without the owners knowledge [82]. When a computer is infected, the bot is preconfigured to connect to a control server, e.g. Internet relay chat server, and the server, owned by the attacker, is able to control that infected computer. The attacking user of the botnet can thereby launch e.g. a distributed denial of service attack by commanding the infected computers to overload their victims. The concept is that the attackers sends malicious software instantaneously to several computers and infects computers with vulnerabilities in their security systems [51], and also to contaminate more computers through the existing computers in the botnet.

2.3.3.2 Infected computers as a network

Groups that owns botnets has managed to generate incomes out of this, since the maintenance of such network is relatively of a low cost, and does not require a high level of knowledge.

According to a study of the economics of botnets [83], the income of a botnet is based on the ability to infect new computers and keep them protected from being discovered by antivirus software and located by authorities, which requires a lot of effort. That is why it is easier for a user to lease or buy a botnet than actually making the infection themselves. The lease of e.g. a mail botnet that meet certain requirements can generate an income of $2 000 each month. The actual amount depends on the number of zombies within the network, which is why a small botnet, with some hundreds of zombies, is calculated to generate an income of $200-700 each month. This gives the average cost of a botnet to be $0.50 per zombie.

A larger network has been registered to cost $36 000, having 100 000 zombies. It is very difficult to count all functional botnets on the Internet, but in fact there are many botnets that has over 3 600 zombie computers within the network. Note that it is not only private computers that gets infected and involved in a botnet, there are also computers in corporations, government offices and also military workstations [84] that has been included into botnets. The risk of getting infected arises since all computers are connected to the same Internet.

There are indications, in the same study [51], of aggregated traffic from 10 Gbit/s to 100 Gbit/s in botnets with over 100 000 zombie computers. If each zombie would send a full-sized packet per second (pps), which means 1 500 bytes or 12 000 bits per second, the aggregated traffic would then generate at least 120 Gbit/s in a botnet with 10 000 000 zombies. This kind of capacity could theoretically take down almost any server on the Internet [85].

2.3.3.3 Computers as weapons

Unprotected computers tend to compromise the operating system risking getting unwanted software installed. There are potentially over 2 billion computers with an Internet connection around the world, according to the Internet World Stats [86], that theoretically could be included in a botnet and thereby be used as weapons against intended victims (often referring to servers, but could also be referred to computers of private users). The amount of computers in Sweden exceeds 7 million [84], where every single one of them could be infected and included in a botnet within Swedish borders. McGregory claims [51] that McAfee [88] reported that during the end of 2012, 22 million new computers were contaminated, which is an average contamination rate of 300 000 computers every day.

In July 2013 the Code Red worm took advantage of vulnerabilities in the Microsoft Internet Information Service (IIS), and by that giving a great interruption on the Internet traffic. According to the computer emergency response team [89], the worm had infected around 26 000 computers per hour around the world. If the intention with this attack were to recruit zombies, the attacker would have created a botnet with over 350 000 zombie computers in only 14 hours [90].

The Swedish national computer emergency response team (CERT-SE) [91], established by the Swedish Civil Contingencies Agency, collects information of contaminated computers within Swedish borders [92], sorting them out to identify whether they belong to Swedish government authorities, municipalities or other public organizations. The latest compilation [93], registered during the beginning of February to the beginning of March of 2014, shows that 49 286 computers were infected at that moment. According to the Internet World Stats [86] Sweden, as part of Europe, has more precisely around 8 500 000 users on the Internet, and reports shows that the next types of attack tends to be performed by using smartphones as they become more widespread worldwide [79, 94].

2.4 Prediction by statistics

Powerful computers started to appear in the beginning of 2000 [6] and it was then attacks started to be performed from computers with higher clock rates. Higher clock rate generated higher calculation speed which is a requirement to generate unwanted data that is sent. More powerful attack was not so likely until after 2000 [38]. The statistics of today shows that it is possible to generate data with a capacity up to 300 Gbit/s [69].

2.4.1 Moore´s law

Moore's law [6] was founded around 1970 with the purpose to claim that the processing power of computers would double every two years. What it really meant was that the number of transistors would double every two years. It is important to distinguish the development of transistors and the processor capacity. During 1970 the capacities varied from 740 kHz to 8 MHz and during 2000 - 2009 it varied from 1.3 to 2.8 GHz. This means that the capacities had barely doubled within a period of ten years, which is not according to Moore's law since this does not apply to processor capacities. During 2000 the total number of transistors in the CPU was 37.5 million while in 2009 the number of transistors had reached 904 million. The law applies on transistors rather than capacities, but makes it possible to predict how the future of processor capacities could look like as guidance, which is valuable. A histogram of the development from 1997 until 2012 [95] is illustrated in Figure 7.

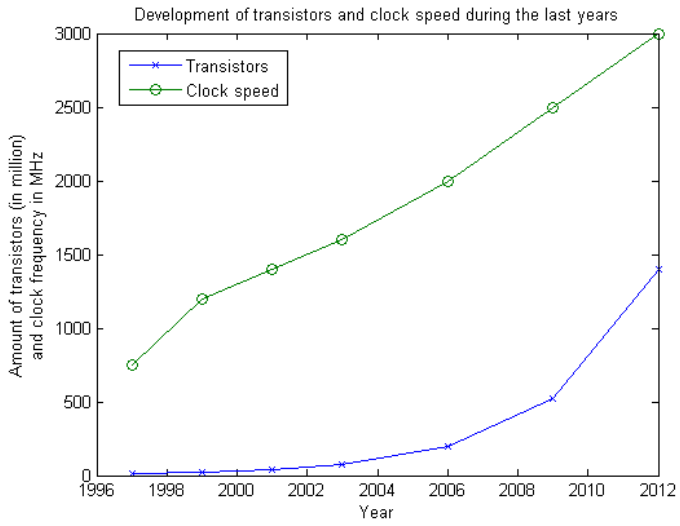


Figure 7. Roadmap for transistors and clock speed.

2.4.2 Development of Internet service providers in Sweden

The Swedish Internet Infrastructure Foundation, .SE, acts for a better development of the Internet environment in Sweden [96]. Within this foundation there is a service called "Bredbandskollen" [97] that offers measurements among Swedish users regarding the actual internet bandwidth.

A report [98] compiles the Internet usage and bandwidth from several Swedish Internet service providers. This report includes different Internet connection types, such as fiber, cable, 3G and LTE etc. Fiber and cable are two types of Internet connections that are used in regular households, while 3G and LTE are wireless portable Internet connections, where 3G has a maximum speed of 2 Mbit/s [99] and LTE has a maximum speed of 100 Mbit/s [100]. The difference between fiber and cable is that fiber is more expensive than copper cable but it covers longer distances without losing any strength in the signal, in comparison to copper cable that needs to be amplified [101].

The same report [98] shows both average upload bandwidth and average download bandwidth from different Internet service providers. Note that only fiber and cable bandwidth are presented in Table 9 (for upload) and Table 10 (for download). Full description can be found in Appendix B.

Table 9. Average upload speed history from 2008 – 2013 in Mbit/s, compilation: [98].

ISP	Type	2008	2009	2010	2011	2012	2013
AllTele	Fiber	12.9	25.6	30.7	29.3	31.1	31.9
AllTele	Cable	n/a	n/a	n/a	9.8	10.7	10.4
Bahnhof	Fiber	23.9	26.2	26.5	27.1	28.4	33.0
Bahnhof	Cable	n/a	14.7	13.7	10.1	12.9	14.3
Bredband2	Fiber	n/a	n/a	27.4	27.2	27.7	36.2
Bredband2	Cable	n/a	n/a	14.3	6.9	11.0	22.1
Bredbandsbolaget	Fiber	13.9	15.2	14.6	13.9	17.2	25.0
Bredbandsbolaget	Cable	6.3	6.8	2.5	n/a	n/a	n/a
Com Hem	Fiber	2.4	5.5	7.2	n/a	11.0	16.1
Com Hem	Cable	2.8	5.1	5.2	5.9	6.8	8.5
Tele2	Fiber	n/a	13.0	15.1	16.7	18.9	20.9
Tele2	Cable	n/a	2.1	5.8	6.6	6.9	8.8
TeliaSonera	Fiber	11.7	16.0	15.6	15.3	19.7	28.7
TeliaSonera	Cable	2.4	4.2	2.3	6.4	8.3	10.9

Table 10. Average download speed history from 2008 – 2013 in Mbit/s, compilation: [98].

ISP	Type	2008	2009	2010	2011	2012	2013
AllTele	Fiber	22.9	36.7	43.2	46.0	45.6	47.3
AllTele	Cable	n/a	n/a	n/a	23.0	25.1	27.5
Bahnhof	Fiber	40.4	45.4	47.5	48.4	52.8	59.7
Bredband2	Fiber	n/a	n/a	47.9	45.2	46.2	55.4
Bredbandsbolaget	Fiber	43.2	52.3	54.4	53.9	54.9	65.7
Bredbandsbolaget	Cable	20.6	23.7	15.4	n/a	n/a	n/a
Com Hem	Fiber	13.8	36.4	50.4	n/a	41.1	47.6
Com Hem	Cable	13.1	23.6	35.3	40.9	42.3	52.5
Tele2	Fiber	n/a	38.0	43.0	49.0	48.0	49.0
Tele2	Cable	n/a	7.7	28.0	36.0	33.0	41.3
TeliaSonera	Fiber	27.0	36.7	39.2	41.6	45.5	52.8
TeliaSonera	Cable	7.2	10.3	14.1	17.0	20.0	25.3

2.5 Criminal minds

Researchers from the Georgia Institute of Technology [102] claims that distributed denial of service attacks is one of the attacks that belong to the never-ending threats and they also claim that it is a preferred technique used by many attackers worldwide [103]. This section describes some possible motivations and reasons behind distributed denial of service attacks.

During the years, the motivations behind the attacks have been changing from e.g. practical jokes to political statements [103]. As mentioned in the history of denial of service attacks (see chapter 2.3.1.1) it started as practical jokes or to just make statements and has lately developed to business services, which has involved many people making the motivations more diverse.

A modern attack allows both experienced and inexperienced users to participate, since they are performed by fully developed tools and methodologies. Everything that is needed to perform an attack is served, for free, online on the Internet (see chapter 2.3.1.2). That is why the question is not how computer users are able to perform such an attack anymore, it is rather why.

According to a study by Ollmann [103] there are mainly three different kinds of attackers. The first category of attackers is called Professionals, which are the users that are the actual criminals that generate financial profit by developing and providing these tools to lease or extortion. The second category is called Gamerz, which are typically over the average when it comes to technical understanding. Gamerz are difficult to generally categorize, since they could be either misguided or malicious teenagers, operators or creators of distributed denial of service attack tools. Gamerz are known to use smaller botnets, and in some cases organize themselves into a bigger botnet by combining their own botnets. The third and last category are the so called Opt-in, which are computer users with or without advanced technical knowledge that accepts and in many cases gives permissions to be included in a botnet as agents, by converting their computers to zombies. Opt-in attackers are often involved because of protest movements with different causes as reasons.

Since the motivations of the attacks can be many, the same study [103] defines the most common objectives of successfully accomplishing a distributed denial of service attack, there are:

- Espionage – "business or curiosity".
- Extortion – "'pay to live' or simply to show control and power".
- Nuisance – "just because they can or to temporary make a statement".
- Protesting – "to make difference or simply operate a campaign".

Independent of the motivations behind an attack, the Internet became a place of conflicts as soon as it gained visitors on cyberspace [38], since the risk to get into disagreements and conflicts increases.

According to Mirkovic et al [104], there are some studies showing that people can behave differently in real life comparing to online. Antisocial people can suddenly express themselves very well behind a computer, when not facing the counterpart. This tends to lead to expression with no limitations, where Internet users in some cases bully other people, a phenomenon called trolling. The term troll defines people, often associated as sadists that are searching for attention, revenge, pleasure or to simply damage social communities due to boredom.

Due to the mix of personalities on Internet-based communities, where the real identity of a person or user is unknown, it tends to generate a higher self-confidence in an attack toward victims of higher values such as a state. Those attacks can become more significant in the future, if they are performed by groups with powerful resources and great knowledge [38]. Groups with these skills are known as nation-state actors, and could be one of the most dangerous groups of attackers.

2.6 Security standards

The Swedish Civil Contingencies Agency has developed a framework as support for information security [105] that has the purpose to support all types of organizations that are willing to establish and implement an information security management system, and by that use the international standards of the ISO 27000 series (see next section). This methodological support is designed to facilitate and support the work with information security in both public and private sectors, for establishing and maintain a justified confidence in the functioning of a society.

The Swedish National Computer Emergency Response Team has also developed an incident management process [106] that is mainly for their internal incident management processes, but the process is also accessible for other organizations. The process involves the steps: identify, limit and prevent.

In order to achieve a system as secure as possible, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have established guidelines to support the development of such a system, described in next sections.

2.6.1 ISO/IEC 27000 as support

ISO/IEC 27000 [107] consists of a few security standards that goes under the international title; “Information technology - Security techniques - Information security management systems - Overview and vocabulary”.

The purpose of this standard is to provide an overview and introduction of ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards. Information security management systems consist of e.g. policies, procedures, related resources and activities that protects the information assets. The Information security management system is an aid to establish, monitor, review and improve the information security of organizations. By analysing the requirements imposed for protection of their information assets and applying appropriate controls, it contributes to a successful implementation of information security management systems. ISO/IEC 27000 and the security standards explain thoroughly everything that is necessary to achieve successful implementation.

2.6.2 ISO 31000 as support

ISO 31000 [108] focuses on risk management - principles and guidelines; how an organization should manage risks in their governance, strategy and planning, management, reporting, processes, strategies, valuations and culture. The standard is a guidance for the development, implementation and to improve risk management in these various processes. The standard uses two different concepts that are linked to each other; risk management that involves the architecture (principles and processes) to manage risks on an effective way, and managing risks that is the application of the architecture on a particular risk. In some cases an organization has already adopted a risk management process and can thereby use this standard as an evaluation tool on their existing process.

2.7 Risk management

This section describes the terminology for vulnerabilities and risk analysis. It also includes how risk analyses are performed and used.

2.7.1 Risk analysis

The purpose with this section is to give an overview about risk analysis regarding information security [109]. Risk analysis is a wide spread field and can be applied in different kinds of situations. When talking about information security it is important to protect the organisations information assets, and risk analysis is a helping aid for adapting the correct protection. Risk analysis is also a helping aid [110] in the compilation of an information security policy for an organization. Labuschagne and Badenhorst have summarized risk analysis within information security as following:

- Risk analysis is a necessity, both in the development of an information security policy and in defining a security plan for implementation.
- Business risks tend to be an important factor by senior management and by introducing a risk analysis, it can get the senior management more involved in information risk management.
- The most important outcome of a risk analysis is to identify measures for identified threats.
- Risk analysis can provide information needed to perform a cost-benefit evaluation practice for information security program.

To help Swedish organizations with their risk analysis, the Swedish Civil Contingencies Agency has created a document [109] that is proven and based on foundations from the Swedish national police and also fulfils the requirement seen in ISO/IEC 27000. Figure 8 describes the assignments that need to be performed during a risk analysis.

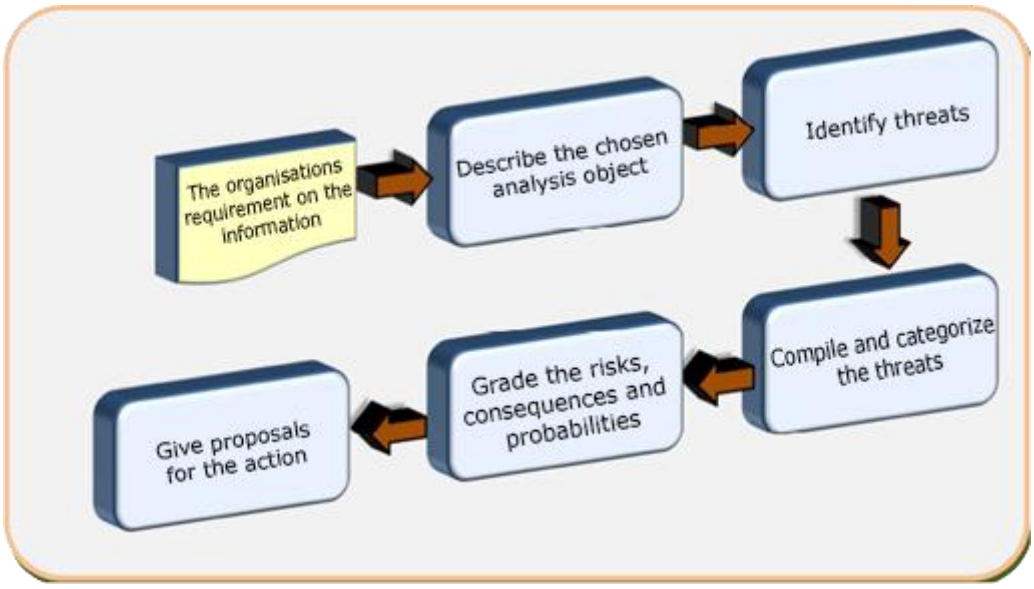


Figure 8. Assignments during a risk analysis.

The first step is to select and describe the analysis object. The analysed objects are selected from the organizations information assets. It is important that the assets are described in detail so it is clear what should be included in the analysis and not. Often it is not possible to analyse all the assets and thereby chose the assets that are the most critical for the organization or are by other reasons extra important to analyse. This assignment is ready when the analysed objects are chosen and described, the limits are documented and the entire group has agreed on what is going to be analysed. The next step is for the group to brainstorm about the threats against the analysed objects. To help the group, two questions can be asked: "what are the threats against the information assets?" and "what can happen?".

After this assignment, all potential threats against each chosen analysed objects should be documented and every threats is clearly documented and put in its context. The next step is to sort and group similar threats with each other, removing duplicates and clarifies the threats if necessary. The assignment is ready when the group has a number of threats that are clearly described and written down.

The next step is assessing the risk, consequence and likelihood. Every threat will first be evaluated and then located in a consequence- and likelihood matrix. Having this matrix, it is possible to evaluate the risk for each threat. The result of the matrix will give the opportunity to e.g. prioritize of different measures.

The likelihood is about how likely it is that the threat will occur and the consequence is how the organization will be affected if the threat becomes real. Figure 9 is an example of a consequence- and likelihood matrix with threats located in different areas.

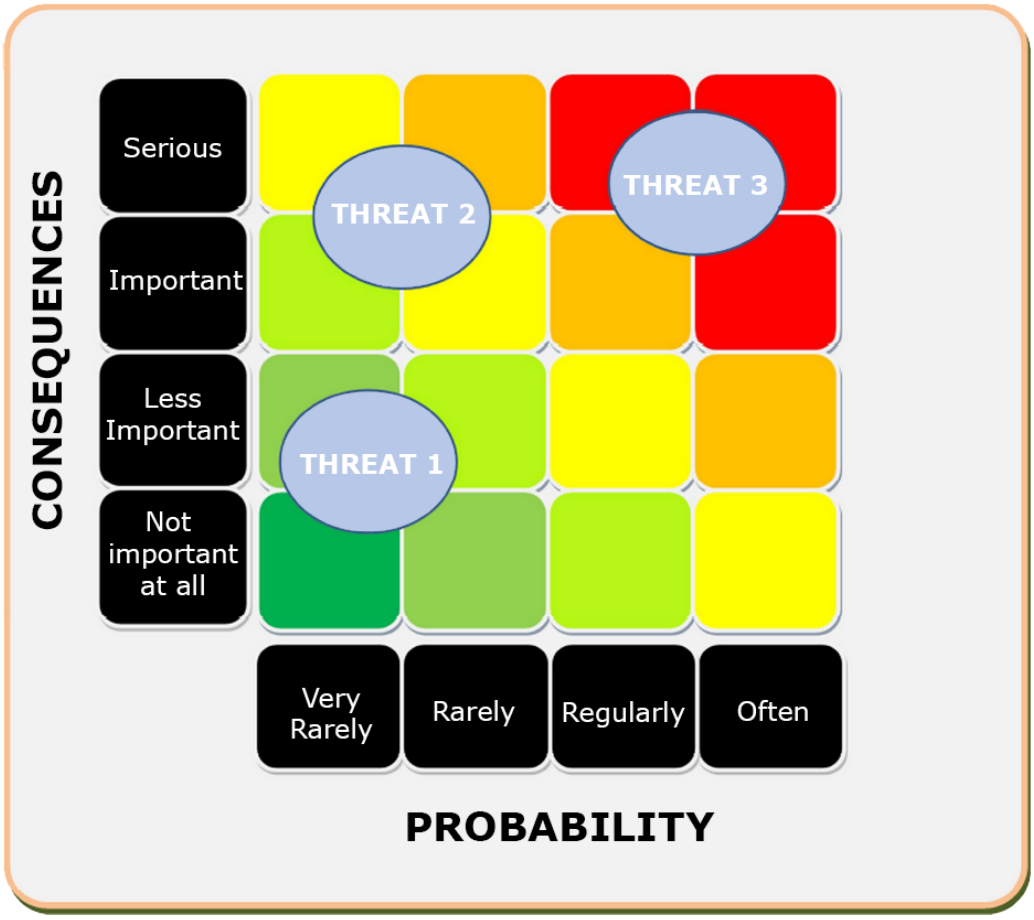


Figure 9. Consequence- and likelihood matrix.

This assignment is ready when it is possible to overview the risks, the consequences if the risks becomes reality and how likely it is to happen. The result should also be visualized in a consequence- and likelihood matrix. The last step is about going through the identified risks and come up with suggestions about how they should be handled. One alternative is if the risks can be handled later but if the risk has great likelihood and great consequences it is important to treat the risk immediately as it can involve critical risks for the organization. When this assignment is done there should be some suggestions for measurements and recommendations.

2.7.2 Risk assessment

Risk assessment [111] is used in order to determine what threats exist to a specific asset and the risk levels. The risk levels helps the organization to prioritize the threats and thereby select appropriate controls measures, safeguards or countermeasures to minimize the risk to an acceptable level. The risk assessment process can be divided into six steps: asset definition, threat identification, determine probability of occurrence, determine the impact of the threat, controls recommended and documentation.

It is important that in the beginning define the process, application, system or asset that is under review, and also to establish the boundaries of that is to be reviewed. It is a common problem that projects fail because the boundaries were to poorly define. The next step is to identify the threats. Threats are undesirable events that could harm the asset that is under review. There are three major categories of threat sources:

- Natural threats – floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- Human threats – events that are either enabled by or caused by human beings, such as unintentional acts or deliberate acts.
- Environmental threats – long term power outages, pollution, chemical spills, and liquid leakage.

One method to create a list of threats is to create checklists and another method is by examining historical data. Having historical data it is possible to see which events that have occurred and how often. It is also necessary to determine the annual rate of occurrence, ARO. Another method is to brainstorm every threat that comes in mind.

When the threats have been defined, the next step is to determine how likely the threats will occur. The likelihood will indicate the probability that a potential threat may be exercised. The probability can either be high (very likely that the threat will occur within the next year, medium (possible that the threat may occur during the next year) and low (highly unlikely that the threat will occur during the next year). When having the probability it is possible to determine the impact that the threat will have on the organization. The probability and impact creates a matrix (see Figure 10) that generates a risk level that can be assigned to each threat and the organization can identify appropriate actions. The impact can also be high (shutdown of critical business unit that leads to a significant loss of business, corporate image, or profit), medium (short interruption of critical process or system that results in a limited financial loss to a single business unit) and low (interruption with no financial loss). When the risk level has been assigned, it is possible to identify controls or safeguards that could eliminate the risks or at least reduce the risk to an acceptable level. It is important to identify all controls and safeguards and also examine e.g. how effective they are. If the risk level is not reduced using one control, maybe another control needs to be examined. The results of the steps are summarized in Table 11. The last step is to document the result so that the senior management can easily make decisions on policy, procedures, budget and management change.

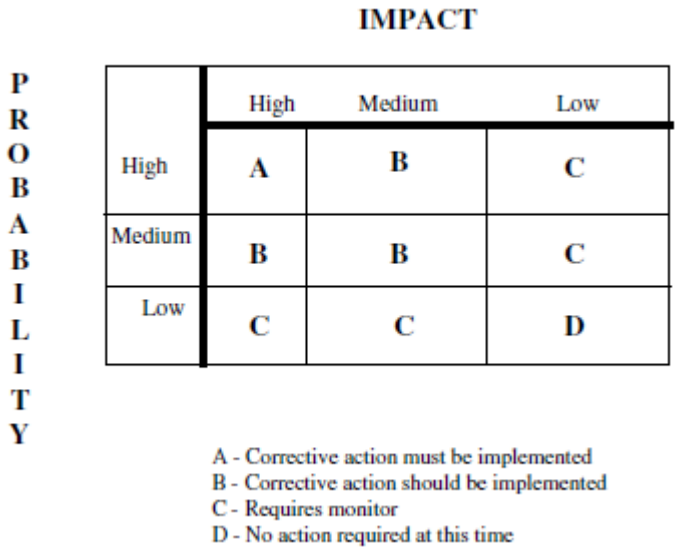


Figure 10. Probability - impact matrix

Table 11. Threats

Threats	Applicable Yes/No	Probability 1=Low 2=Medium 3=High	Impact 1=Low 2=Medium 3=High	Risk Level	Control Selected	New Risk Level

2.7.3 Security risk management

By adapting IT [112] gives a great number of potential risks. Companies that are dependent on IT resource must be prepared on higher risks than companies that are less reliant. Top management teams must gathered and interpret the information from many different internal and external sources in order to ease the analysis from their actions. What the companies want from their security risk management program, SRM, see Figure 11, comes from the risks that might affect the company. Kotulic and Clark claims that flexible organizations are more willing to have an effective SRM program. Another starting point is the conception of fit. Organizations must prevent properties of internal fitting or their processes of organizational structure must be consistent.

It is also important that the organizations have a security policy in order to find the necessary structure which gives a more effective security organization. IT resource posture contains techniques, capacities, assignments and information, and how and why they are being used. The top management team has a great role in the SRM program as they can bring differences in the leading attitudes and views towards security risks that can affect different choices relative to the appropriate security measures that are required. Experienced risk is another important question. Managers can be classified as risk takers or risk avoiders relative to the organization and security risks. Executive management is necessary for a successful implementation of IT. The top management commitment is a requirement for a successful implementation of a SRM program in an organization.

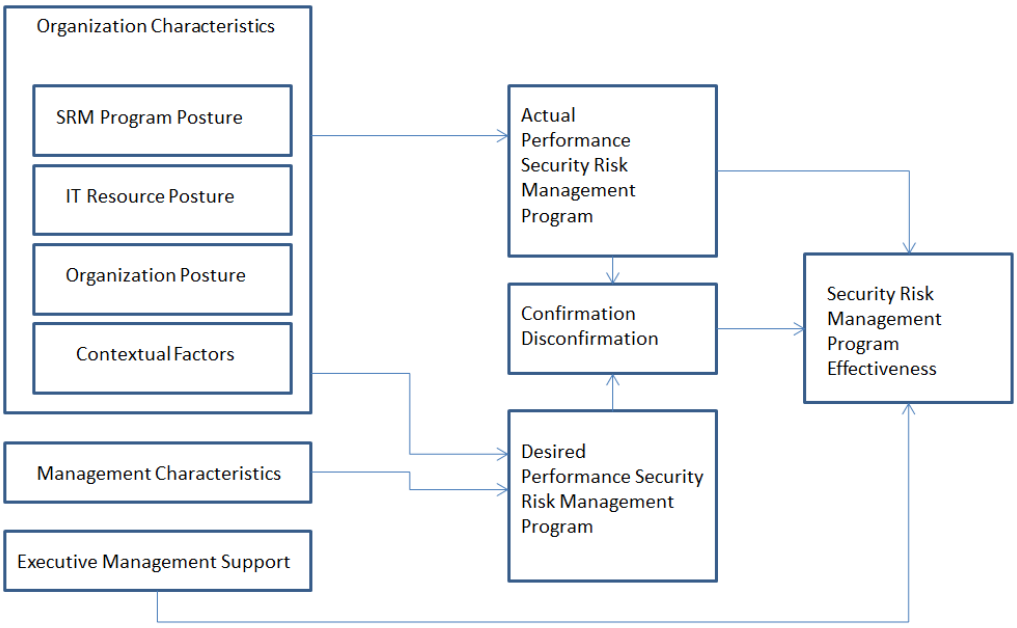


Figure 11- Probability – Security risk management

2.7.4 Cost-benefit approach

The advantages with a security technology depends on how often an attack are expected to occur, how much damage the attack are likely to provide and how effective the security technology are to mitigate the damages from the attack. A cost-benefit analyse [113] can link the communication gap between security managers and IT managers. The IT managers want to know that their investments in security mitigates the risks to an accepted level and the security managers wants to be sure that the chosen design are the most secure. The advantages with a structured cost-benefit analyse are:

- Security managers make their assumptions explicit and capture decision rationale.
- Sensitivity analysis shows how assumptions affect design decisions.
- Design decisions are re-evaluated consistently when assumptions change.
- IT managers see whether investment is consistent with risk expectations.

IT managers are motivated to minimize the security costs but maximize the benefits. Comparing the costs between alternative security architectures is significantly easier than comparing advantages because proven financial analysis can more accurately estimate costs. Benefits are based on uncertain events and incomplete knowledge. No one can predict of often an attack will occur and how effective the chosen security will be. Experienced security managers can intuitive and implicitly estimate the risk and the effectiveness in their risk mitigated strategies. The key to a great security cost-benefit analyses is to make this intuitive real.

Security Attribute Evaluation Method, SAEM, is a cost-benefit analyses process in order to analyse decisions regarding the security design. This process relies on a quantitative risk and benefit assessment where analysts accomplish structured interviews with IT and security managers to produce the original data. Organizations carefully analyse the results of each step before next step. If the result are not useful or does not appear within the managers concern or experience, the managers can change the original data.

The process includes four steps:

- A security technologies benefit assessment.
- An evaluation of the effect of security technologies in mitigating risks.
- A coverage assessment.
- A cost analysis.

The benefit or effectiveness of a security technology is an assessment of how well the technique mitigates a risk. A choice of technique can mitigate risks in two ways: prevent an attack to occur or mitigate the consequences of a successful attack. Security technologies can mitigate the consequences of an attack as security managers can detect an attack which gives them the opportunity to either stop an ongoing attack or identify the damage. Therefore, the security technologies are classified by their effect on the risks. Sometimes the security technologies fails for different reasons which have led to that security expert recommend to use more than one counter measure towards unexpected threats, a principle called defence-in-depth. The National Institute of Standards and Technology recommend security managers to use techniques that contain protection, detection and recovering. What the security managers want in the first place is to stop a threat from succeeding but if a threat gains access to a system it is important to quickly detect the intruder and recover from the damage. By using defence-in-depth it is possible to classify the security technologies based on protection, detection and recovering. After the classification the managers can identify which techniques that mitigate different threats. The difficult part in the benefit analysis is to quantify the effectiveness of the counter measures. This is because during the interview with the security managers, the analyst asks the managers to estimate the effectiveness of each technique for each threat. These estimations are based on the security managers experience of working with these techniques, their judgments of the organizations ability to correct configure and maintain the technique, his expectations on level of competence and motivations of the intruders, and the organizations policies and system design. After this an evaluation can be done of how each security technique mitigates risks. In this step the benefit assessment is applied to the threat frequencies and outcomes to determine how the overall threat index is affected.

There is also another principal that can be adapt, breadth-of-coverage, that means it should exist at least one mitigate strategy for each risk. If there is not a strategy for a threat, the security manager can use another security technology. There are also security techniques based on costs, e.g. purchase, education, maintenance and installation costs. Security costs can require much time but SAEM bring security managers the attention of which technique that gives most benefit.

2.7.5 Risk mitigation

When the threats have been identified, the risk levels established and controls chosen, management can use various risk mitigation techniques [111] to complete the process. There are a few common techniques and it is important when choosing technique to have the business mission in mind.

- Risk assumption – after examining the threats and determining the risk level, it is for the best for the business to accept the potential risk and continue operating.
- Risk alleviation – the management approves the controls that will lower the risk to an acceptable level.
- Risk avoidance – the management chooses to eliminate the process that could cause the risk and thereby be able to avoid the risks.
- Risk limitation – The standard process meaning limiting the risks by implementing controls that minimize the impact of a threat.
- Risk planning – Meaning developing an architecture that prioritizes implements and maintains controls.
- Risk transference – Compensate for a loss, e.g. purchasing an insurance policy.

2.7.6 Financial impact

A breach defines as an ”infraction or violation of a law, obligation, tie, or standard” [114]. A security breach can also be seen as a crime or an infraction of a security policy. In the information security world, a security breach is a violation of an information systems security policy. Example of this is theft, embezzlement or changing in data, unauthorized using of computer services or unauthorized access to passwords or destroying data via computer viruses. Risk assessment is an important component when talking about security breaches. Risks linked to information system are a great concern in organizations. In a study in USA and Europe, risks connected to computers and Internet was ranked number one in Europe and number two in USA. This is because the consequences of a security violation can be connected to the company's financial performance. Gordon et al. has proposed a framework for managing cyberrisks. It involves assessing the risks in a security violation in order to involve prevention that requires preventing the violation. These counter measures are divided in technical or formal and financial. The last step is to retrain the accepted risk level. The financial impacts of the security breaches are of interest for the companies that are planning the budget for their information security. Depending on the companies size an assessment of the whole information security environment can be expensive and impractical. Information security risk assessment is a helping aid in identifying threats against the security and evaluates their severity. Information security brings the questions about the effect of vulnerabilities and how much it will cost the organization.

But the assessment of the financial losses is a difficult step in the risk assessment for the following reasons:

- Many organizations are unable or unwilling to quantify their financial losses due to security breaches.
- Lack of historical data as many security breaches are not reported.
- Companies can become fearful of negative economic consequences resulting from the publication of a security breach.

There is a need to assess the risk of a security breach. It is by measuring the impact of a crime on the market value of a company. The approach captures the capital market with the market's yield expectations for losses caused by the breach. This is a great way in which companies are affected more by PR that the attack itself. In addition, managers strive to maximize a company's market value by investing in projects that increase shareholder value or minimize the risk of loss of shareholder value.

2.7.7 Vulnerabilities

Weaknesses that prevent a system from working properly are commonly defined as vulnerabilities [115]. A study made by Aven [115] implies that there exist different types of vulnerabilities which could be related to infrastructure objects or physical objects, but also related to cyber objects. It is by identifying these kinds of weaknesses within a system that risk analysis can be made (explained in next section), giving attributes for consequences whether they are financial loss or loss of other important functions in e.g. a state or society. A typical framework for risk analysis is often based on the description of risks and the likelihood of those risks to happen, affecting attributes as e.g. confidentiality, integrity and also privacies. The knowledge of how to implement these tools generates whether the framework is useful or not.

3 Methodology

The research of this thesis is built upon a survey and a simulation that has the intention to examine the current resilience of Swedish government authorities against denial of service attacks. A distributed denial of service attack is a specific phenomenon that potentially threatens the security systems of Swedish government authorities. To get more accurate results in this study, a number of surveys have been sent to different Swedish government authorities, that gives an understanding of their current capacity situation (see section 3.2). The idea is to use documented knowledge and expertise in this subject to understand the problem of having such threats.

It is important to anticipate the ethical concerns [116] within this study, since data will be retrieved from several participants that represent their authorities. Each responder is anonymous in order to protect the security of each Swedish government authority, meaning that responder is a delegate and thereby answers for their entire authority. All participants will be informed of the aim of this research by letting them know the work they contribute with and what the final result of this thesis will be. Every anonymous responder is expected to give a general overview of the security system against a distributed denial of service attack. The survey shall not interfere with their privacy and shall not promote improprieties that might reflect on their organizations. The participants shall not risk to be offended by the survey to minimize the risk of not answering. If any unofficial information is considered to be used within this study, it should have support by official channels in order to be included.

3.1 Research design

Before choosing a research design, four questions can be examined: what questions to study, what data are relevant, what data to collect, and how to analyse the results [117]. According to Patel and Davidson [118], it is important to manage the relationship between theory and empirism. By using the theory, it will make it possible to get knowledge about reality. There are three concepts that can be used; deduction, induction and abduction.

This research will have a deductive approach (see Figure 12), as the existing theory will be applied in the real life to see how the reality matches the theory. The existing theory helps to understand what information that needs to be retrieved, how the information should be interpreted and how the results should be related to the existing theory. An advantage of working deductively is that the study gets less subjective views from the researcher. This thesis includes a mix of qualitative and quantitative methods [117], although the quantitative method represents a major part of the thesis as it consists of collecting data. Qualitative method is only used for allowing the responders to give their own reflections.

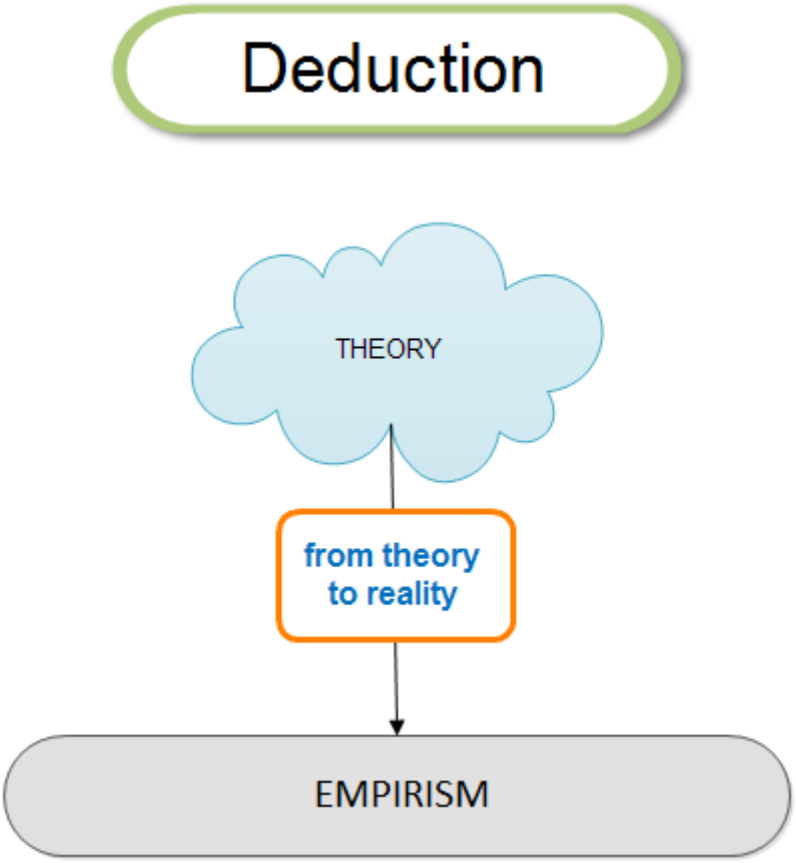


Figure 12. The deductive approach.

3.2 Data collection

To be able to answer the research questions, this study uses two different techniques of data collection, primary data and secondary data. Primary data is collected material [119], which in this case is retrieved from a survey. Secondary data is data that is already collected and documented [119], e.g. books and papers, which is the material compiled in the theory. The flowchart of primary and secondary data is illustrated in Figure 13. Note that it is important to be critical of the collected data and simultaneously examine how reliable and valid the information is.

Figure 13. Flowchart of data collection.

3.2.1 Primary data

Primary data is collected through a survey, where the responder answers for their authority. The purpose with the survey is to bring additional information that is useful to the chapter of result and conclusions. In the development of the survey, it is important to compose the questions as neutral as possible, well deliberate and not offensive. The survey will avoid e.g. valuations or general statements. The credibility of the survey depends on the questions which is why all questions have to be well defined and explained to minimize misunderstandings. When having empirical studies, it is important to know how data should be gathered and later be interpreted. The operational definition should be close to the theoretical definition. In this study, the questions in the survey will be based on the theoretical information to be able to see if the theory matches the reality. This will be further described in section 3.4.1.

3.2.2 Secondary data

Secondary data is collected by gathering academic material which has been retrieved by using the University library as a source. Examples of these databases are IEEE Xplore and Science direct.

These databases give a base for finding definitions and getting deeper understanding of the chosen subject.

Text books have also been included as a complement to gain additional information. Several reports from different organisations have been found by using search engines online.

These organisations have proven to be trustworthy since both authorities and academic papers refers to them. A compilation of the reports shows the development and the current situation of distributed denial of service attacks. Those sources are:

- Akamai.
- Arbor Network.
- Computer Emergency Response Team, both org and se.
- Prolexic.
- Swedish government authorities documents.

3.3 Choice of simulation tool

The simulation tool, called Opnet Modeler Suite [120], is used in order to verify the research material, e.g. the achieved theoretical values. It is also used to achieve sustainable results. The Opnet software is able to generate results based on certain values that are manually configured. It is a software that models a simulation of a system as discrete events and has several existing models based on current protocols, which are used in different network types and technologies.

In this case, the simulation is built as an adjusted model according to the purpose of this thesis to simulate a realistic scenario, e.g. to generate appropriate traffic to investigate the reaction of a certain system. Note that the traffic generator works according to input values of own choices, that in this case came from several authorities. It is important to have relevant values as input values in order to get useful results. Those results get compared with the expected values to be able to analyse the final results.

The values that have been used in the simulation can be found in the result chapter, see section 5.2.

3.4 Approach

The work of this study is divided into different phases that together provide the complete result. These phases are surveys, simulations and risk assessment, which are illustrated in Figure 14, showing the final result as a template of guidance for Swedish government authorities.

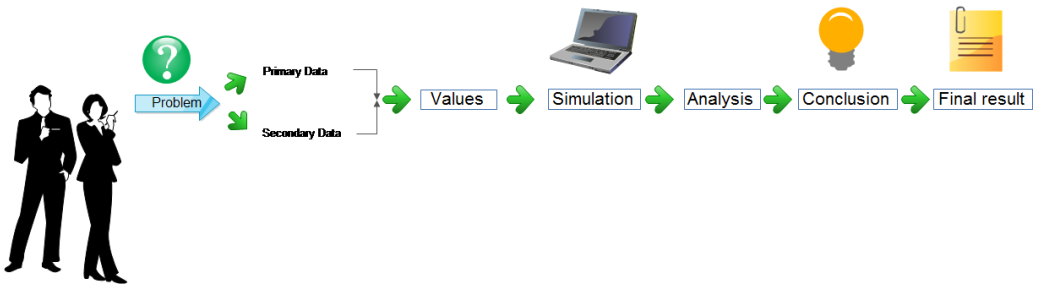


Figure 14. Visualization of the approach.

3.4.1 Survey guide

As mentioned earlier, working deductively gives the possibility to obtain an overview of reality based on theories. In this thesis, a survey will generate data based on Swedish government authorities' measurements that together with the theoretical values of this study is used in the simulation.

The data from the surveys shows the current capacities that Swedish government authorities can handle. The survey (see appendix A) is supposed to work as a complement and give confirmation to this study. The aim of this study has to be clearly communicated towards the participants, and so does the structure of all questions in every section within the survey in order to obtain a logical structure to retrieve an accurate result, which requires that the responder should have specific qualifications, skills or experience within this subject. The targets for this study are therefore people with the general position as "information security specialist". The final work will be offered to be distributed among the participants after closure.

In order to collect data about the authorities' current situation, the survey has been divided into different sections. The first section will provide data in the presence of the simulation. In this section, questions will be asked about the authorities' current situation, e.g. how many users their servers are expected to manage. These data will give a base, to be able to begin the simulation. The second section will provide more detailed data about denial of service attacks that will be used, together with the data from section one, for the simulation. In this way, attack simulations can be created.

The third and fourth sections will give data about the documentation, the communication and cooperation. These questions will generate an overview of the current situation regarding documentations, communications and cooperations, having questions about how the authorities spread information about different threats; if they report incidents, if a cyberattack occurs and if they share resources between authorities.

Initially, questions were asked about the authorities' current situation in order to obtain an overview of the authorities' extent as the aim is to categorize the size of the authorities.

Based on the theoretical information described in section 2.3.2, questions in part 2 of the survey have been asked to confirm the information.

This has been done by first see whether the authorities have been attacked or not and then compile the most common attack types and their duration. The questions in part 3 of the survey are based on the information described in Chapter 2.5 and in Chapter 2.7, where in 2.5 shows that attacks often occur in pure damage or in order to seriously damage a system to make a statement.

It also appears that the attacks occur for economic reasons, however, this is excluded in the survey because of the attacks with economic motives predominate over private companies that engages economical profit. Through this, the scenarios in the survey have been developed in order to get the level of severity from the authorities' perspective. Using the information in chapter 2.7, the consequences of each scenario have been graded. The questions in part 4 and part 5 have been prepared to see how authorities follow the guidelines that have been developed to increase the security. In the theory, it appears that e.g. an increased defence can be created by forming an alliance which requires authorities to cooperate or initiate cooperation. The questions are based from chapter 2.6 and 2.7.

3.4.2 Generating results

The given data from theory is used to create simulations. Theoretical values have been retrieved by interpreting several reports to identify realistic scenarios regarding amount of workstations and legitimate traffic within an authority. The amount of necessary infected computers needed to reach certain capacity can be calculated by retrieving the results of simulated overloads in the network.

A cumulative frequency graph [121] is used as a base to show the occurrence of differently sized attacks, which gives an understanding of how likely it is for an authority to survive a specific attack. A part of the survey gives information of the capacity that different authorities have, to be able to calculate whether the attack succeeds or fails, according to the size of the authority. The information of the different Swedish government authorities will be generalized into small, middle and large authorities.

The result of the differently sized authorities are presented based on the data from Figure 5 in section 2.3.2.1 and is also combined with the consequences of the different scenarios which are presented as an adjusted impact and likelihood matrix.

The matrix has been created based on Figure 11 in chapter 2.7.3 in order to identify which consequence that is of higher score in the two scenarios given in the survey. Since the scenarios include several consequences for the same grading scale, the consequences have been merged into percentage occurrence to obtain an overview of the result for each grading scale.

To identify which consequence that is of higher score, a grading system has been constructed by assigning a score from 1 to 5 to each consequence level (see Table 12); where "Not important at all" gets a score of 1 and "Critical" gets a score of 5. By multiplying the score of the consequence level and the percentage occurrence, it brings different scores according to the seriousness of the consequences during an attack.

A linear regression equation method [122] is used as an approximation tool to predict the future of e.g. computer capacity regarding the clock rate and to calculate the capacities of bandwidth that Internet service providers possibly could offer in a near future. The regression function can be stated as Equation 1, where Y_i is the outcome, β_0 and β_1 are parameters, X_i is a constant and ε_i is an error term, if the function is linear:

$$Y_i = \beta_0 + \beta_1 X_i + \varepsilon_i \quad (1)$$

The error term has been calculated by using standard error [123]. In order to use standard error (see Equation 3) the standard deviation, S_D, has to be calculated first by using Equation 2, where y_i is the size of the observation, y is the average size of the sample and N is the number of observations in the sample.

$$S_D = \sqrt{\frac{\sum(y_i - y)^2}{N}} \quad (2)$$

After calculating the standard deviation, the standard error, S_E, can be calculated by dividing the standard deviation by the square root of the number of observations.

$$S_E = \frac{S_D}{\sqrt{N}} \quad (3)$$

Table 12. Score system for grading consequences.

Consequence level	Score
Critical	5
More important	4
Important	3
Less important	2
Not important at all	1

4 Design

This chapter describes the construction to achieve relevant results in order to accomplish this thesis.

4.1 Building scenarios

Statistics can be calculated by creating a possible scenario showing how a government authority could work. The scenario should include both internal workstations where employees work with, almost, unlimited access but also external workstations where employees can access their work with some restrictions. The following scenario (see Figure 15) could illustrate an example of a basic and legitimate scenario where assumptions are made of a network consisting of 50 internal workstations and 25 external workstations, this example intends to reproduce a typically small authority such as a small customer service office, where all workstations are connected to every server in the internal system.

After creating the scenario, one botnet was added (see Figure 16) focusing on the FTP server to show the behaviour when increasing the number of zombies, which is made by increasing number of workstations. Several tests, with different values in the workstation attribute, are constructed to obtain a greater understanding and accuracy for the statistics.

When understanding the behaviour with one botnet, several botnets (see Figure 17) were added in order to achieve an illustration of a large-scale distributed attack, also by editing the attribute for the botnets. Each botnet can then be defined with workstations, allowing access as e.g FTP clients, which symbolises infected computers, also known as zombies, within the network.

The outcome of this construction is to give an understanding of development in the network traffic when attacking with smaller botnets. The setup of the network is defined in Table 13.

Table 13. Network setup in Opnet, connection types.

Amount	Type	Tech Spec	Other information
1	FTP Server	Sun Ultra 10, simple CPU 333MHz, 64Kb I/O	Solaris
1	Ethernet Switch	Ethernet16_switch_adv, up to 16 Eth Interfaces. 10, 100, 1000 Mbit/s.	Spanning Tree, IEEE 802.1D, IEEE 802.3.
6	Router	Ethernet2_slip8_gtwy_41	LAN, R.U, Botnet Router.
12	Switched LAN	Eth_switched_lan, 100BaseT (Fast Ethernet), Switching speed: 500.000, 2.000.000	TCP, UDP over IP. Free setup on Workstations, up to 120.000.
1	Firewall	Ethernet2_slip8_firewall, multihomed-server. 10, 100, 1000 Mbit/s.	Ethernet, BGP, IGRP, IP, OSPF, RIP, TCP, UDP.
1	Internet	ip32_cloud, supporting up to 32 serial.	BGP, IGRP, IP, OSPF, RIP, TCP, UDP.
6	Internet Connection cable	PPP_DS3, Duplex Link, Router/Firewall to Internet. Data rate type of signal: 44.736 Mbit/s.	75 ohm coaxial cable and connectors.
19	Internal Internet Connection Cable	10Gbps_Ethernet, Duplex Link,	Full duplex Ethernet cable.

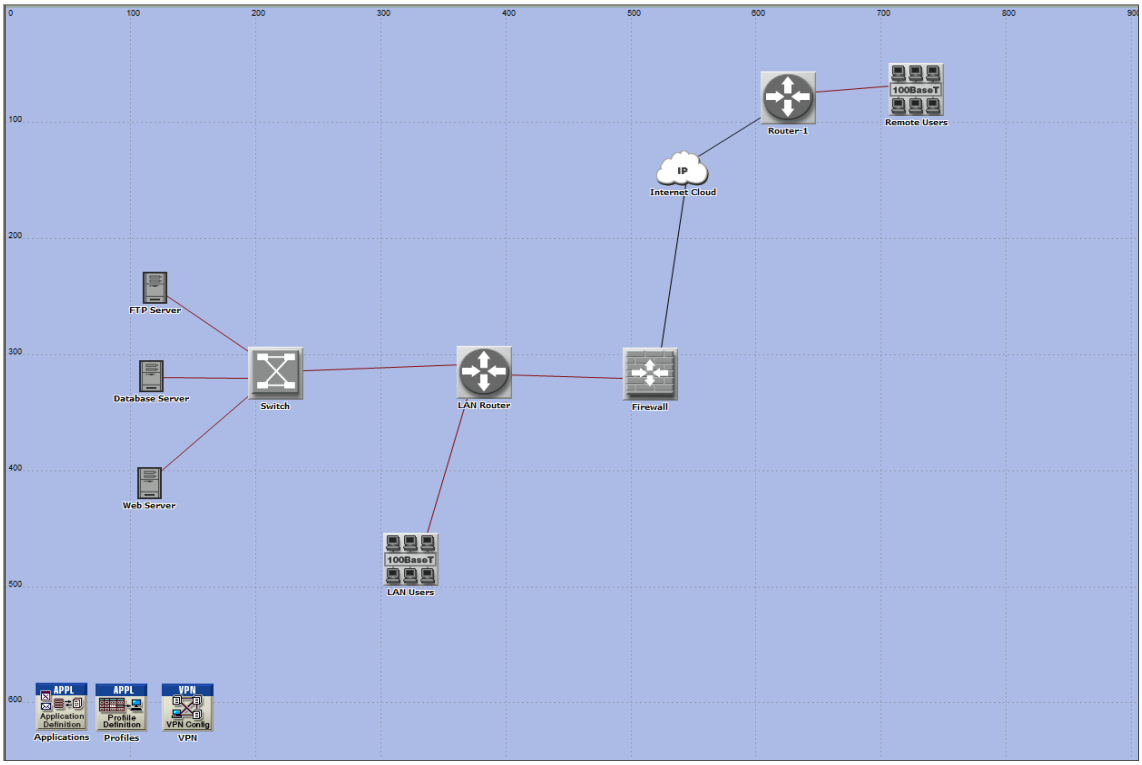


Figure 15. Basic scenario, normal traffic is assumed.

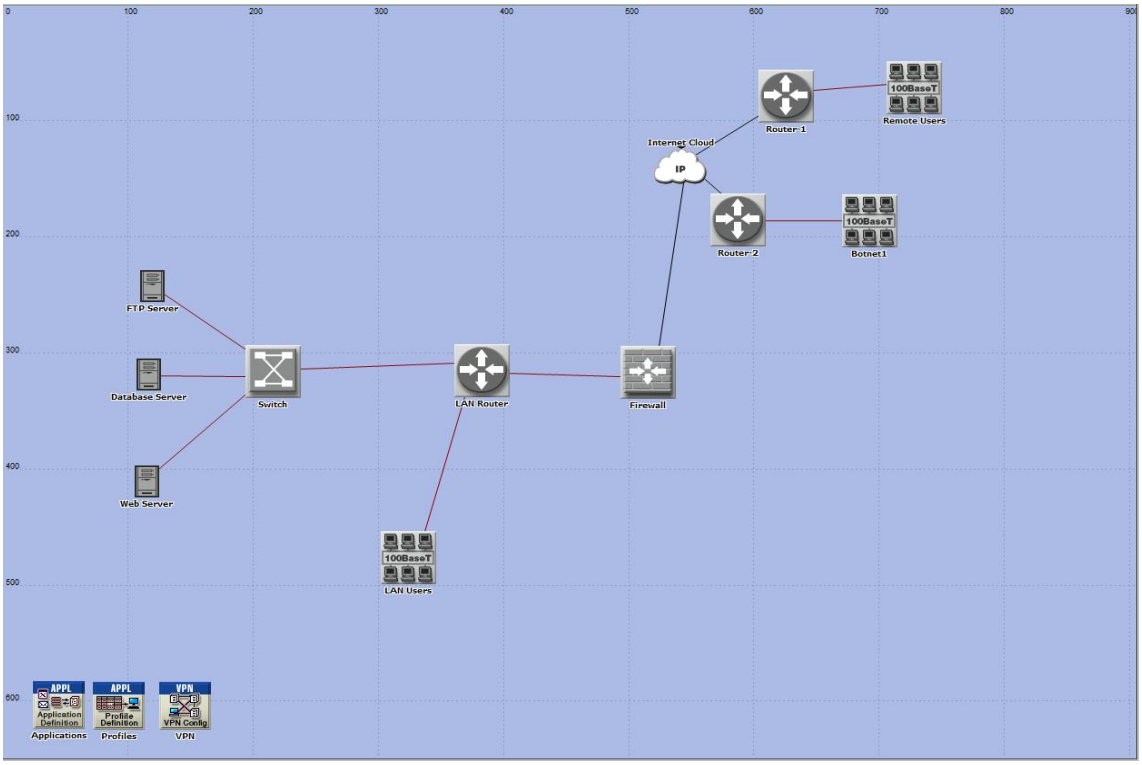


Figure 16. Basic scenario with one botnet added.

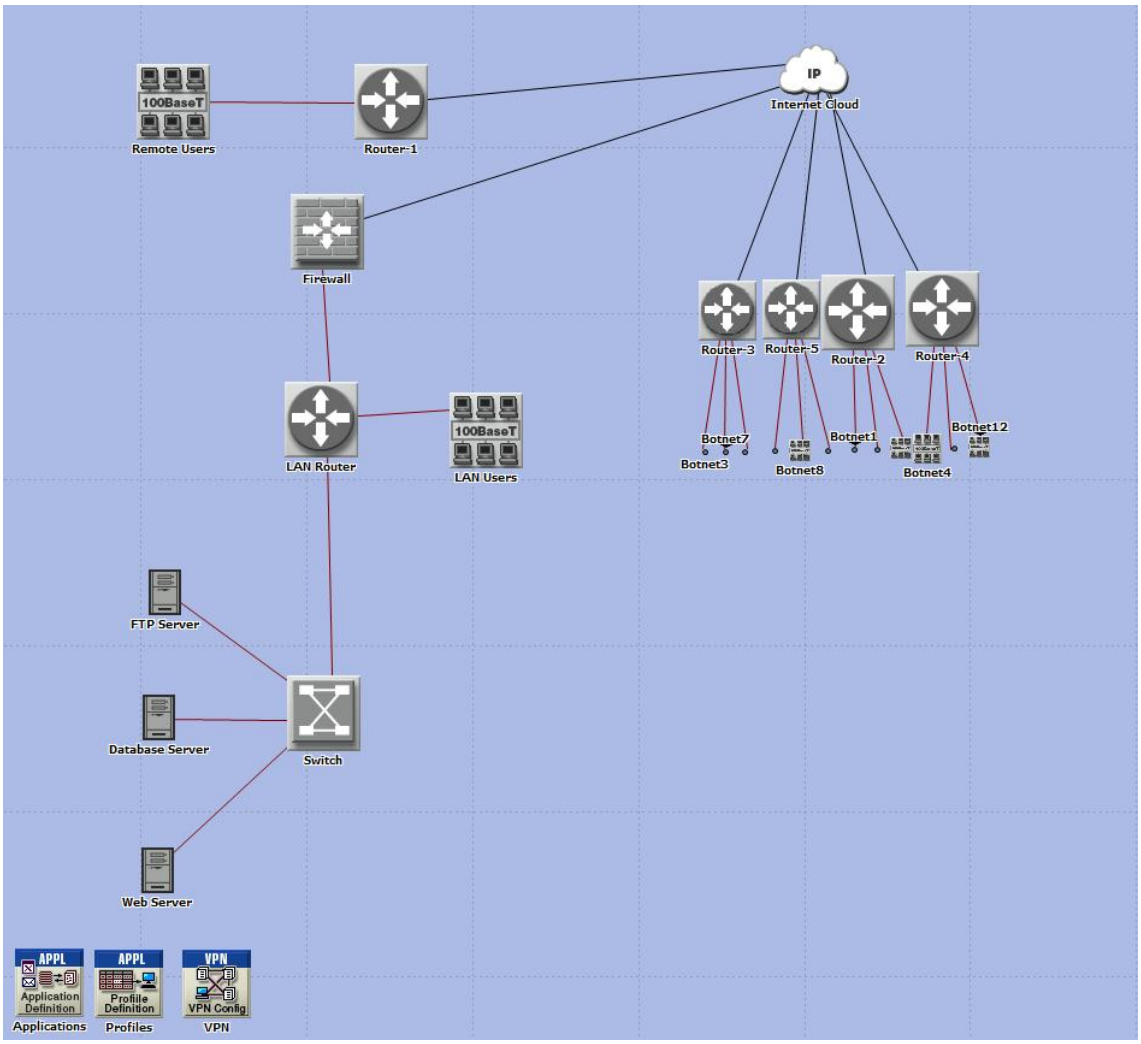


Figure 17. Basic scenario with several botnets added (12 botnets in this figure).

4.2 Occurrence of attacks

Statistical values of differently sized attacks presented in chapter 2.3.2.1 are used and converted into a cumulative frequency graph (see Figure 18). The measurement of the attacks starts with lower than 1 Gbit/s where the occurrence of that case is 20% and the next interval is between 1 Gbit/s and 5 Gbit/s having the occurrence of 25%, which together combined from less than 1 Gbit/s up to 5 Gbit/s gives an occurrence of 45%. The graph increases by adding each occurrence of the attack to the previous. This continues for all cases and is thereby added together to give a full overview of the dispersion of the attacks. The graph is constructed to be used as a base graph in order to illustrate Swedish government authorities' current situation in surviving an attack, where the data from the survey gives a realistic zone on this graph with the information of likelihood of surviving.

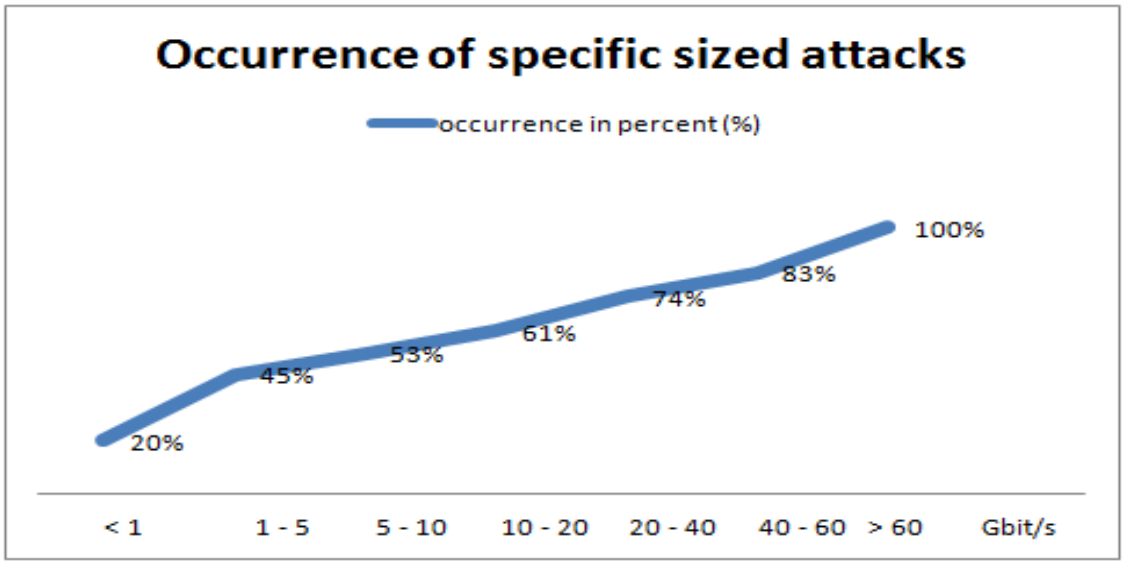


Figure 18. Base-graph for occurrence of specific sized attack.

5 Result

Chapter 5 includes the results of this thesis and answers the research questions. Note that every section within this chapter includes several figures and tables that present the entire result. Section 5.1 presents the predictions of how the development of the clock rate will continue to increase. Section 5.2 presents an overview of the amount of infected computers needed to reach certain capacities in an attack. Section 5.3 is related to the need of infected computers to reach certain capacities regarding the upload bandwidth and how it will develop in the next coming five years. Section 5.4 presents a visualization of the current situation among Swedish government authorities given by the survey. Section 5.5 is related to the previous section by giving a reflection of the classification of the consequences in different scenarios, which are graded in a scale. Finally section 5.6 presents the current situation in surviving an attack depending on the size of the authority and the size of the attack.

5.1 Clock rate prediction using Moore´s Law

Linear regression was applied to the values from the theory of Moore's law (see chapter 2.4) to be able to continue the increasing curve and by that estimate the clock rates for the future. The result is an equation that can predict the clock rate capacity, C_{cr}, by having the year, y, as input. $C_{cr}(y)$ is defined as:

$$C_{cr}(y) = 156.11y - 3.1109 * 10^5 \pm 381.66 \quad (4)$$

Since an interval of five years is relevant for this thesis the estimation was made until 2020, giving a clock rate capacity of around 4254 MHz, which means approximately 4.25 GHz (see Figure 19 for an overview).

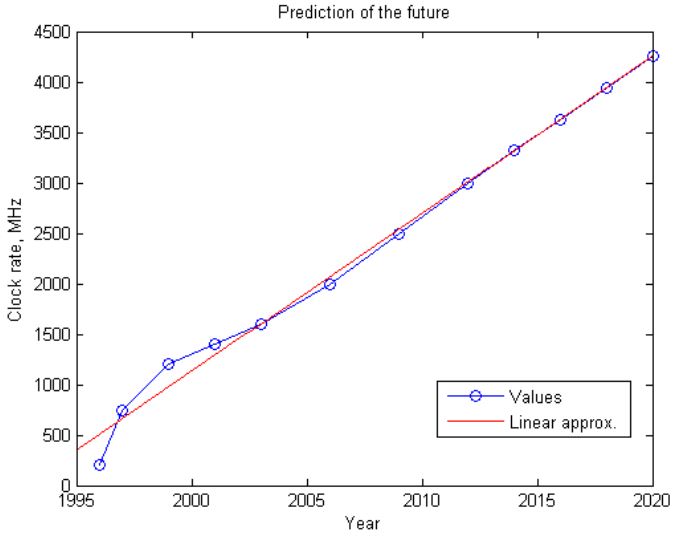


Figure 19. Five years prediction of clock rate.

5.2 Calculating the need of zombies

The definition of workstations needed to reach a certain capacity is calculated by using the results from the several simulations that were made according to the construction in Chapter 4.1.

Those simulations gave a base for a formula that could be used to illustrate the necessary amount of zombies to reach a specific capacity. The values for a simulation of a three hour long scenario are presented in Table 14, while smaller simulations of 60 minutes long scenario respectively 30 minutes long scenario are presented in Table 15. The graph illustrating the values of the simulation, where 50 zombies generates 0.147 Mbit/s and with an interval adding 50 zombies each time up to 2000 zombies generates a capacity of 2.755 Mbit/s (compiled in Table 13) is presented as Figure 20. These values gives the following formula by using linear regression, where n represents the number of zombies to achieve certain capacity of a botnet in bit/s, C_b:

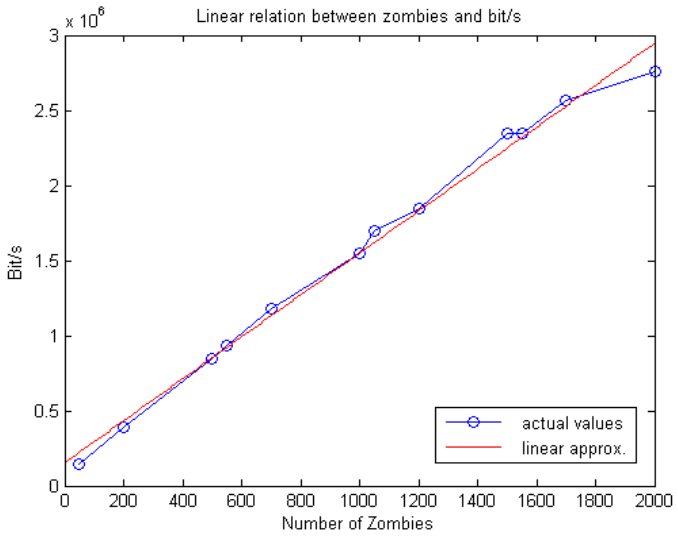
$$n(C_b) = \frac{C_b - 154240}{1395.6} \pm 0.25 \quad (5)$$

Table 14. Zombies needed for specific capacity.

Zombies	Average Capacity (Mbit/s)
50	0.147
200	0.389
500	0.850
550	0.931
700	1.176
1000	1.546
1050	1.693
1200	1.848
1500	2.346
1550	2.346
1700	2.564
2000	2.755

Table 15. Large scale simulations.

Duration of simulation (minutes)	Zombies	Average Capacity (Mbit/s)
60	60 000	39.428
60	96 000	35.529
30	120 000	26.000



Figur 20. Linear relation between zombies and bit/s up to 2000 workstations.

5.3 Predicting the average upload bandwidth

The average upload bandwidth measured by Swedish Internet service providers shows that the capacity differs depending on connection type (see Figure 21). The average values from chapter 2.4.2 have been merged into an average upload bandwidth for each year where all Internet service providers are included; see Table 16 for detailed description.

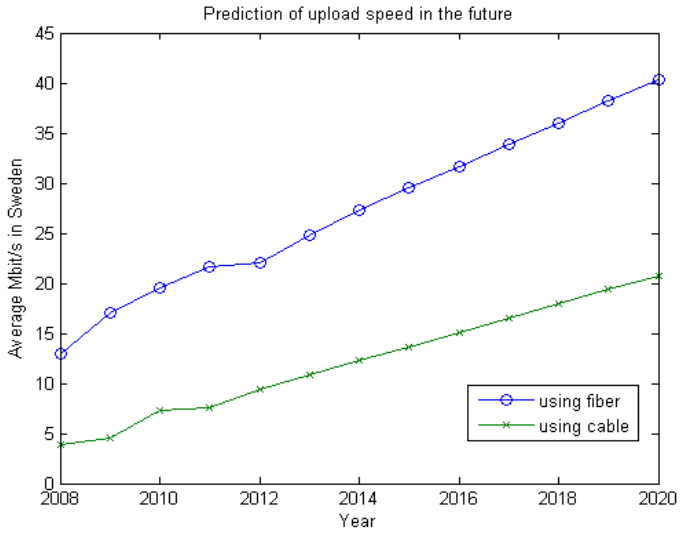
In this case the figure shows the connection types fiber and cable, which gives a base for the following two formulas by using linear regression, where y represents the year to be predicted to achieve certain upload fiber capacity, C_{uf}, and upload cable capacity, C_{uc}:

$$C_{uf}(y) = 2.1746y - 4352.3 \pm 94.81 \quad (6)$$

$$C_{uc}(y) = 1.4243y - 2856.3 \pm 1.56 \quad (7)$$

Table 16. Average upload speed in Mbit/s based on average values from ISP.

Type	2008	2009	2010	2011	2012	2013
Fiber	12.96	17.03	19.58	21.58	22.00	24.82
Cable	3.83	4.55	7.30	7.61	9.43	10.83



Figur 21. Linear relation between year and average upload speed in Mbit/s, for fiber and cable connection.

5.4 Results of survey

A survey was sent to 21 Swedish government authorities. The outcome was replies from 8 of 21 authorities that are anonymized due to security and ethical reasons.

The technical questions were included as part 1 and part 2 in the survey and a summary of the result is presented in Table 17. The non-technical questions were included as part 2, 3 and 4 in the survey and the result is presented in Table 18.

Consequences based on two different scenarios were graded in the survey by the authorities. Figure 22 and Figure 23 illustrates the scenarios and how the Swedish government authorities have classified different levels of the consequences regarding the scenarios.

The first question in Table 17 describes that 7 of 21 have been victimized by any IT-related attack and that 6 of 8 have been attacked by an overload attack. The next question about the duration of the attacks shown to be that 60% of the authorities answered that the duration was between 0 and 6 hours, 20 % answered between 7 and 12 hours and 20% answered that the duration was between 1 and 3 days. Most of the authorities, in 57% of the cases, have a network built with over 500 servers.

In 14% the answer was that the authorities has a network with between 11 and 50 servers, and the same percentage answered a network with between 101 and 200, at last also 14% had a network with between 201 and 500 servers.

The next question was about the data traffic and how much specifically the authorities servers could handle. The authorities answered 100 Mbit/s, 200 Mbit/s, 450 Mbit/s, 2 Gbit/s and 10 Gbit/s. How many visitors that visited the website every day was a total of 200, 100-1 000, 1 500, 2 500, 4 000 and 7 000 visitors. The first question in Table 16 gave a list of the most common denial of service attacks and which of the attacks the authorities recognized. The result was that 6 of 8 knew ACK and DNS, 5 of 8 knew HTTP GET, ICMP, SYN and UDP. 4 of 8 knew UDP Fragment and Chargen.

All the authorities answered that they perform risk analysis, consequence analysis and that a contingency plan exist in case of the occurrence of an attack, but none (0 of 8) follows the standard ISO 31000. 5 of 8 use the standard ISO 27000 and any form of LIS, to improve the IT-security. The question asked if every IT-incident was reported, 4 of 8 answered yes, internal and external, 4 of 8 answered yes, internal and 1 of 8 answered yes, external. The next question gave a list of how employees get updated about IT-related threats. 5 of 8 updated through seminars, 4 of 8 through reports (weekly/monthly), 7 of 8 through meetings and 3 of 8 through workshops. All of the authorities answered yes on the question if cooperation with other authorities exists and the supplementary question gave a list of which type of cooperation. 8 of 8 answered that they exchange information with each other, 3 of 8 share resources and 2 of 8 cooperate with spare of capacity. Only 3 of 8 answered that their IT-maintenance is outsourced and these three authorities answered yes if there are any specific requirements developed for managing IT-incidents.

The two scenarios Vandalism & Protest and Society Threats had three consequences; Information is denied to client, internal communication is disrupted and external communication is disrupted. In the first scenario, Vandalism & Protest, 0 of 8 answered not important at all for all three consequences.

1 of 8 answered less important also for all three consequences. 3 of 8 answered important for the two consequences information is denied to client and internal communication is disrupt, while 2 of 8 answered important for consequence external communication is disrupted. 2 of 8 answered more important for consequences information is denied to client and internal communication is disrupted and 4 of 8 answered more important for consequence external communication is disrupted. 2 of 8 answered critical for all three consequences. In the second scenario, 0 of 8 answered not important at all for all consequences. 0 of 8 answered less important for consequence information is denied to client while 2 of 8 answered less important for both internal communication is disrupt and external communication is disrupt. 3 of 8 answered important for information is denied to client, 2 of 8 answered important for internal communication is disrupt and 1 of 8 answered important for external communication is disrupt. 2 of 8 answered more important for consequences information is denied to client and external communication is disrupt and 1 of 8 answered more important for internal communication is disrupt. 2 of 8 answered critical for all three consequences.

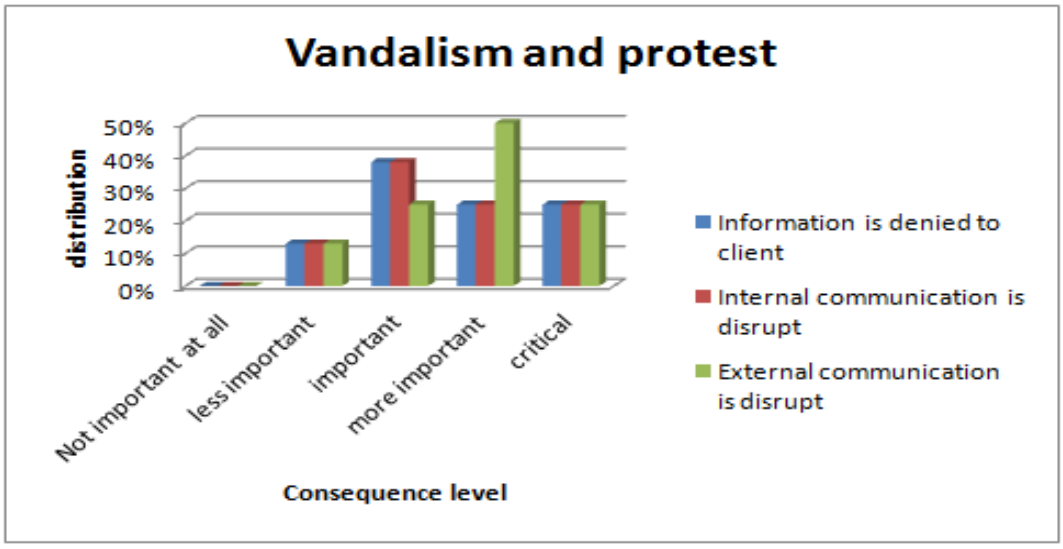
Table 17. Technical results.

Questions	Answers
Have you been victimized by any IT-related attack?	Yes: 7 of 8. No: 1 of 8.
Have you been attacked by an overload attack?	Yes: 6 of 8. No: 2 of 8.
What was the duration of the attack?	0 – 6 hours: 60% 7 – 12 hours: 20% 1 – 3 days: 20%
The network within the authority is built upon how many servers?	11 – 50 : 14% 101 – 200: 14% 201 – 500: 14% +500: 57%
How much data traffic can the servers handle?	*6 of 8 answered,* 11 – 50 servers: 2 Gbit/s 101 – 200 servers: 10 Gbit/s 201 – 500 servers: 100 Mbit/s +500 servers: 200, 450 Mbit/s 1000 servers: 10 Gbit/s
How many visitors visit the website every day?	*6 of 8 answered,* 200 100 – 1000 1500 2500 4000 7000

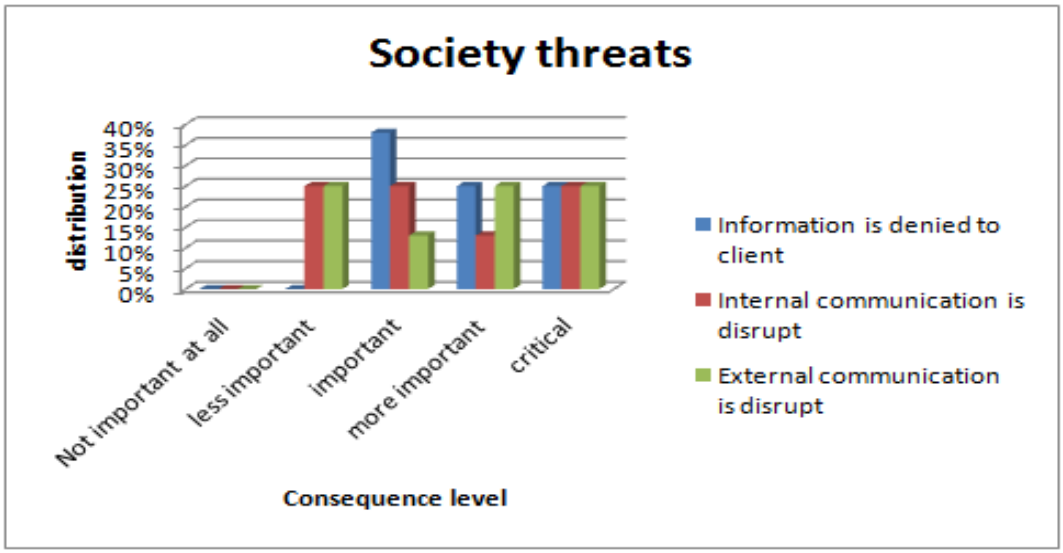
Table 18. Knowledge and consequence results.

Which of the following types of Denial of Service attacks are known and recognized? (Multiple choices allowed.)	***8 of 8 answered,*** ACK: 6 of 8 DNS: 6 of 8 HTTP GET: 5 of 8 ICMP: 5 of 8 SYN: 5 of 8 UDP: 5 of 8 UDP Fragment: 4 of 8 Chargen: 4 of 8 Other: 6 of 8
Are risk analysis and consequence analysis performed?	Yes: 8 of 8 No: 0 of 8
Are any of the following standards used to improve the IT-security? (Multiple choices allowed.)	*8 of 8 answered,* ISO 27000: 5 of 8 ISO 31000: 0 of 8 Any form of LIS: 5 of 8 Other: 1 of 8 None: 1 of 8
Does a contingency plan exist in case of the occurrence of an attack?	Yes: 8 of 8 No: 0 of 8
Are every IT-incident reported?	*8 of 8 answered,* Yes, internal and external: 4 of 8 Yes, internal: 4 of 8 Yes, external: 1 of 8 No: 0 of 8 Other: 3 of 8
How do employees get updated about IT-related threats? (Multiple choices allowed.)	*8 of 8 answered,* Seminars: 5 of 8 Reports (weekly/monthly): 4 of 8 Meetings: 7 of 8 Workshops: 3 of 8 No need for updates: 0 of 8 Other: 5 of 8

Does cooperation with other Swedish government authorities exists?	Yes: 8 of 8 No: 0 of 8
If yes, which type of cooperation?	*8 of 8 answered* Exchange of information: 8 of 8 Share of resources: 3 of 8 Spare of capacity: 2 of 8 Other: 4 of 8
Are parts of the IT-maintenance outsourced?	Yes: 3 of 8 No: 5 of 8
If yes, are there any specific requirements developed for managing IT-incidents?	Yes: 3 of 3 No: 0 of 3



Figur 22. Vandalism and protests as attack scenario.



Figur 23. Society threats as attack scenario.

5.5 Classifying consequences

The following results are scores obtained by using the methodology of classifying consequences, described in section 3.4.2.

The total score is a product of the consequence levels and answers given from the survey (see Figure 22 and Figure 23). These two matrices are given the opportunity to decide which consequence that is considered to be most serious by looking at the highest score. The two matrices are divided regarding to the two scenarios, where Table 19 shows the grades of the consequences in the case of vandalism and protest while Table 20 shows the grades of the consequences in the case of society threats. In the scenario of vandalism and protest (Table 19) the consequence "external communication is disrupted" shown to be the consequence with highest score. While the consequence with highest score in the scenario of society threat shown to be "information is denied to client".

Table 19. Grading consequences in scenario of vandalism and protest.

	Score	Information is denied to client	Internal communication is disrupt	External communication is disrupt
Critical	5	0.25	0.25	0.25
More important	4	0.25	0.25	0.5
Important	3	0.38	0.38	0.25
Less important	2	0.13	0.13	0.13
Not important at all	1	0	0	0
Total score:		$(5 * 0.25) + (4 * 0.25) + (3 * 0.38) + (2 * 0.13) + (1 * 0) = 3.65$	$(5 * 0.25) + (4 * 0.25) + (3 * 0.38) + (2 * 0.13) + (1 * 0) = 3.65$	$(5 * 0.25) + (4 * 0.5) + (3 * 0.25) + (2 * 0.13) + (1 * 0) = 4.26$

Table 20. Grading consequences in scenario of society threats.

	Score	Information is denied to client	Internal communication is disrupt	External communication is disrupt
Critical	5	0.25	0.25	0.25
More important	4	0.25	0.13	0.25
Important	3	0.38	0.25	0.13
Less important	2	0	0.25	0.25
Not important at all	1	0	0	0
Total score:		$(5 * 0.25) + (4 * 0.25) + (3 * 0.38) + (2 * 0) + (1 * 0) = 3.39$	$(5 * 0.25) + (4 * 0.13) + (3 * 0.25) + (2 * 0.25) + (1 * 0) = 3.02$	$(5 * 0.25) + (4 * 0.25) + (3 * 0.13) + (2 * 0.25) + (1 * 0) = 3.14$

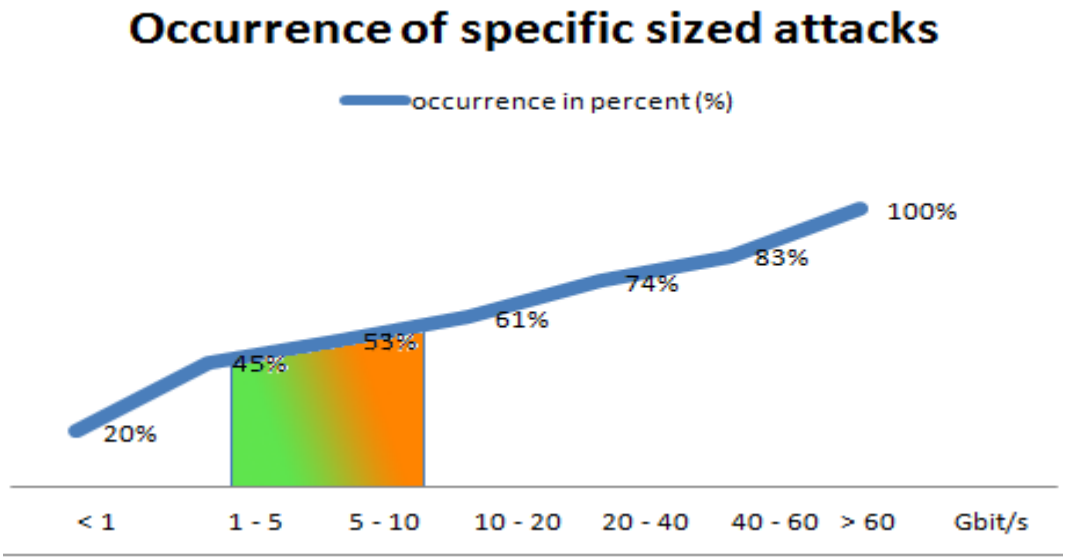
5.6 Current situation in surviving attacks

In this section three graphs will be presented showing how a small, middle and large authority will survive during an attack. The graphs are created from the base-graph in section 4.2. A small sized authority is, according to the result of the survey (see Table 16), between 2 Gbit/s and 10 Gbit/s. A middle sized authority is between 20 Gbit/s and 50 Gbit/s, and a large sized authority exceeds 100 Gbit/s.

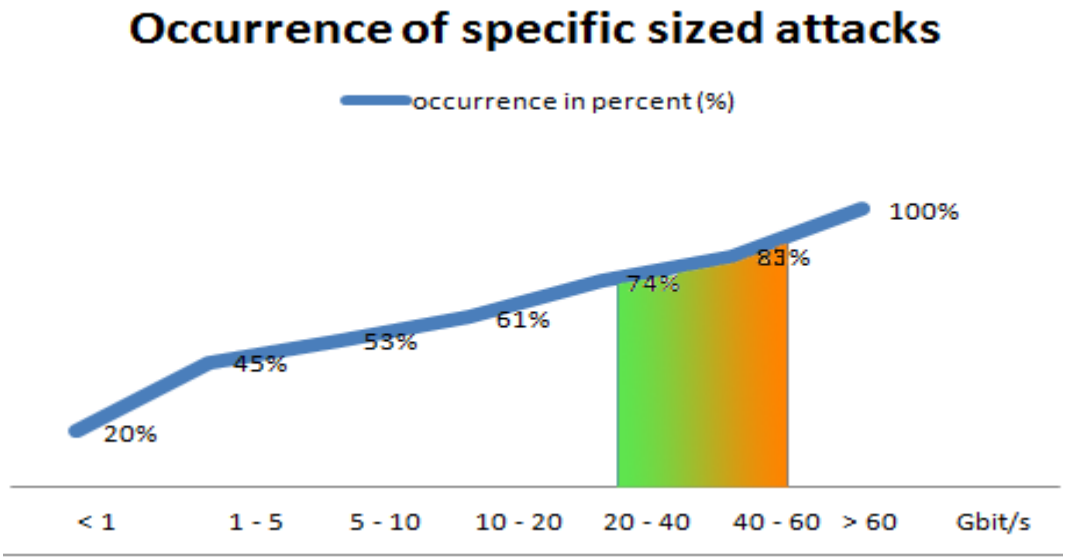
The probability of surviving an attack in the interval 1 Gbit/s to 10 Gbit/s is in between 45% to 53%, depending on the actual capacity of the authority, when having a small sized authority. This gives a risk of 47% in not being able to survive an attack at all, but is in a risk zone up to around 55% of all the attacks, since the authority could have different capacities within this zone. The case of a small sized authority is illustrated in Figure 24.

When having a middle sized authority the probability of surviving an attack in the interval 20 Gbit/s to 60 Gbit/s is in between 74% to 83%, depending on the actual capacity of the authority, which gives a risk of 17% of not being able to survive an attack at all, but is in a risk zone up to around 26% of the attacks, since the authority could have different capacities within this zone. The case of a middle sized authority is illustrated in Figure 25.

The third graph, illustrated in Figure 26, shows that a large sized authority survives all attacks measured in this study. Note that a large sized authority with a capacity that exceeds 100 Gbit/s would survive practically all attacks up to 100 Gbit/s before entering a risk zone. The exception is for the attacks measured to be in a size of 309 Gbit/s, which are very uncommon and still unlikely to occur.



Figur 24. Risk of DoS on a small sized authority.



Figur 25. Risk of DoS on a middle sized authority.

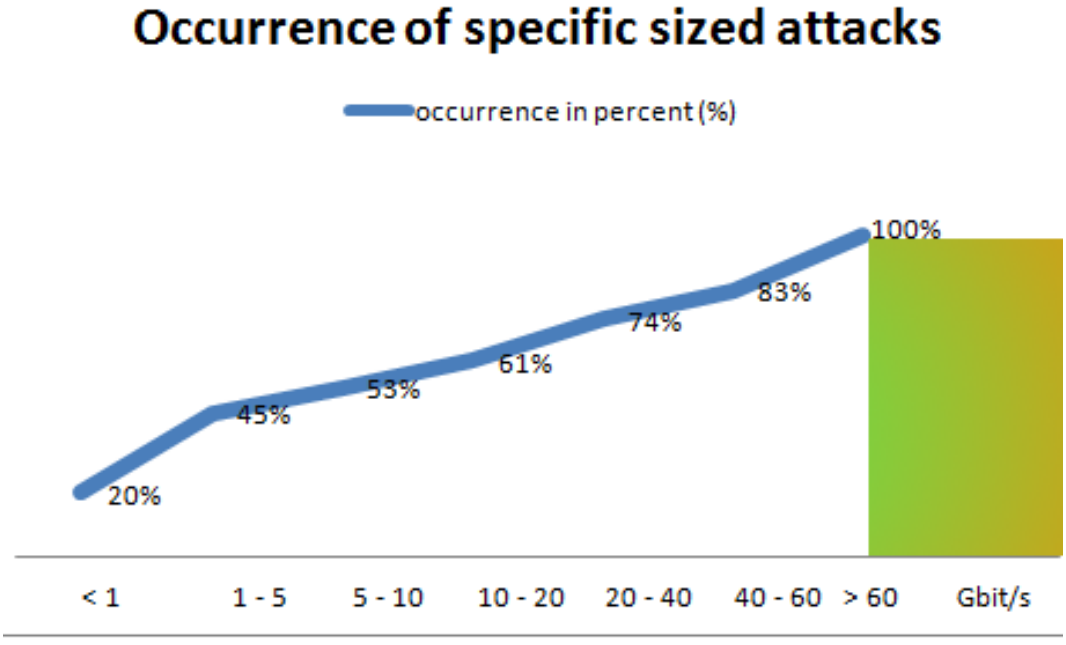


Figure 26. Risk of DoS on a large sized authority.

6 Discussion

The overall aim of this thesis was to investigate whether Swedish government authorities are or are not prepared against a modern distributed denial of service attack on a large-scale by giving results of the current situation and estimating the coming five years.

The goal of this thesis has been reached by answering our research questions by the following statements:

- The Swedish government authorities cannot communicate externally and reach out to the society as impacts during a denial of service attack.
- An increased resilience is when the capacity exceeds 60 Gbit/s.
- 60% of the Swedish government authorities within this study are prepared against a modern distributed denial of service attack.

The sub questions that were taken in consideration in order to achieve the goal have also been answered. The development of computer and server capacity from a historical perspective and the estimation of five years have been answered in section 5.1 using Moore's Law. By using the result from the survey and theoretical data it was possible to estimate which sized attacks that would be dangerous for Swedish government authorities (see section 5.6), and the survey also gave the answer about the consequences (see section 5.4). The question about the importance of the bandwidth and data transfer has been answered with the different equations in sections 5.1, 5.2 and 5.3. The equations show that the upload bandwidth and clock rate will increase which would lead to a less need of infected computers to obtain the same impact. The two last sub questions were a bit difficult to answer as the authorities would not give specific details about their capacities. Parts of these two questions have been answered in the survey, see Table 17.

Even though the study started in one direction and was adjusted during the time it has still followed the original research questions and by that achieved the aim of this thesis. Other suggestions that came up as discussion for continuing this study are presented in section 6.3.

6.1 Evaluating results

It clearly appears that the development of the clock rate has been developing in a linear pattern over the last years, and there are no strong evidence showing that this pattern will change in a near future. What seems to be undoubtedly, given by this thesis, is that even faster computers will be available in the coming years, by looking in the development curve in section 5.1. Moore's law has never taken clock rate into consideration when predicting the development; it is rather the development of the amount of transistors that has been investigated. This means that it would be false to assert that the clock rate development and the transistor development are the same, but one thing that still is possible to say is that it gives a basis for a development that is easier to follow and understand. Even less does Moore's law consider the adjustments that processor manufacturers do to achieve a little higher capacities, e.g. by having dual-core or quad-core processors etc.

That is why this study only works as guidance for predicting the future, since the future will always be uncertain. The equation to predict the future of computers' clock rates, presented as Equation (4), is an equation that works as a guidance to predict the clock rate in clear number for the coming years. An example of this use is to see that computers would have a clock rate of 4.2 GHz in a near future (if no sudden revolution changes the predictions), which is not so unlikely since people talked about computers with clock rates of 3 GHz for some years ago which turned out to be reality nowadays.

A computer that has higher clock rates calculates and works faster. This could mean that it would take fewer computers to both treat and generate more requests in the future than it takes nowadays. The capacities that the simulation within this study provided, gave a basis for the calculations and estimations of how many infected computers that were necessary to reach certain capacities, but it still remains to calculate the margin of error that exists when simulating unknown networks given that the Swedish government authorities keeps the real network structure classified. More accurate values would have been obtained if this was not an affecting factor, since the structure of the simulation could have been a real reconstruction of an authority. The solution to this case was to gradually retrieve results by increasing the amount of workstations in the botnet to investigate the behaviour.

This study made it possible to calculate and estimate the amount of infected computers that were needed in a botnet to achieve certain capacities which is presented as Equation (5). The simulation could only be performed for smaller botnets, due to the limitations of the resources which in this case was the actual computer that performed the simulation, which is why it is necessary to take this into account when calculating the outcome of a large-scale attack. A botnet consisting of 10 000 000 infected computers would theoretically generate a capacity of around 120 Gbit/s without considering any loss of bandwidth what so ever, which in this study only generated a capacity of 14 Gbit/s by using the given equation in this thesis. This means that the difference is of a factor 10. By looking at the graphs in section 5.6, the attack with a capacity of 14 Gbit/s would be able to succeed if the target is a small authority that has a capacity between 1 Gbit/s and 10 Gbit/s. For an attack to succeed if the target is a middle authority having a capacity between 20 Gbit/s and 50 Gbit/s, it would be needed a botnet with 35 000 000 infected computers. By the end of 2012 (see section 2.3.3.3), a botnet was reported with 22 000 000 infected computers.

This means that the Equation (5) gives a number of needed infected computers that is reliable for possible botnets. The last graph (see Figure 26) shows that the risk zone starts after 100 Gbit/s which is possible but not as likely as only a few cases of attacks between 2010 and 2013 reached over 100 Gbit/s (as highest 309 Gbit/s). Nevertheless does the final generated capacity depend on the capacity that the Internet service providers can deliver to those infected computers, which was shown to be an upload bandwidth of 24.82 Mbit/s for the year 2013 if it was connected with a fiber connection or 10.83 Mbit/s if it was connected with a copper cable connection. In the near future, attacks will increase in capacity and attacks will then have capacities of 100 Gbit/s and 300 Gbit/s and would therefore become more likely.

The survey that was sent to Swedish government authorities had a technical part which was the main aim with the survey. In section 2.3.2.1 the duration of the largest attacks was in 48% of the cases in the interval 0 hours to 6 hours, which could be because of the time it takes to manually reconfigure, reboot or simply suspend the attack. This is confirmed by the survey, where the duration from 0 to 6 hours was 60% according to the responders. The non-technical part was most to get an understanding about the situation about the work with attacks and how the authorities prepare in terms of e.g. knowledge and communication.

Regarding different types of distributed denial of service attacks it was HTTP GET, SYN, UDP and UDP Fragment attacks that was most common by the end of 2013. According to the survey, 5 of 8 knew HTTP GET, 5 of 8 knew SYN, 5 of 8 knew UDP and 4 of 8 knew UDP Fragment. Note that some authorities wrote in the comment field that they knew all of the attack types that were proposed. One interesting question was the question regarding risk analysis. All the authorities said that they perform risk analysis but none of them used ISO 31000 that is an aid for risk management. But 5 of 8 used ISO 27000 and 5 of 8 used any form of LIS, two aids for information security. The outcome of this question is interesting as in Sweden it is required by law that Swedish authorities uses ISO 27000. One important question to ask is whether they use these aids and follows the advices? About the cooperation, 8 of 8 answered that they cooperate with other authorities in terms of information exchange and 3 of 8 shared resources. Sharing resources can become, in the future, a great defense against cyberattacks as e.g. authorities can create alliances which makes it harder for an attack to succeed.

The survey included questions where the Swedish government authorities could grade different consequences based on different scenarios, which gave a clear visualization of the importance of being able to externally communicate when having vandalism and protest as a scenario. This is understandable since it could lead to difficulties in performing parts of their tasks, e.g. assisting other authorities' during an attack. But when it comes to societal threats as a scenario, the consequence of not being able to reach out to clients was the most important one. This consequence could lead to inability to inform the society, which could be harmful if it leads to e.g. panic among citizens. However, this is a problem that could be solved by having other communication channels as e.g. line-phones, radios or other media.

6.2 Ethical aspects

The suggestions of this thesis protects the integrity of citizens and employees within a state since it aims to guide Swedish government authorities to increase the capacities to a level that turns an attack to a harmless event, rather than implementing other forms of security on the Internet to avoid such attacks, e.g. monitoring systems. This leads to no need of worrying about the limitations of the system in the case of an overload. An example is if an attack would be performed with a capacity of 50 Gbit/s and the authority has a capacity of 100 Gbit/s then this would not be harmful for that authority, which would be the opposite if the authority is limited to only 10 Gbit/s.

It is a legal right to express opinions in Sweden, even if it is by showing the opinions in form of a demonstration as long as it follows the law. So by using the proposal of this thesis it would generate more difficulties for adversaries to successfully perform cyberattacks against an authority for the purpose of demonstrating. Nevertheless, this way of demonstrating is already breaking the law since it uses illegal methods to achieve the purpose which gives this thesis a higher value to be considered to avoid such cyberattacks.

Having the sensitivity of the chosen subject in mind, some ethical considerations have been made during the study. This thesis has been able to present the situation among Swedish government authorities and thereby guide them without the risk of identifying the authority or the responders.

6.3 Future work

This thesis covers a part of the guidance for authorities to evaluate their current systems given by the three graphs that shows the ability to classify the risk of not surviving an attack and the chance of surviving an attack by identifying examples of small, middle and large sized authorities (in section 5.5). This could however be further developed by letting the authorities set own values that would dynamically generate a new graph each time that shows how well the resilience is according to those input values. This could be a framework that not only Swedish government authorities could use but also organizations that want to eliminate illegal denial of service attacks by knowing the limitations of their own systems. It would also give a hint of how good the resilience would be if they invested in new technology, e.g. higher Internet bandwidth.

Other aspects as suggestions for future work is that the simulation that was made for smaller botnets could also be performed for larger botnets as well by having e.g. a distributed simulation so it does not take so long time to perform as it does with one single computer, which could have been done if the time was not so limited. And also a case study could be done in the private sector in Sweden, which would give even more understanding about increasing the resilience.

It would also be interesting to consider and study how distributed denial of service attacks will continue developing regarding the use of mobile applications on a smartphone as an attacking tool, which seems to be the next generation of attacking methods.

6.4 Final remarks

This thesis has shown that it is possible to create a framework that works as guidance for Swedish government authorities in order to increase their resilience and awareness against denial of service attacks, specifically distributed denial of service attacks. This is definitely a subject that could be further developed as a research project. Another point of view of this thesis is the cross-disciplinary collaboration between two majors that gave more value since both authors has gained knowledge in each area when helping each other.

References

[1] Skolverket, “Pressmeddelande 2013” [www], http://www.skolverket.se/press/pressmeddelanden/2013/allt-fler-datorer-i-skolan-men-stort-behov-av-kompetensutveckling-1.196645
Published 2013-04-16. Retrieved 2014-02-06.

[2] .SE (Stiftelsen för internetinfrastruktur), “Svenskarna och Internet 2011” [pdf], https://www.iis.se/docs/SOI2011.pdf
Published 2011-11-16. Retrieved 2014-02-12.

[3] IDG, “13-åring hittade säkerhetslucka hos Google” [www], http://www.idg.se/2.1085/1.545517/13-aring-hittade-sakerhetslucka-hos-google
Published 2014-02-05. Retrieved 2014-02-06.

[4] News, “Teenage hackers in Australian Federal Police’s sights” [www], http://www.news.com.au/technology/teenage-hackers-in-australian-federal-polices-sights/story-e6frfro0-1226640627727
Published 2013-05-13. Retrieved 2014-02-06.

[5] Nyheter24, “Kända svenska hackare” [www], http://nyheter24.se/nyheter/inrikes/106733-kanda-svenska-hackare
Published 2009-05-06. Retrieved 2014-02-06.

[6] G. E. Moore, “Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff.”, Solid-State Circuits Society Newsletter, IEEE, 2006, Vol. 11, pp. 33-35.

[7] S. H. Fuller, L. I. Millett, *The future of Computing Performance – Game Over or Next Level?*. Washington: The National Academies Press., 2011, ISBN 9780309159517.

[8] Spotify, “About us” [www], https://www.spotify.com/se/about-us/contact/
Established 2007. Retrieved 2014-02-07.

[9] Google Drive, “About” [www], http://www.google.com/drive/about.html
Retrieved 2014-02-07.

[10] Skatteverket, “E-tjänster” [www],
http://www.skatteverket.se/foretagorganisationer/sjalvservice/allaetjanster.4.76a43be412206334b89800031419.html
Retrieved 2014-02-07.

[11] Försäkringskassan, see “Mina sidor och självbetjäning” [www],
http://www.forsakringskassan.se/
Retrieved 2014-02-07.

[12] M. Bogdanoski, “Analysis of the SYN Flood DoS Attack”, I.J. Computer Network and Information Security, 2013, Vol. 8, pp. 1-11.

[13] The Independent, “Google chief: My fears for Generation Facebook” [www], http://www.independent.co.uk/life-style/gadgets-and-tech/news/google-chief-my-fears-for-generation-facebook-2055390.html
Published 2010-08-18. Retrieved 2014-02-12.

[14] Försvarsmakten, “Försvarsmaktens redovisning av perspektivstudien 2013” [pdf],
http://www.forsvarsmakten.se/Global/Myndighetswebbplatsen/4-Om-myndigheten/Dokumentfiler/Perspektivplan/FM2013-27612013-10-01-PERP-2013.pdf
Published 2013-10-01. Retrieved 2013-12-04.

[15] Network World, “Web attackers deface gov’t sites, steal from financials” [www], https://www.networkworld.com/news/2011/031511-web-attackers-deface-govt-sites.html?source=nww_rss
Published 2011-03-15. Retrieved 2014-02-06.

[16] MSB, “Ledningssystem för informationssäkerhet - LIS” [www],
https://www.msb.se/sv/Produkter--tjanster/Informationssakerhet---stod--verktyg/Standardisering/LIS-ISO-27000/
Published 2009-12-07. Retrieved 2014-02-06.

[17] J. Mirkovic, M. Robinson, P. Reiher, “Alliance Formation for DDoS Defense”, New Security Paradigms Workshop, 2003, pp. 11-18.

[18] C. Douligeris, A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art”, Computer Networks 44, 2004, pp. 643-666.

[19] IDG, “Studera.nu kraschade - igen” [www],
http://www.idg.se/2.1085/1.224180/studeranu-kraschade--igen
Published 2009-04-16. Retrieved 2014-02-07.

[20] The Guardian, “Russia accused of unleashing cyberwar to disable Estonia” [www],
http://www.theguardian.com/world/2007/may/17/topstories3.russia
Updated 2007-05-17. Retrieved 2014-02-12.

[21] G. Goth, “The Politics of DDoS Attacks”, IEEE Distributed Systems Online, 2007, Vol. 8, no.8, pp. 1-3.

[22] A. Kosowski, V. Mosorov, “Nessie2 Simulator for Large-Scale DDoS attack analysis”, Perspective Technologies and Methods in MEMS Design, Computer Engineering Department, Technical University of Lodz, 2011, pp. 157-159.

[23] J. Mirkovic, G. Prier, P. Reiher, “Attacking DDoS at the Source”, Network Protocols, 2002, pp. 312-321.

[24] The Wall Street Journal, “Sweden Hit by Web Attacks” [www],
http://online.wsj.com/news/articles/SB10000872396390444223104578038181717932580
Published 2012-10-05. Retrieved 2014-02-07.

[25] Försvarsmakten, “Försvarsmakten polisanmäler belastningsattack” [www],
http://www.forsvarsmakten.se/sv/aktuellt/2012/09/forsvarsmakten-polisanmaler-belastningsattack/
Published 2012-09-13. Retrieved 2014-02-07.

[26] M. E. Whitman, H. J. Mattord, *Principles of information security*, 2011, CENGAGE Learning, ISBN 9781111138219.

[27] J. Andress, *The basics of information security – understanding the fundamentals of InfoSec in theory and practice*, 2011, Syngress Media, ISBN 9781597496537.

[28] G. Dhillon, J. Backhouse, “Information system security management in the new millennium – future users of information systems must address organizational problems at a time when the organizational form is being revolutionized”, Communications of the ACM, 2000, Vol. 43, No. 7, pp. 125-128.

[29] S. Gordon, R. Ford, “Cyberterrorism?”, Computers & Security, 2002, Vol. 21, No. 7, pp. 636-647.

[30] M. M. Pollit, “Cyberterrorism - fact or fancy?”, Computer Fraud & Security, 1998, Vol. 2, pp. 8-10.

[31] Svenska datatermgruppen, “Cyberrymd” [www], http://www.datatermgruppen.se/index.php?option=com_content&view=article&id=89&Itemid=91&obj=a125&uttr=cyberrymd
Retrieved 2014-02-13.

[32] Sveriges Riksdag, “Lag (2003:148) om straff för terroristbrott” [www], http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Lag-2003148-om-straff-for-t_sfs-2003-148/?bet=2003:148
Retrieved 2014-02-27.

[33] Center of Excellence Defence Against Terrorism, *Responses to cyber terrorism*, Amsterdam, Netherlands ; Washington, DC, IOS Press., 2008, eISBN 9781607503118.

[34] Sveriges riksdag, “4 kap. 9 c §. Om brott mot frihet och frid” [www], http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Brottsbalk-1962700_sfs-1962-700/?bet=1962:700#K4
Retrieved 2014-02-27.

[35] Roland Heickero, *Informationskrig i cyberrymden - Elektronisk och digital krigföring i en breddad hotbild*, Totalförsvarets forskningsinstitut, December 2006.

[36] C. Kaufman, R. Perlman, M. Speciner, *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall, 2002. ISBN 9780130460196.

[37] C. P. Pfleeger, S. L. Pfleeger, *Security in Computing*, Prentice Hall, 2006. ISBN 9780132390774.

[38] J. Mirkovic, S. Deitrich, D. Dittrich, P. Reiher, *Internet Denial of Service: Attack and Defense Mechanisms,* 2004, Prentice Hall, ISBN 9780131475731.

[39] The Internet Engineering Task Force (IETF), "Internet Relay Chat Protocol" [www],
https://tools.ietf.org/html/rfc1459#section-1
Published 1993-05. Retrieved 2014-02-17.

[40] H. Beitollahi, G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks", 2012, Vol. 25, No 11, pp. 1312-1332.

[41] C. Timm, R. Perez, *Seven Deadliest Social Network Attacks (Syngress Seven Deadliest attacks),* Syngress Media, U.S., 2010, ISBN 9781597495455.

[42] A. Hussain, J. Heidemann, C. Papadopoulos, "A framework for classifying Denial of Service Attacks", USC/Information Sciences Institute, 2003, pp. 99-110.

[43] CERT, "Denial of Service Attacks" [www],
http://www.cert.org/historical/tech_tips/denial_of_service.cfm
Retrieved 2014-02-13.

[44] CERT, "about us" [www],
http://cert.org/about/
Retrieved 2014-02-18.

[45] CERT, *Results of the Distributed-Systems Intruder Tools Workshop,* Pittsburgh, Pennsylvania, USA, December 7, 1999.

[46] Seattle Post-Intelligencer, "Internet attack slows Web to a crawl" [www],
http://www.seattlepi.com/business/article/Internet-attack-slows-Web-to-a-crawl-5268280.php
Updated 2000-01-18. Retrieved 2014-02-27.

[47] Arbor Networks, *Worldwide Infrastructure Security Report*, 2013, Vol. 9.

[48] V. Durcekova, L. Schwartz, N. Shahmehri, “Sophisticated Denial of Service Attacks Aimed at Application Layer”, Department of Telecommunication & Multimedia, 2012, pp. 55-60.

[49] E. Damon, J. Dale, E. Laron, J. Mache, N. Land, R. Weiss, “Hands-On Denial of Service Lab Exercises Using Slowloris and RUDY”, Information Security Curriculum Development Conference, 2012, pp. 21-29.

[50] Radware, “Slowloris threat case study - Radware” [www], http://portals.radware.com/Multimedia/Security_Zone/slowloris.html?WT.ad=SlowlorisCaseStudy
Retrieved 2014-02-24.

[51] S. McGregory, ”Preparing for the next DDoS attack”, *Network Security*, 2013, Vol. 5, pp. 5-6.

[52] S. Dietrich, N. Long, D. Dittrich, “Analyzing Distributed Denial of Service Tools: The Shaft Case”, *Proceeding LISA ‘00 Proceedings of the 14th USENIX conference on System administration*, 2000, pp. 329-340.

[53] Universität Hamburg, “Distributed Denial-of-Service Tools” [www], http://www.physnet.uni-hamburg.de/physnet/security/ vulnerability/distributed_denial_of_service.html
Retrieved 2014-02-08.

[54] Sourceforge, “Anonymous-DoS” [www], http://sourceforge.net/projects/anonymous-dos/
Updated 2012-04-25. Retrieved 2014-02-28.

[55] Websecurity, “Davoset” [www], http://websecurity.com.ua/davoset/
Retrieved 2014-02-28.

[56] Darknet, “ddosim v0.2 - Application Layer DDOS Simulator” [www], http://www.darknet.org.uk/2010/11/ddosim-v0-2-application-layer-ddos-simulator/
Updated 2010-11-11. Retrieved 2014-02-28.

[57] Sourceforge, “Dereil” [www], http://sourceforge.net/projects/dereil/
Updated 2014-02-12. Retrieved 2014-02-14.

[58] Radware, “HPIC (High Orbit Ion Cannon)” [www],
http://security.radware.com/knowledge-center/DDoSPedia/hoic-high-orbit-ion-cannon/
Retrieved 2014-02-14.

[59] Sourceforge, “Hive Mind LOIC” [www],
http://sourceforge.net/projects/hivemindloic/?source=recommended
Updated 2013-04-10. Retrieved 2014-02-28.

[60] Sourceforge, “Moihack Port-Flooder” [www],
http://sourceforge.net/projects/moidosflooder/
Updated 2012-08-04. Retrieved 2014-02-28.

[61] Sourceforge, “PyLoris” [www],
http://sourceforge.net/projects/pyloris/
Updated 2012-08-26. Retrieved 2014-02-28.

[62] The hackers choice, “SSL-DoS” [www],
https://www.thc.org/thc-ssl-dos/
Updated 2011-10-24. Retrieved 2014-02-28.

[63] Packet storm, “Tor’s Hammer - Slow POST Denial Of Service Testing Tool” [www],
http://packetstormsecurity.com/files/98831/Tors-Hammer-Slow-POST-Denial-Of-Service-Testing-Tool.html
Published 2011-03-02. Retrieved 2014-02-28.

[64] Sourceforge, “XOIC” [www],
http://sourceforge.net/projects/xoic/?source=recommended
Updated 2013-12-08. Retrieved 2014-02-28.

[65] ENISA, “ENISA Threat Landscape 2013” [pdf],
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport
Published 2013-12-11. Retrieved 2014-03-03.

[66] Prolexic, “Company” [www],
http://www.prolexic.com/company.html
Retrieved 2014-03-03.

[67] Arbor Networks, “About us” [www],
http://www.arbornetworks.com/corporate/about-us
Retrieved 2014-03-03

[68] Akamai, "About" [www],
http://www.akamai.com/html/about/index.html
Retrieved 2014-03-03.

[69] Arbor Networks, "Worldwide Infrastructure Security Report", 2012, Vol. 9.

[70] Prolexic Attack Report, *Prolexic believes that attackers are changing strategies to counteract advances in DDoS mitigation practices*, Quarter 3, 2011.

[71] Prolexic Attack Report, *Prolexic believes the nature of DDoS attacks are changing: they are becoming more concentrated and damaging. Packet-per-second volume is increasing dramatically, while attack duration is declining*, Quarter 4, 2011.

[72] Prolexic Attack Report, *Financial services firms get hit by DDoS attacks as malicious packet volume increases 3.000 % quarter over quarter,* Quarter 1, 2012.

[73] Prolexic Quarterly Global DDoS Attack Report, *Application layer (layer 7) DDoS attacks decline as perpetrators attempt to maximize botnet longevity and revenue while minimizing the risk of discovery*, Quarter 2, 2012.

[74] Prolexic Quarterly Global DDoS Attack Report, *Q3 2012 was defined by extremely large DDoS attacks. It is clear that bitrates of 20 Gbps are the new norm*, Quarter 3, 2012.

[75] Prolexic Quarterly Global DDoS Attack Report, *Q4 2012 was defined by the increasing scale and diversity of DDoS Attacks as well as the enduring nature of botnets, Quarter 4, 2012.*

[76] Prolexic Quarterly Global DDoS Attack Report, *DDoS attackers target ISP and carrier router infrastructures with high packet-per-second attacks*, Quarter 1, 2013.

[77] Prolexic Quarterly Global DDoS Attack Report, *Q2 2013 saw significant increases in average DDoS attack bandwidth and packet-per-second rates,* Quarter 2, 2013.

[78] Prolexic Quarterly Global DDoS Attack Report, *DDoS perpetrators changed tactics to amplify attack sizes and hide identities*, Quarter 3, 2013.

[79] Prolexic Quarterly Global DDoS Attack Report, *Malicious actors begin using mobile applications in well-orchestrated DDoS attacks*, Quarter 4, 2013.

[80] International Organization for Standardization, "ISO/IEC 7498-1:1994" [pdf],
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=20269
Updated 1994-11-15. Retrieved 2014-03-04.

[81] D. Geer, "Malicious Bots Threaten Network Security", Computer, IEEE, 2005, Vol. 38, No. 1, pp. 18-20.

[82] K. R. Choo, "Zombies and botnets", Trends & Issues in Crime & Criminal Justice, 2007, No. 333, pp. 1-6.

[83] Kaspersky, "The economics of botnets" [pdf],
https://www.securelist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf
Published 2009-07-22. Retrieved 2014-03-05.

[84] McAfee, "The New Era of Botnets" [pdf],
http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf
Published 2013-01-23. Retrieved 2014-03-05.

[85] X. Liu, X. Yang, Y. Lu, "To Filter or To Authorize: Network-Layer DoS Defense against Multimillion-node Botnets", ACM SIGCOMM Computer Communication Review, 2008, Vol. 38, No. 4, pp. 195-206.

[86] Internet World Stats, "World Internet Usage and Population Statistics" [www],
http://www.internetworldstats.com/stats.htm
Published 2012-07-30. Retrieved 2014-03-05.

[87] Statistiska centralbyrån, "Privatpersoners användning av datorer och internet 2013" [pdf],
http://www.scb.se/Statistik/_Publikationer/LE0108_2013A01_BR_IT01BR1401.pdf
Published 2014-01-16. Retrieved 2014-03-05.

[88] McAfee, "About McAfee Security" (press the link) [www],
http://www.mcafee.com/us/#
Retrieved 2014-03-05.

[89] SANS Institute, “What is Code Red Worm?” [pdf],
http://www.sans.org/reading-room/whitepapers/malicious/code-red-worm-45
Published 2001-08-04. Retrieved 2014-03-05.

[90] C. A. Tais, “General Analysis of The Economy Behind DDoS Attacks”, Hyperion International Journal of Econophysics & New Economy, 2011, Vol. 4, No. 4, pp. 392-403.

[91] MSB, “CERT-SE - Konkurrensneutral IT-säkerhet för näringsliv och offentlig sektor” [www],
https://www.msb.se/sv/ Forebyggande/ Informationssakerhet/IT-incidenterCERT-SE/
Published 2010-09-27. Retrieved 2014-03-05.

[92] MSB, “Ny tjänst från CERT-SE visar infekterade datorer” [www],
https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nytt-informationssakerhet/Ny-tjanst-fran-CERT-SE-visar-infekterade-datorer-/
Published 2012-02-22. Retrieved 2014-03-05.

[93] CERT-SE, “Infekterade datorer i Sverige” [www],
https://cert.se/megamap/
Published 2012-05-08. Retrieved 2014-03-05.

[94] Mobile Security Threat, “Modern day DDoS attacks are using Mobile apps - Prolexic” [www],
http://www.mobilesecuritythreat.com/2014/01/16/ modern-day-ddos-attacks-are-using-mobile-apps-prolexic/
Published 2014-01-16. Retrieved 2014-03-05.

[95] S. Hamilton, “Taking Moore’s law into the next century”, IEEE, 1999, Vol. 32, No. 1, pp. 43-48.

[96] .SE, “Om .SE” [www],
https://www.iis.se/om/
Retrieved 2014-05-10.

[97] .SE, ”Frågor och svar om bredbandskollen – Vad är Bredbandskollen?”, [www]
http://www.bredbandskollen.se/faq.php?sektion=1
Retrieved 2014-05-10.

[98] .SE, *Bredbandskollen – surfhastighet i Sverige 2008 – 2013*, 2014, ver 1.

[99] S. Jindal, A. Jindal, N. Gupta, "Grouping WI-MAX, 3G and WI-FI for wireless broadband", IEEE, 2005.

[100] S-H. Chang, W-J. Liao, "A Broadband LTE/WWAN Antenna Design for Table PC", IEEE, 2012, Vol. 60, No. 9.

[101] N. Unger, O. Gough, "Life cycle considerations about optic fibre cable and copper cable systems: a case study", Elsevier ltd, 2008, Vol. 16, No. 14, pp. 1517-1525.

[102] Damballa, "Who is Damballa?" [www],
https://www.damballa.com/company/who-is-damballa/
Retrieved 2014-03-10.

[103] Damballa, "Understanding the Modern DDoS Threat" [pdf],
https://www.damballa.com/downloads/r_pubs/WP_Understanding_the_Modern_DDoS_attack.pdf
Published 2011-05-10. Retrieved 2014-03-06.

[104] E. E. Buckels, P. D. Trapnell, D. L. Paulhus, "Trolls just want to have fun", Personality and Individual Differences, *In press, Corrected Proof,* 2014.

[105] MSB, "Metodstöd för informationssäkerhet" [www],
https://www.msb.se/sv/Forebyggande/Informationssakerhet/Rad--stod/Metodstod-for-informationssakerhet/
Published 2010-02-22. Retrieved 2014-03-06.

[106] CERT-SE, "CERT-SE:s incidenthanteringsprocess" [www],
https://cert.se/incidenthantering/
Published 2012-05-09. Retrieved 2014-03-06.

[107] International standard ISO/IEC 27000, "Information technology - Security techniques - Information security management systems - overview and vocabulary", 2012.

[108] International standard ISO 31000, "Risk management - Principles and guidelines", 2009.

[109] Informationssäkerhet, "Metod för införande av LIS" [www], https://www.informationssakerhet.se/sv/Metodstod/
Published 2011-12-15. Retrieved 2014-05-23

[110] J.H.P. Eloff, L. Labuschagne, K.P. Badenhorst, "A comparative framework for risk analysis methods", ScienceDirect, 1993, Vol. 12, No. 6, pp. 597-603.

[111] T.R. Peltier, *Information security risk analysis*, Auerbach Publications, 2005, ISBN 9780849333460.

[112] A.G. Kotulic, J.G. Clark, "Why there aren't more information security research studies", ScienceDirect, 2004, Vol. 41, No. 5, pp. 597-607.

[113] S.A. Butler, "Security attribute evaluation method: a cost-benefit approach", 2002, pp. 232-240.

[114] A. Hovav, J. D'Arcy, "The impact of denial-of-service attack announcements on the market value of firms", Risk management and insurance review, 2003, Vol. 6, No. 2, pp. 97-121.

[115] T. Aven, "A unified framework for risk and vulnerability analysis covering both safety and security", Reliability Engineering & Systems Safety, 2007, Vol. 92, No. 6, pp. 745-754.

[116] R. K. Yin, *Case Study Research: Design and Methods*, Sage Publications, 1994, ISBN 9780803956636.

[117] J. W. Creswell, *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches*, third edition, Sage Publications, 2009, ISBN 9781483344669.

[118] R. Patel, B. Davidson, *Forskningsmetodikens grunder - att planera, genomföra och rapportera en undersökning*, Studentlitteratur AB, 2003, ISBN 9144022883.

[119] I. M. Holme, B. K. Solvang, *Forskningsmetodik - om kvalitativa och kvantitativa metoder*, Studentlitteratur AB, 1997, ISBN 9789144002118.

[120] Riverbed, "Network Simulation (OPNET Modeler Suite)" [www], http://www.riverbed.com/products-solutions/products/network-performance-management/network-planning-simulation/Network-Simulation.html
Retrieved 2014-03-13.

[121] A. J. Jelinek, "Use of the Cumulative Graph in Temporal Ordering", Society for American Archaeology, 1962, Vol. 28, No. 2, pp. 241-243.

[122] M. H. Kutner, C. J. Nachtsheim, J. Neter, W. Li, *Applied Linear Statistical Models*, fifth edition, McGraw Hill Higher Education, 2004, ISBN 9780071122214.

[123] D. Biau, "In Brief: Standard Deviation and Standard Error", Clinical Orthopaedics and Related Research, 2011, Vol. 469, No. 9, pp. 2661-2664.

Appendix A: Survey

Enkätundersökning

På uppdrag av Försvarsmakten arbetar vi med ett examensarbete om DDoS-attacker. För att möjliggöra verkliga scenarier i vår studie behöver vi svar från er. Syftet med detta examensarbete är att skapa en mall för att öka säkerheten för en eventuell DDoS-attack.

Delområde 1

Nuvarande situation.

Har ni blivit utsatta för någon IT-relaterad attack?

(Hot relaterat till IT-säkerhet.)

☐ JA

☐ NEJ

Hur många servrar bygger upp ert nätverk?

(Servrar som utgör myndighetens nätverk.)

☐ 1-5

☐ 6-10

☐ 11-50

☐ 51-100

☐ 101-200

☐ 201-500

☐ 500+

Hur mycket datatrafik kan servrarna maximalt hantera tillsammans?

(Beskriv datatrafiken i Gbit/s. Ex. 10 Gbit/s)

Click here to enter text.

Vilken maximal datatrafik klarar den server med minst kapacitet?

(Beskriv datatrafiken i Gbit/s)

Click here to enter text.

Vad använder ni för metoder för att bedöma er kapacitet?

Click here to enter text.

Hur många besöker er hemsida varje dag?

(Ange gärna medelantalet.)

Click here to enter text.

Hur många besökare kan ert nuvarande system hantera?

(Antag eventuella fil-anrop och anrop av diverse e-tjänster.)

Click here to enter text.

Övrig kommentar

Click here to enter text.

Delområde 2

DDoS attacker.

Har ni blivit utsatta för överbelastningar i ert nätverk?

(Någon variant av överbelastning, avsiktligt eller oavsiktligt.)

☐ JA

☐ NEJ

Om ja, vilken hastighet av attacken rapporterades?

(Ange gärna i Gbit/s)

Click here to enter text.

Om ja, hur länge varade attacken?

☐ 0-6 timmar

☐ 7-12 timmar

☐ 13-24 timmar

☐ 1-3 dagar

☐ 4-7 dagar

☐ 1-4 veckor

☐ 1+ månader

☐ Övrigt Click here to enter text.

Vilka typer av Denial of Service attacker känner ni till?

Fler alternativ är möjliga.

☐ ACK

☐ DNS

☐ HTTP GET

☐ ICMP

☐ SYN

☐ UDP

☐ UDP Fragment

☐ Chargen

☐ Känner inte till någon av ovanstående

☐ Övrigt Click here to enter text.

Övrig kommentar om DoS-attacker?

(Berätta gärna om det är något vi möjligtvis missat, som kan vara av värde.)

Click here to enter text.

Delområde 3

Konsekvenser och analys.

Utför ni riskanalyser?

☐ JA

☐ NEJ

Utför ni konsekvensanalyser givet en lyckad attack?

(Både på organisatorisk och på samhällelig nivå?)

☐ JA

☐ NEJ

Gradera följande konsekvenser ni anser vara mest kritiska givet en lyckad attack.

I fallet vandalism eller protest som syfte att förstöra:

	Inte alls viktigt	Mindre viktigt	Viktigt	Mer viktigt	Kritiskt
Information når inte ut till kunder/andra besökare.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbetet förhindras internt.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbete med externa parter försvåras.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					

I fallet hot mot samhället:

	Inte alls viktigt	Mindre viktigt	Viktigt	Mer viktigt	Kritiskt
Information når inte ut till kunder/andra besökare.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbetet förhindras internt.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbete med externa parter försvåras.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					

I fallet "okänt" syfte av attacken (ex. oavsiktlig överbelastning):

Ange alternativt scenario, om sådan finns:

Click here to enter text.

	Inte alls viktigt	Mindre viktigt	Viktigt	Mer viktigt	Kritiskt
Information når inte ut till kunder/andra besökare.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbetet förhindras internt.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					
Arbete med externa parter försvåras.	☐	☐	☐	☐	☐
Denna konsekvens leder till (utgå från samhällskostnader, tidslängd och att samhällskritiska funktioner slås ut): Click here to enter text.					

Delområde 4

Dokumentation och kommunikation.

Baserar ni säkerhetsarbetet på någon/några standarder?

(Någon standardisering?) Fler alternativ är möjliga.

☐ ISO 27000

☐ ISO 31000

☐ Någon form av LIS (Ledningssystem för informationssäkerhet) baserat på ISO 27000

☐ Övrigt Click here to enter text.

☐ Inget av ovanstående

Har ni en handlingsplan om ett angrepp skulle ske?

☐ JA
☐ NEJ

Rapporterar ni varje IT-incident?

(Intern (tillsäkerhetschef inom myndigheten), externt (involverar extern part, ex. polismyndigheten))

Fler alternativ är möjliga.

☐ Ja, både internt och externt

☐ Ja, endast internt

☐ Ja, endast externt

☐ Nej

☐ Övrigt Click here to enter text.

Hur uppdaterar ni medarbetare om IT-relaterade hot?

(Ex. informerar om nya varianter av hot.) Fler alternativ är möjliga.

☐ Seminarier

☐ Rapporter (veckovis eller månadsvis)

☐ Möten

☐ Workshops

☐ Behöver inte uppdatera medarbetare

☐ Övrigt Click here to enter text.

Övrig kommentar.

Click here to enter text.

Delområde 5

Samarbete.

Samarbetar ni med andra svenska myndigheter?

☐ JA
☐ NEJ

Om ja, vilken typ av samarbete?

(Hur samarbetar ni?) Fler alternativ är möjliga.

☐ Informationsbyte

☐ Delar resurser, ex. nätverk, CPU, servrar, etc.

☐ Reservkapacitet vid avbrott

☐ Övrigt Click here to enter text.

Outsourcar ni delar av eller hela er IT-drift?

(Till annan myndighet/företag)

☐ JA
☐ NEJ

Om ja, ställer ni krav på hantering av IT-incidenter?

(Ex. krav på att leverantören har en kontinuitetsplan, täcker planen de krav myndigheten har som tillgänglighet, riktighet, sekretess och spårbarhet.)

☐ JA
☐ NEJ

Övrig kommentar

Click here to enter text.

Appendix B: The upload history of Swedish Internet service providers

Values are presented as Mbit/s.

Operatör och teknik 2008-2013

Operatör	Teknik	2008	2009	2010	2011	2012	2013
AllTele	3G/4G					16,6	18,1
AllTele	DSL			3,8	2,9	2,5	3,0
AllTele	fiber	12,9	25,6	30,7	29,3	31,1	31,9
AllTele	kabel-tv				9,8	10,7	10,4
Bahnhof	DSL		5,1	3,0	2,6	4,1	4,1
Bahnhof	fiber	23,9	26,2	26,5	27,1	28,4	33,0
Bahnhof	kabel-tv		14,7	13,7	10,1	12,9	14,3
Bredband2	DSL			6,8	6,6	6,7	11,0
Bredband2	fiber			27,4	27,2	27,7	36,2
Bredband2	kabel-tv			14,3	6,9	11,0	12,1
Bredbandsbolaget	DSL	1,3	1,2	1,3	1,3	1,3	1,5
Bredbandsbolaget	fiber	13,9	15,2	14,6	13,9	17,2	25,0
Bredbandsbolaget	kabel-tv	6,3	6,8	2,5			
Com Hem	fiber	2,4	5,5	7,2		11,0	16,1
Com Hem	kabel-tv	2,8	5,1	5,2	5,9	6,8	8,5
Hi3G	3G/4G	0,3	0,4	0,8	1,2	1,6	3,1
Netett	3G/4G				0,5	0,7	0,8
Tele2	3G/4G		0,4	1,0	1,3	3,2	5,4
Tele2	DSL		0,9	1,2	1,2	1,7	2,1
Tele2	fiber		13,0	15,1	16,7	18,9	20,9
Tele2	kabel-tv		2,1	5,8	6,6	6,9	8,8
Telenor	3G/4G	0,3	0,3	0,9	1,3	3,6	4,6
TeliaSonera	3G/4G	0,4	0,6	1,3	1,8	3,2	4,6
TeliaSonera	DSL	0,9	0,9	1,0	1,2	1,7	2,0
TeliaSonera	fiber	11,7	16,0	15,6	15,3	19,7	28,7
TeliaSonera	kabel-tv	2,4	4,2	2,3	6,4	8,3	10,9