Tallinn University

Institute of Informatics

Cyber Security in Estonia:
Lessons from the Year 2007 Cyberattack

Master Thesis

Katri Lindau

Author	Supervisor	Head of the Institute
Katri Lindau 3rd of May, 2012	Isaias Barreto da Rosa 3rd of May, 2012	Peeter Normak 3rd of May, 2012
(name, date and signature)	(name, date and signature)	(name, date and signature)

Tallinn
May 2012

Author’s declaration

I declare that this thesis entitled “Cyber Security in Estonia: Lessons of the Year 2007 Cyberattack” apart from work whose authors are clearly acknowledged, this document is the result of my own and original work. This thesis has not been accepted for any degree and is not submitted for any other comparable academic award.

This thesis was completed under the supervision of Isaias Barreto da Rosa on 3rd of May, 2012.

Abstract

Estonia has implemented many different e-solutions in public use including paper-free e-government. While being a leading and an advanced e-society there were no big concerns about cyber security. It all changed after cyberattacks in April and May 2007.

For two-month period Estonian governmental web pages as well as banks and media corporate websites were under virtual attack. After that frightening event the cyber security became an important issue which gained much attention. Now Estonia is a leading country not only because of its well-developed ICT infrastructure and wide range of e-solutions but also in cyber security issues.

This study focuses on cyber security in Estonia; with analyzes of what have changed in Estonia’s cyber security after the cyberattack in 2007 and what the main obstacles to deal with.

Keywords: cyberattack, cyber terrorism, cyber security, network security, computer security, cybercrime

Table of contents

List of tables

List of figures

Chapter 1. Introduction

In introduction author outlines the rationale for this research. It gives the context in which this research is positioned by providing background information that leads to the discussion of the research problem. The statement of the problem is to understand the changes in Estonian cyber security after the cyberattack in 2007. The objectives, research questions and the methodology used in this study are then discussed.

Background information

Computers used as cyber warfare can be significant for the future. Author believes that using computers and the internet in carrying out operations against the country as since now aside the conventional warfare will be growing area. Despite the fact that areas affected are physical, but the computers and internet are virtual, they also affect the real areas of a country (for example economy, communication, infra structures, etc.) in many ways.

After relocation of a Soviet-era statue known as Bronze soldier from intersection in central Tallinn to a nearby military cemetery in Tallinn in April of 2007 Estonia fell under a politically motivated (Ottis 2008) cyberattack between 27 April and 18 May of 2007. Attack lasted twenty-two days. Among the targets were Estonian governmental agencies and services, schools, banks, Internet Service Providers (ISPs), as well as media channels and private web sites (Evron 2008; Tikk, Kaska, and Vihul 2010 via Ottis 2008). Estonia’s main defense was to close down the sites under attack to foreign internet addresses in order to try to keep them accessible to domestic users.

Mägi and Vitsut (2008: 89) have pointed out that before Estonia’s case similar attacks have been classified as hooliganism, criminal or nationalistic. Hooliganism in case which is coordinated by individuals who create or use viruses or break into secured system and they consider their own action like an innocent joke. Criminal in case if the attack is carried out by profit-motivated individuals or group. Nationalistic if the attack is motivated by national or patriotic feelings what are based as a response to against certain institutions’ action and the attack itself is not identified by another state led or initiated, but favored or tolerated. Mägi and Vitsut also say that in Estonia’s case there are clear signs of a nationalist attack, but in world it is special because of the attack’s range, variety and the diversity of targets and clear visible links to the orientation against Estonia which is the reason why those attacks attracted the attention of many worldwide cyber security professionals.

After the attack a number of measures were implemented and Estonia is now the leading European Union country in terms of cyber security. Estonia now hosts the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) and in 2012 the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice will be established in Tallinn, Estonia.

Understanding Estonia’s major learnings from the 2007 attacks and how they are implemented and the procedures that were followed in this process might be very useful to other countries to support creating framing of cyber security policies.

Statement of the problem

The focus of this study is to structure the situation in topic of cyber security in Estonia before the cyberattack in year 2007 and to describe the dynamics of changes after. After the 2007 the developments fastened at the area of cyber security – many frameworks were implemented and organizations created in order to develop the field of cyber security in Estonia.

Aims and objectives

The aim of this thesis is to study and understand the major cyber security policies, practices, changes and learnings at Estonian Government level after 2007.

The key objectives are:

- Understand the key concepts related to cyber security and its infrastructure.
- Understand the specificities on the 2007 cyberattack at Estonian ICT infrastructure.
- Analyze the major cyber security issues at Estonian Government level before and after the attack.
- Understand the learnings and changes at Estonian Government cyber security policies and practices after the 2007 attack.

Research questions

The central questions in this study are:

1. What are the major lessons learnt at Estonian Government level after cyberattack in 2007?
2. What were the practices implemented after attacks in 2007?

Methodology

This study's aim is to understand the changes in Estonia after cyberattack against the government, banks and media concerns in April and May 2007. In order to archive the aim of this study author analyzes available documents and carries out interviews with experts in the field of cyber security in Estonia in order to analyze the changes of cyber security in Estonia after cyberattack in 2007. Then the triangulation method is used to analyze and represent the results of this study.

The analysis of this study is made based on available documents by institutions which deal with the cyber security in Estonia. For example Estonia's Cyber Security Strategy for 2008-2013 and different other policies which were submitted by the Government of Estonia in order to support the development of the secure information society.

Qualitative expert interview methodology (Laherand 2008) was used to conduct interviews. Author decided to use this method because this method allows finding answers to the research questions through experts' experiences and thoughts. Qualitative expert interview methodology is used in social research for expressing the opinion of experts' working at the same field; it stands to be adequate for this works. Also, in order to describe what happened during the attack in 2007 and to point out what were the main problems, the view of experts' is necessary.

Four interviews were carried out. One interview was carried out in English while three in Estonian. The choice of experts was based on the principle to include the security experts and cyber security policy-makers in Estonia. The profile of experts has been explained on following Table 1.

Table 1 – Experts profile.

Name	**Current position**
Agu Kivimägi	Head of Cyber security at IT and Development Centre. Ministry of the Interior, Estonia.
Jüri Kivimaa	Currently a scientist at CCD COE. Formerly information security expert at SEB Estonia.
Rain Ottis	Currently a scientist / senior analyst at CCD COE. Formerly Chief of Cyber Defence Section, Estonian Defence Forces Training and Development Centre for Communication and Information Systems (EDF TDCCIS), Estonian National Defence College (ENDC).
Jaan Priisalu	Director General at Estonian Information System's Authority. Formerly Head of IT Risk Management at Swedbank.

The summaries of interviews are presented in this study in summary form as well as quotations (in italics in the text). Interview plan in English and Estonian and transcriptions of the interviews are added in appendix of this study.

Analyzed state-level frameworks in comparison with the opinion of experts working in the area of cyber security is giving the needed understanding what are the main developments in the area which affect establishing cyber security. In Bryman's opinion triangulation (2006) enables a qualitative analysis. Triangulation produces a result in which the sum of the whole is greater than its parts. Author believes that by combining documents and experts' opinions the analyses of this study has the reliability and validity in order to achieve the intended results and to provide the confirmation of the outcome of this study.

Significance of the study

After relocation of a Soviet-era statue known as Bronze soldier from intersection in central Tallinn to a nearby military cemetery in Tallinn in April of 2007 Estonia fell under a politically motivated (Ottis 2008) cyberattack between 27 April and 18 May of 2007. This attack is considered as the first known such kind of an assault against a country.

After the attack a number of measures were implemented by Estonian Government and Estonia is now a leading European Union member in terms of cyber security. Understanding the major learnings from the 2007 attack, the changes that were implemented and the procedures that were followed in this progress, might be very useful to other countries to acknowledge the cyber threat, raise the awareness and take appropriate action planning into work.

Outline of the thesis

The introduction of this thesis provides background information which frames the work as a whole. The research problem, the objectives and research questions of the study are stated.

The first chapter reviews the literature that is relevant to the topic and gives an overview in terms of cyber risk, attacker classification, attacker's motivation, cyber defense and the importance of international cooperation in order to develop secure cyber world.

The second chapter comprises the data analysis and main findings. Chapter explores the findings accordingly objectives set.

The learnings and conclusions from this study are presented in last part of the thesis. Also in Conclusion part is presented suggestions for areas of further research.

Summary

This introductory chapter has provided background information to this research and discussed the initial reasons for the study. The research problem has been presented and the methodology used in order to archive the results, which are set to this study, has been described. The following chapter reviews the background information related to this study.

Chapter 2. Cyber risk

This chapter presents an overview of cyber threat's nature and its increasing importance to modern times.

1 Nature of cyber risk

Our world is already network-based. The stability of our networked global system and the proper functioning of our countries, cities and daily activities, rely on the Internet. Critical infrastructure including transport, transport security, nuclear power plants, electricity, and communication networks are with potentially devastating consequences for humankind. Cyber risk in by nature an invasive, multi-pronged and multi-layered threat, without visible weapons or attributable actors, characterized by an escalating number of attacks both on and off the radar. (Stauffacher, Sibilia & Weekes 2001)

As every progress and development offers positive opportunities, there are always criminal minds that will use this to their advantage.

This master thesis focuses on cyber security aspects in government and its institutions. Dependency on the networks is the evidence of state's innovative mind, but it also means that there is new a type of threat that should be understood and considered. More different cyber ecosystems lead us to stronger reliance on different information and communications technology (ICT) which can mean catastrophic consequences if it is under attack.

For now, most cyberattacks do not directly target lives, but the organized vandalism of cyberattacks could be serious if it prevents a society from meeting basic needs like providing food. (Lin, Allhoff & Rowe 2012)

Same aspects are stressed out by European law enforcement agency Europol. Accordingly to Europol in recent years the internet has considerably facilitated communication and promoted global development and interaction. At the same time, new, modern challenges have emerged in the form of cybercrime as criminal groups exploit these technological advantages. Still the biggest security threats to the internal European Union come from terrorism, international drug trafficking and money laundering, organized fraud, counterfeiting of the euro currency and people smuggling, but new threats like cybercrime with trafficking in human beings and other modern-day dangers are rising. Europol admitted in 2011 that the value of the cybercriminal economy as a whole is not known, but estimates global corporate losses alone at around 750 billion Euros per year. (Europol Public Information 2011)

Europol brings out that European Union is clearly an attractive target for cybercrime because of its advanced Internet infrastructure, rates of adoption and increasingly Internet-mediated economies and payment systems. (Europol Public Information 2011)

In 2008 Suleyman Anil, head of NATO Computer Incident Response Capability Co-ordination Centre, warned that computer-based terrorism poses the same threat to national security as a missile attack. The determined cyberattack on a country’s online infrastructure would be “practically impossible to stop” he said. (Heath 2008)

International Institute for Strategic Studies (ISS) in England announced that cyber warfare “is growing threat” in the beginning of year 2010. IISS director-general John Chipman even said: “Despite evidence of cyberattacks in recent political conflicts, there is little appreciation internationally of how to assess cyber-conflict”. He compares the problem of cyber-warfare to the 1950s problem with possible nuclear war. (Tisdall 2010)

Comparison of missile attack and cyber terrorism may seem overwhelming, but not if we give a thought of potential threats and results of attack. At first sight cyber terrorism causes inconvenience or financial loss. E-mail spam, hacked or down websites or credit cards does not seem like real terrorism acts. But after some serious attack against bank’s systems bank could close down any traffic in accounts. That means no money moving between accounts of individuals and companies as well as national. This means highway to panic on streets – without ability to access their money people would not have the opportunity to satisfy immediate needs – buy food, fuel, etc.

In conventional warfare comparing cyber war it is easier to bring out certain evidence - at least we can understand that this is a war. This almost philosophical question is still unanswered – when do we name and treat the action as an attack?

2 Characters of cyberattacks

2.1 Definition

Howard & Longstaff (1998) define an attack as a series of steps taken by an attacker to achieve an unauthorized result. Unauthorized means that this is not approved by the owner or administrator (and authorized means that this is approved by the owner or administrator).

2.2 Nature of attack

Cyber threats are the response to the weaknesses and vulnerabilities in the system. It is commonly mentioned by researchers (Johnson, 2010; Brunette & Mogull, 2009; Greene, 2006; Whitman & Mattord, 2004) that cyber security as information security in particular involves three core principles:

- Confidentiality – protecting;
- Integrity – maintaining;
- Availability - ensuring.

On the other side there is system vulnerability and therefore threats (Gelbstein & Kamal 2002) because of those three core principles outlined before.

Typically, those three core principles are distracted by accordingly to Rufi (2006):

- Misconfigured hardware or software;
- Poor network design;
- Inherent technology weaknesses;
- End-user carelessness;
- Intentional end-user acts.

It is important to knowledge that all those threats can be identified and therefore taken into consideration to minimize the risk, but the risk can never be abolished.

Thuraisingham (2005) divides general cyber threats into seven groups:

- Authentication violations – for example steeling passwords could be a result in authentication violations;
- Nonrepudiation – hiding the sender of an e-mail or hiding accessing to the webpage;
- Trojan horses and viruses – using malicious programs to cause different damage;
- Sabotage;
- Fraud – for example using bank accounts information to steal money;
- Denial of service and infrastructure attacks – for example attacking telecommunication system, power system, heating system, etc.;
- Natural disasters – computers are also vulnerable to natural disasters and no human attack needed for damage.

Cyberspace offers new opportunities for warfare as the virtual environment offers to create an environment to affect the ‘real’ world. Lin, Allhoff, Rowe (2012) point out that cyberspace is more attractive than conventional military actions that require the expense and risk of transporting equipment and deploying troops in enemy territory, not to mention the political risk. Also cyber weapons could be used to attack anonymously at a distance while still causing much mayhem. Targets rank from banks to media to military organizations. It is essential to understand that actually no one connected to the Web, previously connected to the Web or using software in any process is completely immune to the cyberattack.

Problem with cyberattackers includes three major issues. Firstly, Internet environment is anonymous and secondly cross-border nature makes it hard to track and investigate the attack.

According to Lipson (2002) the Internet was never designed for tracking and tracing user behavior which is the reason why tracking and tracing attackers is an extremely difficult task. Secondly, the Internet was designed on the robust way to make it resistant to external physical attack or accident, but there was no equivalent concern with regard to the possibility of internal cyberattacks by the Internet's own users. A packet's source address (IP address) is untrustworthy because an advanced user can modify it and therefore hide its true origin. Other way is to examine is to compromise a number of intermediate hosts and to then use them as stepping stones on the way to the final target which is more effective way to trace down the attacker, but attacker can arrange things so that the packets could be mixed and tracing will fail.

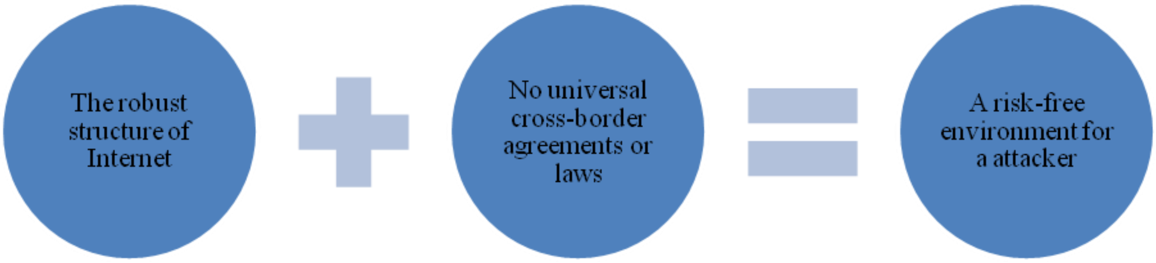

The robust structure of Internet
No universal cross-border agreements or laws
A risk-free environment for a attacker

Figure 1 – Internet's structure and lacking in laws creates risk-free environment for attackers. Adapted from Lipson (2002).

Consequently, as the attacker is anonymous, it is from difficult to impossible to determine the attacker which makes the attack itself risk-free for the attacker. If usual attack activities produce the risk of counter-attack, then because of anonymous nature of cyberattacks this method is rather secure for attacker.

Third important aspect of cyberattacks Lipson (2002) brings out is that attacks often cross multiple administrative, jurisdictional and national boundaries and there are no universal technical standards or agreements for performing the monitoring and record keeping necessary to track and attacks. There also are not universal laws or agreements for to track the attacks. Cross-border nature makes it hard to track and investigate. Also, as cyberattacks can be committed from a long geographical distance, it does not require any travelling from the attacker, attack can be committed from anywhere to everywhere.

All these aspects make cyberattack not so demanding for financial resource, but possible value of damage and therefore profits can be huge. Also, attack can be carried out easily and it does not require much resources and skills which makes it even more attractive to criminal minds.

Attack methods

Attack methods can be considered as a response to information and network vulnerabilities. It is important to notice that vulnerabilities are not only cyber systems lacking of security, but also devices itself such as computers, routers, servers, switches, etc.

Rufi (2006) divides attacks into four primary classes:

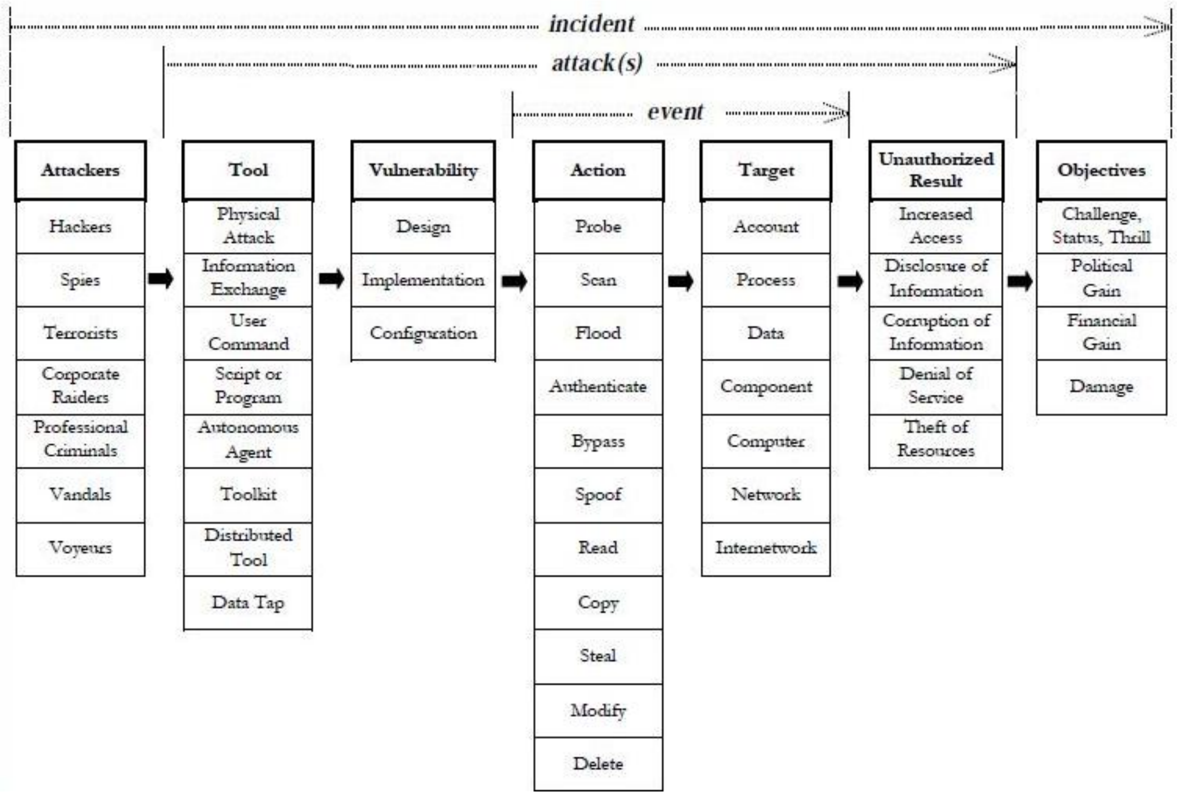
- Reconnaissance – an unauthorized discovery and mapping of systems, services, vulnerabilities; gathering of information;
    - Packet sniffers
    - Port scans
    - Ping sweeps
    - Internet information queries
- Access – an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password;
    - Password attacks
    - Trust exploitation
    - Port redirection
    - Man-in-the-middle attacks
    - Social engineering
    - Phishing
- Denial of service (DoS) – disabling or corrupting networks, systems, services with the intent to deny services to intended users; also crashing or slowing down the system; also deleting or corrupting information;
    - Ping of death

    - Masquerade/IP Spoofing attacks
    - Distributed Denial-of-Service attacks (DDoS)
- Malicious code – damaging, corrupting the system; forcing the system to replicate itself, denying services and/or access to networks, systems, services; copying of information and echoing it to other systems.
    - Trojan horse
    - Worm
    - Virus

Kumar, Srivastava and Lazarević (2005) classify computer attacks and intrusions according to the attack type as following:

- Denial of Service (DoS) attacks:
    - Operating system attacks – targeted on specific operating systems,
    - Networking attacks – creates limitations to networking protocols and infrastructures;
- Probing (surveillance, scanning) – collecting information about IP addresses;
- Compromises – for example buffer overflows, breaking into the system, gaining privileged access to hosts:
    - R2L (Remote to Local) attacks – for example gaining access to a computer without permission via internet,
    - U2R (User to Root) attacks – attacker has an account on a computer system misuses or elevates existing user privileges by exploiting a vulnerabiligy.

Howard and Longstaff (1998) for example have developed the full incident taxonomy to show relationship between attackers, tools, vulnerability, actions, targets, unauthorized results and objectives (see Figure 2).



Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

Figure 2 – Computer and Network Incident Taxonomy. (Howard & Longstaff 1998)

Howard and Longstaff (1998) defined the incident as „a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites and timing“. They see the attack as a series of events which may be multiple actions against target(s).

Attacker's motivations

There are slightly different approaches to classifications of attackers. Mainly the classifications are made considering motivation of an attacker.

Author believes that the abundance of motivators shows that the motivation for the attack might not be a single aspect, but rather complex of more. Different approaches are not always strictly comparable as motivators are approached from different aspects. Still author believes that acknowledging them all helps to understand the dynamics' of attacker's motivations.

Leeson and Coyne (2005) divide the community of hackers into three classes separated by motivation – “good” hackers, fame-driven hackers and “greedy” hackers. “Good” hackers are the ones who illegally break into computer systems, but voluntary share security weaknesses with those in charge of these systems. Fame-driven hackers are unethical and seek infamy and break into the electronically stored information of vulnerable parties and wreak havoc. “Greedy” hackers are motivated by profits. Leeson and Coyne point out that profit-driven hacker can be “good” or “bad” depending upon which type of behavior yields the greatest monetary return. This approach is economy-based and suites if the consideration is about economical damage of cyberattacker.

Jayawickrama (2008) points out that cybercrime are driven by same motivations as conventional crime:

- Economic benefits – personal and/or organizational financial gains,
- Power – desire to impact large systems and organizations,
- Revenge – desire to inflict loss or damage,
- Adventure – challenge of mastering complex systems,
- Ideology – desire to express,
- Lust – self gratification.

Jayawickrama’s point of view is that stays crime in “old” world as the same as in “virtual” or “cyber” world. On cybercrime it is not the act itself which is new, but the environment in what the crime is committed.

Mägi and Vitsut (2008) classify cyberattacks into three:

- Hooliganism – attack is coordinated by individuals who create or use viruses or break into secured system. They consider the attack as an innocent joke.
- Criminal – attack is carried out by profit-motivated individuals or group.
- Nationalistic – attack is motivated by national or patriotic feelings as a response to certain institutions action. Attacker is not launched or operated by another state, but is clearly favored or tolerated by another state.

They do not consider in this classification of cyberattacks state sponsored or managed attacks, but Mägi and Vitsut (2008) do consider cyberspace and information technology as information warfare – the manipulation of others and protection of own information-based processes, information systems and computer infrastructure to gain information superiority.

Gandhi, Sharma, Mahoney, Sousan, Zhu and Laplante (2011) approach give dimensional approach to cyberattacks dividing them into four groups by motivations – social, political, economic and cultural. It is worth to note that it is difficult to separate social and cultural motivators. Political factors are protest on political or government actions, dissatisfactions against the launch of a public document, policy or law, retaliation against acts of aggression of physical attacks, also cyber espionage. Economic factors are financial gain, economic recession and greed. Socio-Cultural factors are land and cultural disputes and anniversaries of historic events.

Of course, those factors are the basic; there certainly are variations of these. As seen on the following figure 3 from Gandhi, Sharma, Mahoney, Sousan, Zhu and Laplante, dimensions cross each other and it is often difficult to classify the cyberattack only by one motivator. In fact, it is complicate to find pure example of sociologically or culturally motivated attacker because these two motivators are closely connected to each other.

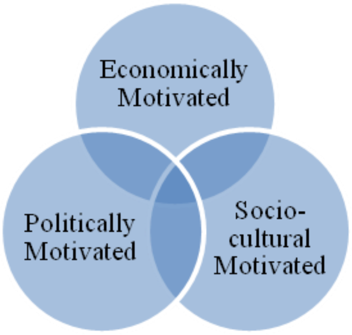


Figure 3 – The distribution of cyberattacks across CSEP dimensions. (Gandhi, Sharma, Mahoney, Sousan, Zhu & Laplante 2011)

On following Figure 4 is represented the author's figure to summarize the attacker's motivations mentioned by previously represented approaches – Mägi and Vitsut's classification and CSEP dimensions from Gandhi, Sharma, Mahoney, Sousan, Zhu and Laplante.

Attackers are divided into three groups - hooligans, criminals and state-driven attackers - with subgroup of terrorists in group of criminals. All these groups are influenced by different aspects of social, cultural, economical and political issues.

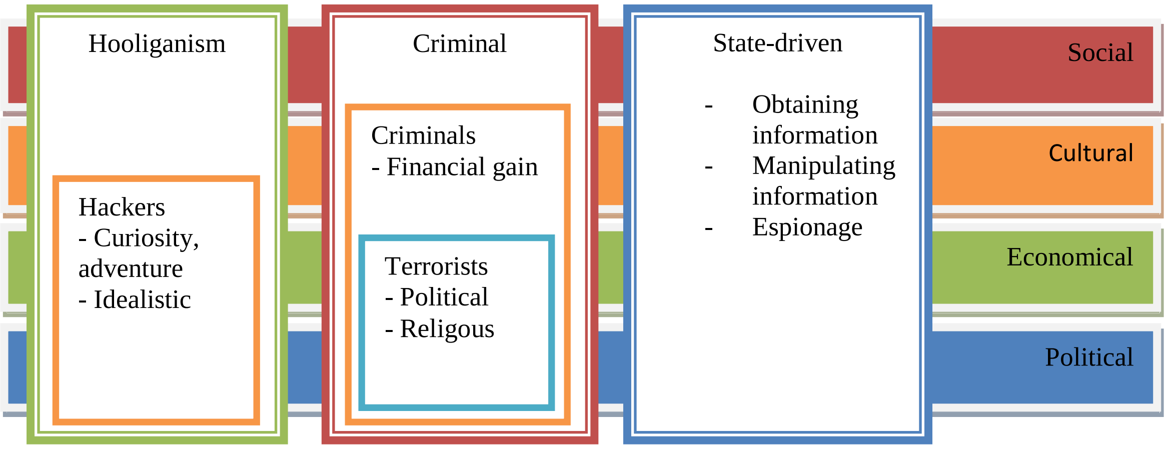


Figure 4 – Classification of cyberattacks by motivations.

Weimann (2004) brings out Denning's (2000) definition for cyberterrorism:

> *Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate of coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*

Weimann also stresses out that it is important to distinguish between cyberterrorism and hacktivism (hacking tied with political motivations). Even politically motivated, hacktivism does not amount to cyberterrorism. The difference is notable when understand that hacktivists do want to protest and disrupt; they do not want to kill or maim or terrify. But Weimann also admits that the line may sometimes be blurring, especially if hacktivists are acting for terrorists consciously or not.

3 Cyber defence

3.1 Development of the threat

As seen on Figure 5 where is shown statistics of total vulnerabilities cataloged during 1995 until the 2008 (quarters 1-3) to Computer Emergency Response Team/Coordination Center (CERT/CC), the number of vulnerabilities started rise rapidly in years 1999 and 2000 and have multiplied since then.

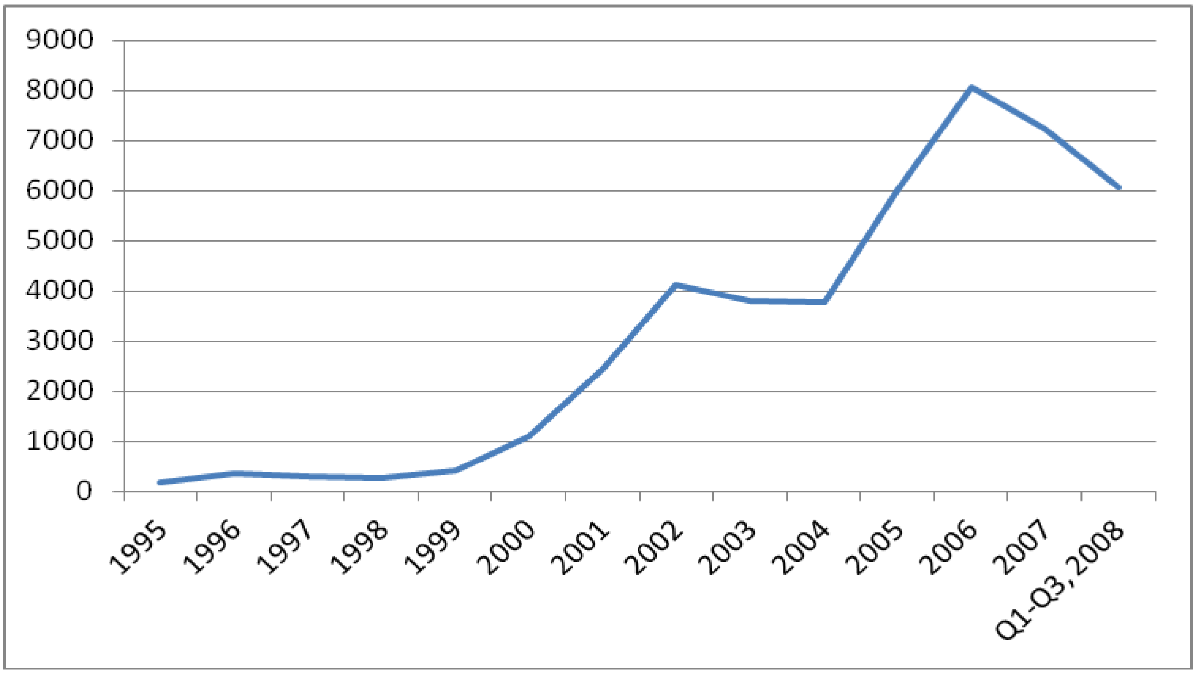


Figure 5 – Total vulnerabilities cataloged by CERT/CC during the period 1995 - Q1-Q3, 2008.

Mikko Hypponen, the Chief Research Officer for F-Secure, provided a review (2012) in NATO Review magazine of security predictions which focuses on crime, computers and security in 2012. In this review Hypponen states that there will be more attacks by criminals and also by hactivists. Today's malicious software is not written by hobbyist hackers anymore, but by professional criminals who are making money with their attacks. In the review Hyppionen also says that the international community has failed to address the real nature and extent of the problem, action against online criminals is often too slow, the arrests few, penalties are often very light. This is the reason why according to review online crime is continuing to grow rapidly; potentially large profits and the relatively limited risk of getting caught and punished have encouraged the development of criminal economy in internet.

In order to describe the threat development, Rattray (2010) have constructed phases to describe evolving threats presented on Figure 6. Accordingly to Rattray, hacker phase started at 1986 and includes writing viruses of curiosity. Firewalls, software patching and correctly configured servers and computers can protect information from attackers. In early 2000s begun the criminal/commercial phase which means using backdoors, keyloggers, spyware, adware, botnets, etc. Attacks are more persistent with sophisticated malware. In mid 2000s begun advanced, dedicated phase when well resourced efforts are targeting at intellectual property and network use. In this third phase is important to notice that attacks are hard to find and can continue activity even when discovered. All phases are continuous in time.

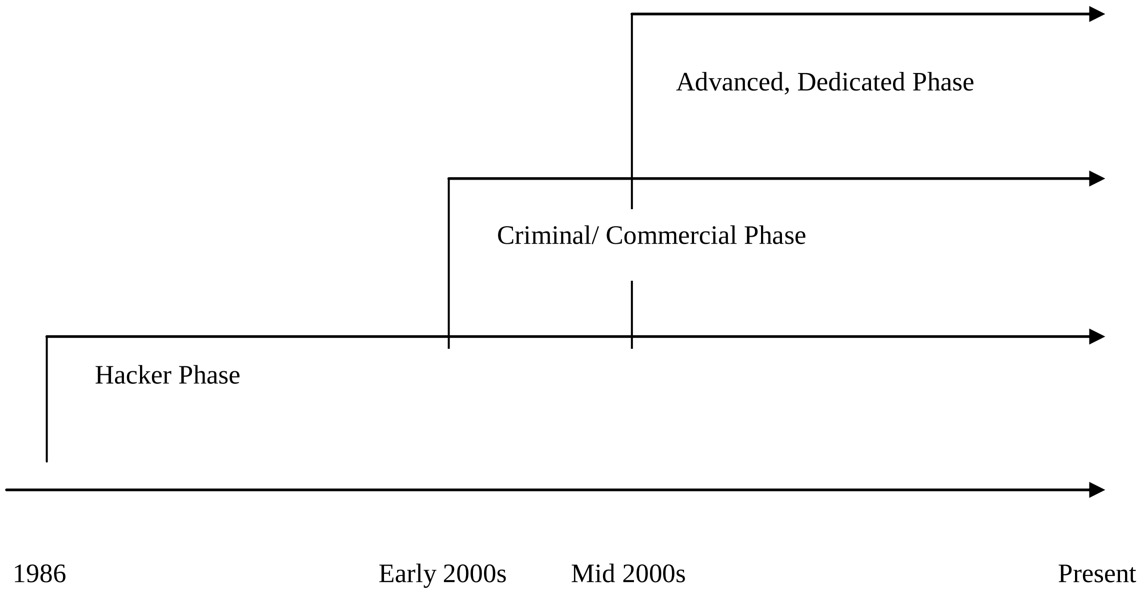


Figure 6 – Evolving threats in the Ecosystem. (Rattray 2010).

To illustrate the development of attackers and used methods, Rattray uses a figure, presented on Figure 7 below, where is shown how attackers' skill level is increasing at the same time while attack sophistication is decreasing. Attackers can do now more damage needing less. According to Rattray as in early 1990s attacks were conducted by amateurs and perhaps benevolent hackers, attacks got more threading in early 2000s when there raised new money-motivated criminal and commercial phase attackers to advanced and dedicated phase starting in mid 2000s.

.

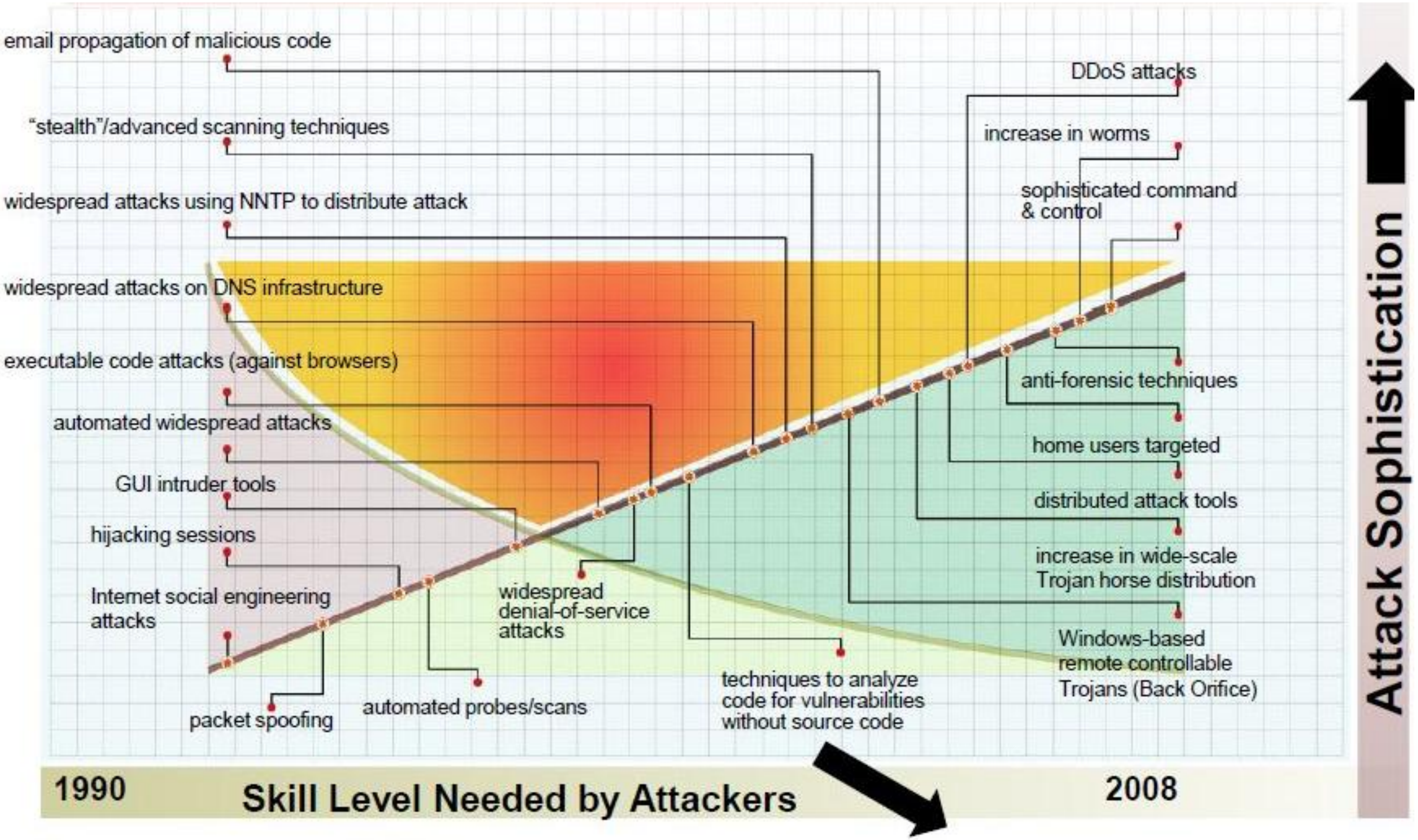


Figure 7 – Attacks are easy to conduct (SE/CERT CC (2008) via Rattray).

3.2 Cross-border cooperation

As attacks evolve more sophisticated, there is growing need for cross-border cooperation in order to maintain the security and fight with cyberattackers. Stauffacher, Sibilia and Weekes (2011) have brought out that like with many cross-border and cross-cutting issues in today’s world, thinking and action should focus on a multi-stakeholder, multi-layered patchwork of interconnected solutions, overlaid by an international code and/or additions to existing international agreements and treaties which could be acceptable for most parties. They say that all countries need to examine and assess the need for modifying existing laws to address cyber-specific issues. They also underlined that while cyber-security is critical, and the rights of the citizen and user to live and operate in a safe environment is of the utmost importance, any solution should not diminish the freedom of the Internet, or impede the hugely enriching role it has in our society.

Ghernaouti-Hélie (2011) pointed out that for every country that is reducing the digital divide through investment in infrastructure only, without taking into account the need for security and control of ICT risks as unsolicited incident, malevolent acts, etc., would result in the creation of an unsafe environment for its citizens. He says that it should be imperative that developing countries not only introduce measures to fight against cybercrime, but also control the security of their infrastructure and information technologies departments. According to Ghernaouti-Hélie it is important to acknowledge cybercrime and cyber security challenges, its economic and management issues, political issues, social issues, technical issues, legal and law enforcement issues; it is crucial to create effective cybercrime laws that are enforceable at national and international levels taking into account the right to privacy.

Same is outlined in Center for Strategic and International Studies (CSIS) Commission on Science and Security’s report (2002) on cyber security where is stressed out that cyber security is the collection of administrative tools, authorization processes, vulnerability scanning, intrusion detection, maintenance verification, and other tools and techniques used to protecting information systems. It also is also a set of rules, protocols, and procedures that guide system designers, system administrators, and everyday users. Additionally, cyber security is the integration of numerous information systems and protection schemes across a network of similar and disparate, but interconnected systems.

Perhaps most significant milestone in history of securing the internet is the establishment of Computer Emergency Response Team Coordination Center (CERT/CC) by Defence Advanced Research Projects Agency (DARPA) at Carnegie Mellon University's Software Engineering Institute in 1988 as a response to Internet Worm incident. As Howard and Longstaff (1998: 1-2) has noted the aim of CERT was to provide the Internet community a single organization that can coordinate responses to security. Since then, the CERT/CC is responsible for Internet-related incident response. As Internet is now diverse, CERT/CC have established a variety of computer security incident response teams with specific constituencies, such as geographic regions or various government, commercial and academic organizations.

Schjolberg (2007) brings out that international and also regional organizations have taken the lead in harmonizing national legislation on cybercrimes – experts and specialists of United Nations, United Nations Office on Drugs and Crime (UNODC), International Telecommunication Union (ITU), The Council of Europe, G8 Group of States, European Union, Asian Pacific Economic Cooperation (APEC) and Organization of American States (OAS) for example are designing global framework on cybercrime including terrorism.

The 2001 Council of Europe Convention on Cybercrime is a historic milestone in the combat against cybercrime. It was opened for signatures in November, 2001 and entered into force on July 1, 2004. The total number of signatures not followed by ratifications are 15, and 32 States have ratified the Convention. Of all member States of the Council of Europe only Andorra, Monaco, Russia and San Marino have not signed the convention.[1]

[1] The Council of Europe's official Treaty Office, Retrieved April 11, 2012 from http://conventions.coe.int.

Chapter 3. Cyber security in Estonia

1 Introduction

This chapter gives an overview about cyber security in Estonia. Chapter starts with introduction to Estonia and second part is divided into three sections by placing Estonia's Bronze soldier's related cyberattack in 2007 a central point – before that attack, attack itself and changes after attack.

2 Estonia

Geographically most of Estonia's borderline is coastline, but Estonia has land borders with Russia and Latvia. Estonia lies on north-eastern edge of the European Union.

Area of the country is 45 227 km^2 and population around 1.3 million. Type of Government is parliamentary democracy. Estonia is a member of European Union and NATO since 2004, and a member of Schengen zone since 2007.

In 2009 Ministry of Economic Affairs and Communications and members of Estonian Association of Information Technology and Telecommunications founded The Estonian Broadband Development Foundation in aim to make 100Mbit/s broadband available to the majority of Estonian households and businesses by the year 2015. During the programme is done design and construction of fiber-based physical network on a way that 98% of the residential houses, businesses and authorities are located closer than 1.5 km of the basic network. Programme is financed by different EU Structural Funds. [2]

Soiela (2010) states that the use of computers and the Internet by enterprises in Estonia has reached its peak, because there is no more room for further increase – almost all enterprises with ten and more persons employed use computers and have Internet connection and this has been so for the last three years. The share of households with Internet connection at home is continuously increasing also — in the 1st quarter of 2009, 63% of households had access to the Internet at home, in the 1st quarter of 2010 — 68%.

On following figure 8 there is visualized the growth of Internet users in Estonia. As seen on the figure, 76.5% of the population was using Internet in 2011 and since the year 2005 the growth per the year have been 2%[3].

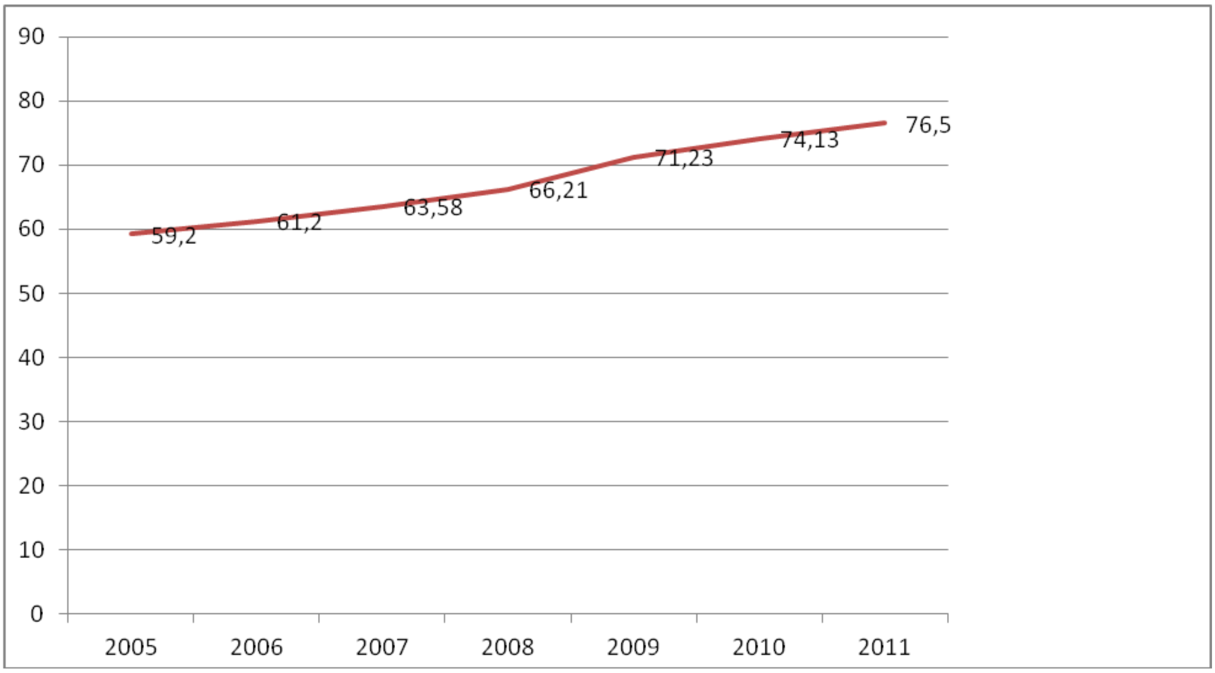


Figure 8 – Internet users in Estonia (percentage). Statistics Estonia (2012).

[2] Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (2009) Development vision of next-generation broadband network in Estonia Retreaved April 11, 2012 from http://www.elasa.ee/public/files/Estonian%20Broadband%20Vision.pdf.
[3] Statistics Estonia. Retrieved May 2, 2012 from http://www.stat.ee/.

The United Nations global survey of e-government (2012) have brought out Estonia as one of the leading in world e-government development in 2012 – Estonia has ranked the 20th place with index 0.7987 remaining at the same level as two years before in 2010, but increasing the index. In e-participation Estonia have ranked in place five (0.7632) along with Australia (0.7632) and Germany (0.7632). It is an interesting fact that Estonia along with Finland and Spain has declared Access to the Internet as a legal right of the citizens.

The International Telecommunication Union (2011) placed Estonia by the ICT development index in the 33rd place in 2010 with the index 6.16. Before, in year 2008 Estonia gained 28th place with the index 5.81. The ICT development index is a composite index made up of 11 indicators covering ICT access, use and skills. In this research 152 countries were evaluated.

2.1 E-Government in Estonia – an overview

Layne and Lee (2001) proposed four-stage model to explain the evolution of e-government seen on following figure 8. On the first stage *Catalogue* government provides information and some static documents on-line. During the second stage called *Transaction* databases and simple online services are provided. The third stage is called *Vertical Integration* and is focused on linking local and state systems. The last, fourth stage is *Horizontal Integration* which connects different systems into one unified service.

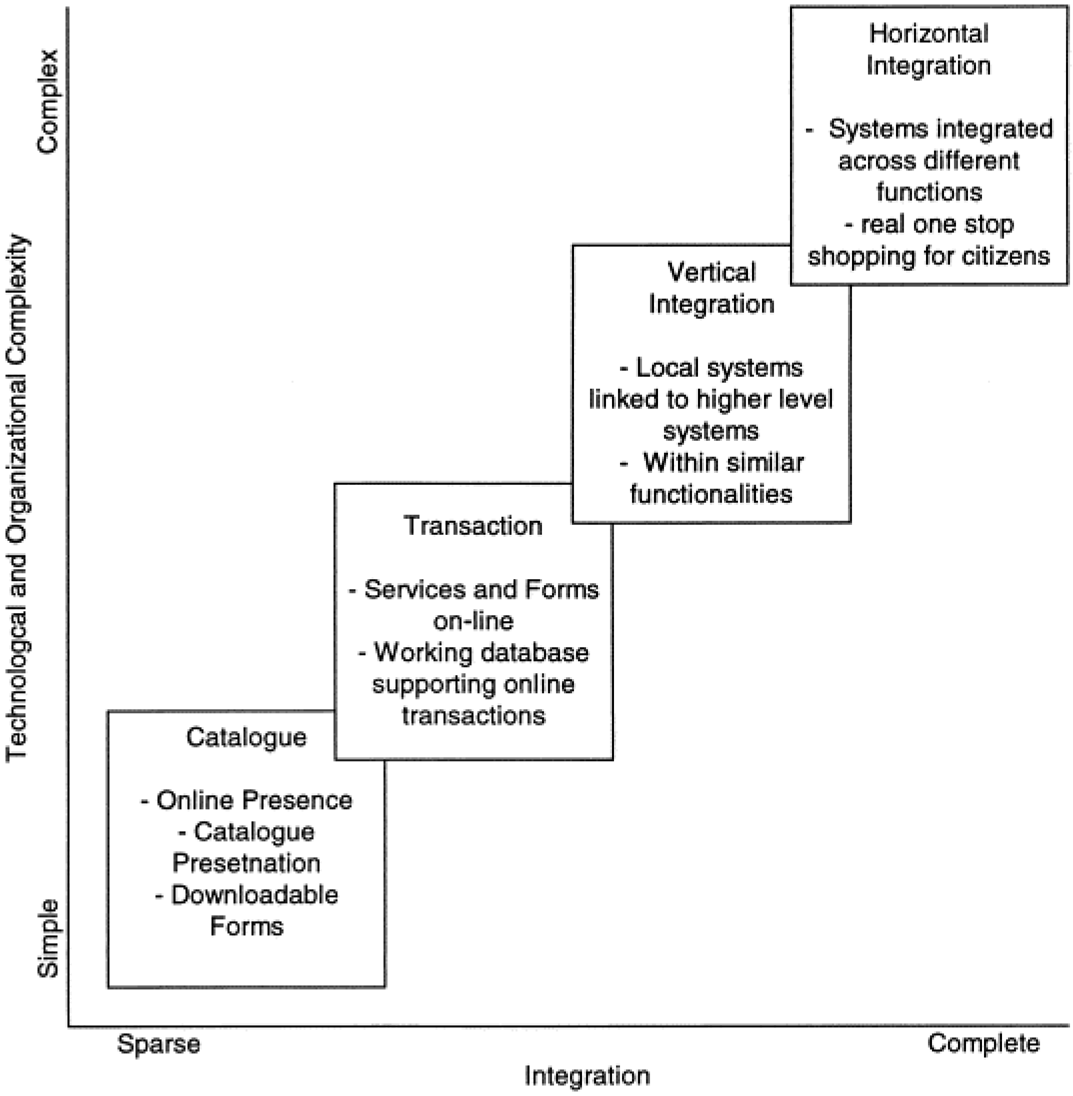

Horizontal Integration
- Systems integrated across different functions
- real one stop shopping for citizens
Vertical Integration
- Local systems linked to higher level systems
- Within similar functionalities
Transaction
- Services and Forms on-line
- Working database supporting online transactions
Catalogue
- Online Presence
- Catalogue Presetnation
- Downloadable Forms
Technologcal and Organizational Complexity
Complex
Simple
Sparse
Complete
Integration

Figure 9 – Steps towards E-Government by Layine and Lee (2001).

Moon (2002) and Siau and Long (2005) have implemented five-stage model in which the last stage is similarly placed the citizen's participation – Moon names it political participation and Siau and Long e-democracy. Jayashree and Marthandan (2010) specify that e-society may include different services like e-business, e-health services, e-payments, e-procedurement, e-education, e-banking, e-democracy, e-parliament, e-billing, etc., in a way where there is a relationship between governments, markets and private sector.

Estonian government has used a striking information system of e-Government where all operations are done in an electronic environment without paper for more than a decade.[4]

X-Road and Digital ID

Two key ingredients are the X-Road and Digital ID. The X-Road, launched in the year 2002, is a tool that connects all the decentralized components of the system together so that various public and private sector's e-services databases can exchange data. Digital ID launched in 2001 in nationally standardized system for verifying a person's identity both in digital environment and physical world, and signing digital documents.[5] In 2007 the alternative for ID-card was implemented. M-ID offers identification and signature of digital documents via mobile phone. Today over 86% citizens have ID-cards.

In March 2007 Estonia had world's first national general elections with an Internet voting option for the Parliament (Riigikogu). The mobile-ID was used for the first time in March 2011 for personal identification for iVoting in Parliamentary Elections in Estonia.

E-Services

Starting June 2007 Estonian businesses were able to submit their annual accounting reports electronically using the Company Registration Portal. Since the beginning of that year it takes only 15 minutes to establish a firm in the Internet; company will be legalized within a few hours and an undertaker may start with business the same day. In August 2007 the Estonian Tax and Customs Boards began to offer an e-service to local authorities enabling them to make inquiries on the income of the taxpayers living in their area. Also, in 2007 the website Osalusveeb was launched. It allows Estonian citizens, associations, civil society stakeholders who have registered as a user to express opinions on drafts published by the Government. At the end of the year 2007 a new version of the Estonian State portal eesti.ee results from the merge of the former State Information portal and the Citizen portal, creating a single integrated service.

[4] Estonian Information System's Authority's webpage http://www.ria.ee/facts-about-e-estonia/ accessed April 11, 2012.

[5] Estonia ICT Demo Center's webpage http://e-estonia.com/e-estonia/digital-society accessed April 11, 2012.

In February 2008 improved Tax and Customs Board's online service was able to submit Estonians tax returns electronically. In 2011, 92% of people declared their income electronically.

Police patrol cars are equipped with computers and an internet connection allowing to receive information about a driver and his car without a driving license or car documents. The system has an access to more than 15 databases (3 of these outside Estonia) directly or via X-Road.

For teacher-student-parent communication there is an electronic tool called E-Kool (e-school). Every year approximately 35 000 people (almost every school-leaver) use the opportunity to get the results of state examination as an SMS to their mobile phone and can get the result in real time.

There are many more e-services in Estonia – in areas of business, citizens, education, government, healthcare, infrastructure, public safety and utilities. Basically everything can be done via Internet using X-Road and/or digital authentication.

2.2 Online banking in Estonia

The share of cash in circulation is decreasing and Estonia's payment environment is essentially electronic: electronic payment channels and non-cash payment methods are preferred. Estonia has approximately 1.3 million inhabitants. Based on statistics from August 2011 99.6% of banking transactions are done electronically. According to Bank of Estonia[6] there were more than 1.7 million bank cards in use in 2011 (see figure 9).

[6] Bank of Estonia. Retrieved February 2, 2012 from http://statistika.eestipank.ee/?lng=en#treeMenu/AVALEHT.

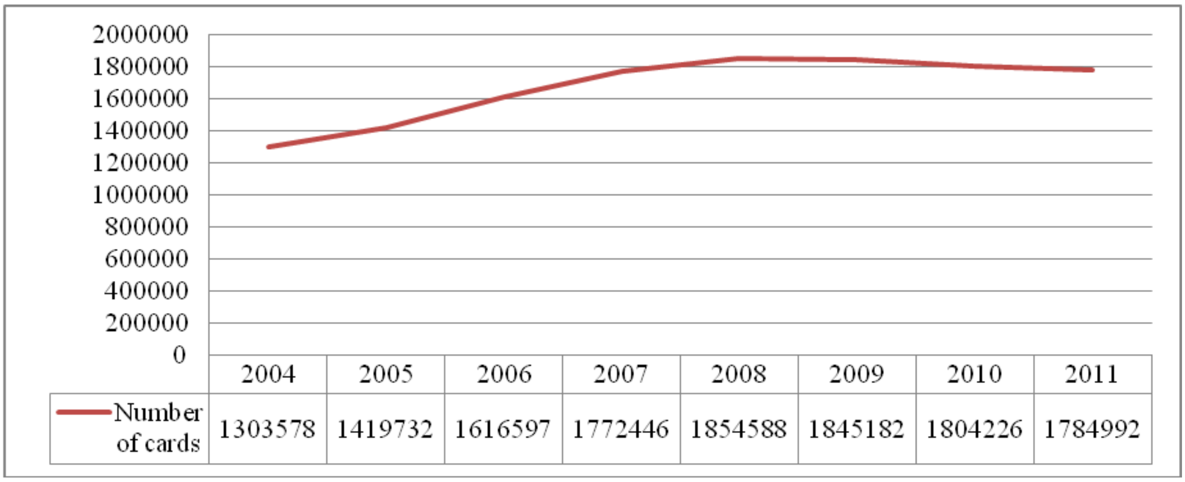
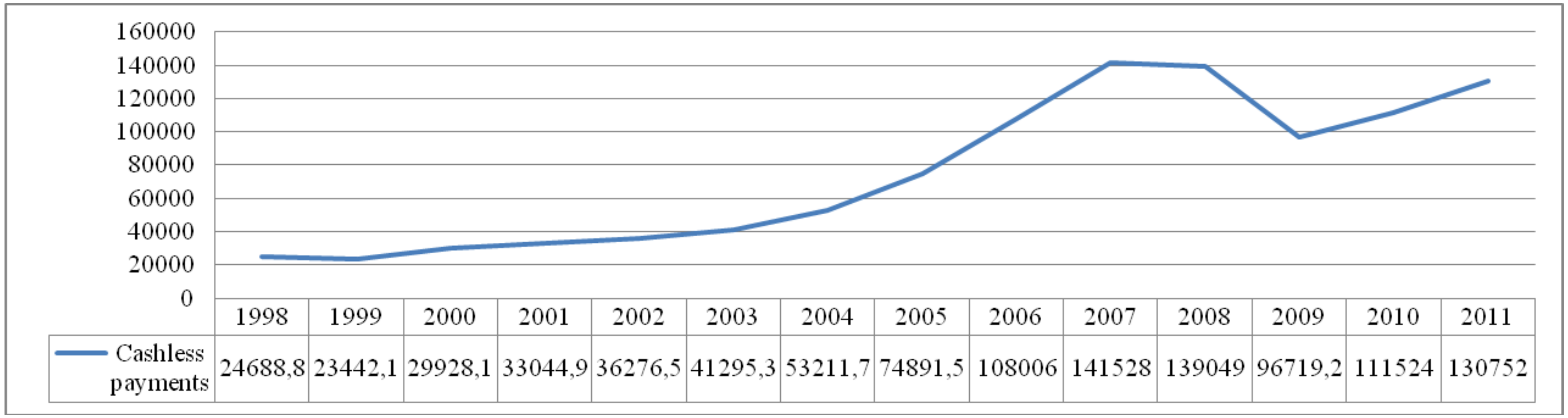


Figure 10 – Number of bank cards in Estonia. (Bank of Estonia, 2012)

Values of cashless payments made by non-financial corporations and households have increased six times from 1998 (see figure 10). The noticeable decrease in 2009 was due to global economical breakdown.

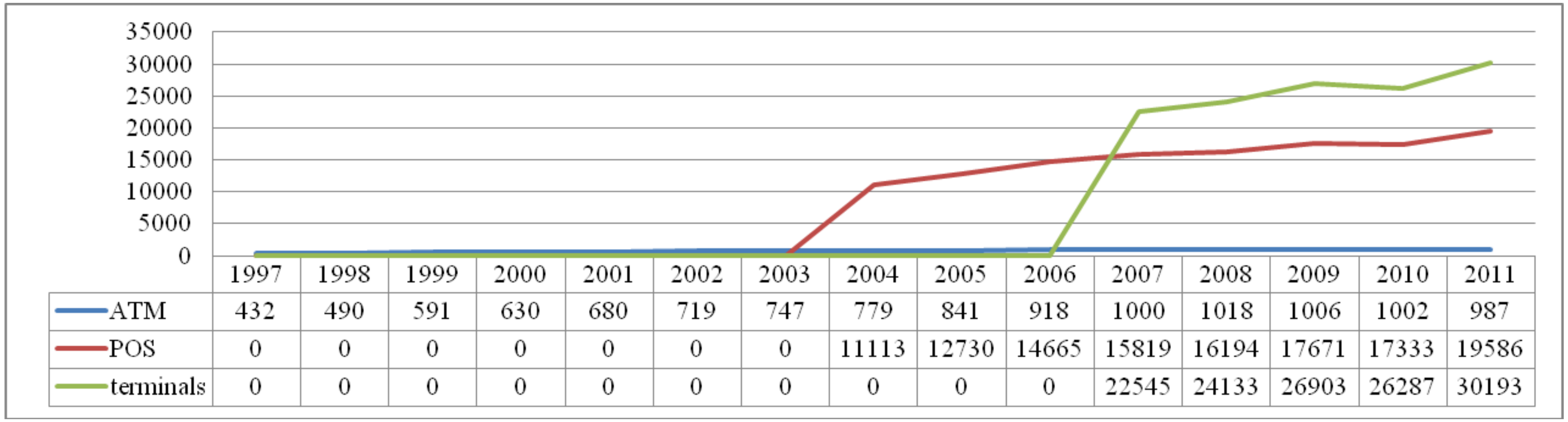
On the figure 11 you can see the visualized change in number of ATMs (automated teller machine which is an electromechanical device that permits authorized cardholders, typically using machine-readable plastic cards, to withdraw cash from their accounts and/or access other services, such as balance enquiries, transfer of funds or acceptance of deposits), POSs (provisions of goods and services at terminals) and POS terminals (devices allowing the use of payment cards at a physical not virtual point of sale).

Number of automated teller machines (ATMs) has doubled from 432 in 1997 to 987 in 2001. POSs came into usage in 2004. Since then the number of POSs has increased almost twice to 19 586 pieces. POS terminals came into usage in 2007 and the number of terminals is also steadily increasing to 30 193 terminals in 2011.



	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Cashless payments	24688,8	23442,1	29928,1	33044,9	36276,5	41295,3	53211,7	74891,5	108006	141528	139049	96719,2	111524	130752

Figure 11 – Value of cashless payments made by non-financial corporations and households (EUR). (Bank of Estonia, 2012)



	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
ATM	432	490	591	630	680	719	747	779	841	918	1000	1018	1006	1002	987
POS	0	0	0	0	0	0	0	11113	12730	14665	15819	16194	17671	17333	19586
terminals	0	0	0	0	0	0	0	0	0	0	22545	24133	26903	26287	30193

Figure 12 – Number of ATMs, POSs and POS terminals (pieces). (Bank of Estonia, 2012)

2.3 Conclusion

Examples given above represent only a small part of e-Estonia. Compared with the Layne and Lee (2001) proposed four-stage model, we can say that Estonia can be situated on fourth stage as its systems are complex and complete – across different functions systems are integrated and complex. Clearly there is political participation as Moon (2002) requires and e-democracy proposed by Siau and Long (2005). Not to mention relationships between government, markets and private sector what are required for implementing e-government by Jayashree and Marthandan (2010).

As on one hand it shows Estonia's great progress in developing e-services, it also shows increased reliance on information technology systems and therefore rapidly growing need for cyber security basis to provide safe and reliable systems.

3 Cyber security in Estonia before year 2007

3.1 Overview

The following gives an overview of developments on information society and cyber security levels before cyberattack in 2007.

Framework's level

In year 1998 entered into force Estonian parliament approved the Principles of the Estonian Information Policy[7]. This was the first document of the information society in Estonia. Principles served as a basis for an action plan for establishing an information society. The action plan was in basis for all Government agencies to present specific proposals to the Cabinet every year together with schedules, sources of finances and responsibilities for implementation of information policy programmes. Similar to the concept of establishing an

[7] Principles of Estonian Information Policy (1998) Riigi Teataja I 1998, 47, 700.

information society approved by European Union, the interest of the State covers both public and private sectors.

There were four main areas in focus in developing Information Policy Action Plan:

- Modernization of legislation;
- Supporting the development of the private sector;
- Shaping the interaction between the State and citizens;
- Raising awareness of problems concerning the information society.

Until the year 2003 this document was the guiding document for the development of information society in the conceptual basis.

In 2003 Estonia ratified the Council of Europe Convention on Cybercrime (submitted for member-state ratifications in 2001, entered into force in 2004).

In 2004 the Principles of the Estonian Information Policy 2004-2006 was elaborated and approved by the Government. This document was the fundamental of the development of information policy for the period 2004-2006 and expired on January 1, 2007. Ott (2004) stated that the Principles of the Estonian Information Policy for 2004-2006 included also the aspects of IT security aiming to elaborate the basic principles of IT security. It stated that in co-operation with the private sector, a national IT security centre will be established. The centre will be vested with the following tasks: registering of attacks, informing of all parties involved, elaborating and distributing safeguard measures, and increasing awareness about IT security.

In year 2004 Department of State Information Systems of the Ministry of Economic Affairs and Communications revealed the first version of Estonian IT Interoperability Framework.

The Estonian IT interoperability framework is a set of standards and guidelines aimed at ensuring the provision of services for public administration institutions, enterprises and citizens both in the national and the European contexts in order to increase public sector efficiency in Estonia by improving the quality of services provided to citizens and enterprises both at the Estonian and EU level. Document is open for proposals from public, private and third sector organizations as well as from other interested parties. The framework is in constant progress – document is reviewed and, if needed, updated annually. (Estonian IT Interoperability Framework, version 2.0)

In year 2006 The Estonian Information Society Strategy 2013 was approved by the Order of the Government of the Republic Nr 667. Framework given in this document comprises five primary fields of IT security both public and private sector. The following table 2 outlines the fields along with examples of respective activities and field coordinators.

Table 2 – Five primary fields of IT security in „The Estonian Information Society Strategy 2013“. Tepandi (2007).

Field	**Examples of activities**	**Co-ordinating authority**
Co-operation and co-ordination	Co-ordination of conducting the risk analysis of the Estonian IT environment; raising of the effectiveness of handling security incidents in Estonia	Ministry of Economic Affairs and Communications
Acknowledgement And training	Provision of IT security training for the top management and IT managers of public agencies; raising of the awareness of security issues in schools and universities	Ministry of Education and Research in co-operation with the State Chancellery, the Ministry of Defence and the Ministry of Economic Affairs and Communications
Elaboration of regulations	Drafting and updating of legislation on information security and electronic communications; drafting of regulations for the protection of critical information infrastructure; co-ordination of database administration pursuant to the requirements of the system of security measures; elaboration of information security standards applied in public procurement	Ministry of Economic Affairs and Communications in co-operation with the Ministry of Internal Affairs
Protection of	Provision of protection of information infrastructure;	Ministry of Internal

information infrastructure	organization and coordination of fight against cybercrime	Affairs in cooperation with the Ministry of Defence
Implementation Activities for the protection of people and assets	Implementation of personal data protection measures; development and introduction of secure (ID card based) standard solutions; launch of crossborder ID card based services	Ministry of Internal Affairs in cooperation with the Ministry of Defence

Abridgement of Estonian IT Interoperability Framework aims to create the safe, secure and aware information society in Estonia. The information security issues are the same as the Estonian Information Society Strategy 2013 IT security fields.

Organizations' level

In 1996 Estonian Informatics Council[8] was formed under the law of the Estonian Government (RT I, 79, 1409). The Council is responsible for the delivery of the general principles and proposals for drafting the ICT strategy development. Since June 2011 the Estonian Informatics Centre re-organized to the Estonian Information System's Authority (EISA) and added a new purview - supervision.

In 1998 Estonia was accepted as an official full member of International Council for Information Technology in Government Administration (ICA). ICA was established in 1968 and is a non-profit organization established to promote the information exchange of knowledge, ideas and experiences between Central Government IT Authorities on all aspects of the initiation, development and implementation of computer-based systems in and by Government.[9]

In 2000 the Estonian Computer Association (AFA, founded in 1992) and the Association of Telecommunications Companies (TEL, founded in 2000) merged into the Association of Estonian Information Technology and Telecommunications Companies. The official name of the new organization is Estonian Association of Information Technology and Telecommunications (ITL). ITL is a voluntary organization, with primary objective to unite

[8] Formation of Estonian Informatics Council (1996). State Gazette I, 79, 1409.

the Estonian information technology and telecommunications companies to promote their co-operation in Estonia's development towards information society, to represent and protect the interests of its member companies and to express their common positions.[10]

In 2001, Estonia’s most influential companies in private sector Swedbank, SEB, Elion, EMT, MicroLink, BCS, IT Grupp, Starman, IBM and Oracle established a foundation called Look@World. The aim of the foundation was to encourage the use of the Internet and popularize it. In May 2006 biggest telecom companies and banks of Look@World Foundation and Ministry of Economic Affairs and Communication signed a cooperation agreement “Computer Protection 2009” aiming to design Estonia the most secure information society in the world by year 2009. Within three years were provided thru this project basic computer and Internet training for 100,000 Estonians and opened 500 public Internet access points. (Aro 2008)

In 2005 established the Computer Emergency Response Team of Estonia (CERT Estonia) – it was the first organization in Estonia with direct responsibility for handling security incidents, ensuring respective co-ordination between different organizations and providing assistance in responding to security threats (Information Technology in public… 2005). CERT Estonia is responsible for the management of security in .ee computer networks and also national contract point for international co-operation in the field of IT security.[11]

Educational level

In year 1996 was established Tiger Leap Foundation. Foundation was named as an allusion to the “East Asian Tigers”, the countries whose economy boomed in part as a result of information technology use. The Tiger Leap Foundation is working under the Estonian Ministry of Education and Research with the aim to increase Estonian school education quality utilizing modern information and communication technology.[12]

[9] International Council for Information Technology in Government Administration webpage http://www.ica-it.org/index.php?option=com_content&view=article&id=49&Itemid=53 accessed April 22, 2012.

[10] The Estonian Association of Information technology and Telecommunications (ITL) webpage http://itl.ee/?op=body&id=58 accessed April 26, 2012.

[1111] CERT Estonia webpage http://www.cert.ee/ accessed April 22, 2012.

[12] Tiger Leap Foundation homepage http://www.tiigrihype.ee/?op=body&id=45 accessed April 22, 2012.

In order to ensure education in field of information technology the Estonian Information Technology College (IT College) was founded in year 2000 by Republic of Estonia represented by Ministry of Education and Research, University of Tartu, Tallinn University of Technology, Estonian Telecom, Estonian Association of Information Technology and Telecommunication. College offers private non-profit higher education and is owned by the Estonian Information Technology Foundation (EITF).[13]

3.2 Analysis

As shown from the documents which coordinate the establishment of an information society, the work in government level shows understanding the need of framework in developing the e-society. Security concerns were first outlined in the Principles of Estonian Information Policy 2004-2006. It is noteworthy that from the beginning the private sector was involved to develop an information society – the cooperation helped to create the background of trust which paid off when security issues became a problem.

According to Rain Ottis, scientist / senior analyst with the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) the Estonian cyber security situation was undergoing several key developments at the time before attacks in 2007 – the CERT-EE had been established, and CCD COE was in the process of being established – as Estonia was developing massive e-services landscape there was also a rising interest of cyber security. Still, on that time, most of the attention was on what and how to develop nor how to protect it in case of an attack.

Ottis also agreed that on the government-level there was not so much concern of cyber security matters as attack against state or public services, but against private sector businesses:

> *In practical terms, the primary perceived cyber security risk at the time was criminal in nature (attacks against banks and their customers). The major banks in Estonia were quite used to dealing with this type of threat, but the law enforcement capability was still relatively weak.* Rain Ottis.

[13] The webpage of IT College. Retrieved April 22, 2012 from http://www.itcollege.ee/en/it-college/.

Jaan Priisalu, Director General at Estonian Information System's Authority adds that in 1998 begun the cooperation between banks and all who were involved in security issues were thinking about cyber security. To politicians concerns over cyber security were not so much topic of.

> *At the level of specialists there was cooperation and managers allowed this to happen. Cooperation was not prohibited, but it was not particularly promoted as well.* Jaan Priisalu.

The fact that on the state level cyber security was not a significant concern (but, as Priisalu stressed – situation in Estonia on the field of cyber security was definitely better than in many other countries), the attack did not bring a helpless situation. As businesses in private sector had the desire and willingness to give the advice and help in needed expertise and knowledge the controlling and overcoming cyberattack was quite smooth and successful. However, it signaled a lack of educational level which needed to be solved in order to have sufficient specialists with necessary knowledge. As the dependence of cyber environment was growing at every level, the need for such specialists was clearly increasing.

4 Estonia’s Bronze soldier’s related cyberattack

4.1 Description of the attack

After relocation of a Soviet-era statue known as Bronze soldier from intersection in central Tallinn to a nearby military cemetery in Tallinn in April of 2007 Estonia fell under a politically motivated (Ottis 2008) cyberattack between 27th of April and 18th of May of 2007. Attack lasted twenty-two days. Among the targets were Estonian governmental agencies and services, schools, banks, Internet Service Providers (ISPs), as well as media channels and private web sites (Evron 2008; Tikk, Kaska, and Vihul 2010 via Ottis 2008).

The moving of monument began on the 26th of April 2007 accompanied of mostly peaceful protesters. In the evening a more violent crowd emerged and after few hours of violent clashes with the police the rioters turned away and proceeded to vandalize and loot the nearby stores. Police regained control of the situation by morning. (Ottis 2008)

By April 28th the cyberattack against Estonia was officially recognized as being more than just random criminal acts (Kash 2008 via Ottis 2011). According to Goodman (2010) the attacks mostly consisted of huge numbers of privately owned computers jamming Estonian government and business websites with meaningless or malicious information. Ottis (2008) marks that in general the attack method used was Denial of Service (DoS) or Distributed Denial of Service (DDoS). A few more complex attempts were made to hack into systems, for example using SQL injection. Some of these attacks had success at non-critical sites. The targeted systems included web servers, e-mail servers, DNS servers and routers, but most visible to the public were the attacks against web servers.

To combat the malicious traffic originated from outside Estonia, some banks temporarily cut off all foreign traffic while remaining accessible for clients in Estonia (Ottis, 2008). Goodman (2010) states that Estonia's response to the attacks proved effective – initially Estonia's network closed off for some international traffic and states with numerous clients was closed, but few attackers were slowly permitted back onto Estonian networks.

There has been an intriguing discussion about who was behind the attacks. The malicious traffic often contained a clear indication of Russian language background. Ottis (2008) brings an example malformed queries directed at a government website included phrases like "*ANSIP_PIDOR=FASCIST*" (Mr. Ansip was the Estonian Prime Minister at the time). Also the instructions for attacking Estonian sites were disseminated in many Russian language forums and websites. These instructions often contained detailed information about motivation, targeting and timing, as well as a specific description for launching attacks.

According to Agreement on Mutual Legal Assistance[14] between Estonia and Russia, signed in 1993, the states render each other legal assistance that includes procedural acts provided by law and conducted by the party who has received the request for mutual legal assistance. Estonian Public Prosecutor's Office asked Russian Federation's assistance in conducting preliminary investigations in a criminal matter, but received an answer what stated that „the agreement stipulates that legal assistance shall be rendered in the framework of the procedural acts, according to the legal acts of the contracting party who has received a request, but it does not require cooperation in the field of operative prosecution measures in order to identify the location of a person'". Estonian Prosecutor General's Office admitted that Russia's approach is formally correct. (Tikk and Kaska 2010)

4.2 Analysis

So far only one person has been convicted of carrying out cyberattacks in the spring of 2007 – in January 2008 a 20-year old student in Estonia, Dmitri Galuškevitš was fined for organizing a DDoS attack against the website of a political party in Estonia. As stressed out by Ottis (2008) Galuškevitš' conviction was possible only because he committed the attacks from Estonia and therefore enough evidence could be collected.

Many researchers have stressed out the difficulty in investigation of cybercrimes represented by sophistication of cross-border assistance in cybercrimes investigation. As discussed by Goodman (2010) the problem with investigation of cyberattacks and lack in cross-border cooperation poses obvious problems as states attempt to develop an effective cyber deterrence strategy. Although cyberspace may be a stateless domain, the international law and domestic criminal laws should be updated and improved to hold states responsible, make them liable, or at least encourage mutual assistance in fighting cyberattacks that originate in their territory. As Russia did not agree to cooperate with Estonia in the investigation of attacks, has caused the opinion that attacks were either coordinated or at least approved by Russian government. However, there is no state-level common understanding or decision that Russian government had a leading role in this case. Also experts who were interviewed disagree:

> *Government role in the event remains unproven, except for the fact that the Russian government refused law enforcement cooperation to investigate the cyberattacks.* Rain Ottis

In Priisalu's opinion the fact that Russia refused law enforcement cooperation just improves that attack against Estonia was state-sponsored by Russian Federation.

[14] Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed on January 26, 1993. RT (State Gazette) II 1993, 16, 27; RT II 2002, 14, 58.

Russia's behavior and legal decision not to assistance Estonia in investigation of cyberattack shows how difficult is to investigate those types of crimes and indicates the need of cross-border cooperation in the area. It also shows that how powerful and full of opportunities is the environment of the Internet and other environments connected to it is whether the criminals are led by criminal group or led or approved by the state. This means that each country must concern of ensuring themselves in terms of cyber security including exclusion of possible cyberattacks. And for countries the international cooperation is essential in order to ensure cyber security in field of national safety as well as fighting crime.

But there is not the only problem the will of cooperation to determine the origin of cyberattack. Goodman (2010) have also underlined that as World Wide Web technology is owned by private network infrastructure firms, states should establish agreements under which these companies would provide key information to investigators seeking to attribute malicious activity in cyberspace in order to prevent similar attacks.

Priisalu stressed out that the well-known DDoS attacks were not the only attack methods used – there also was unauthorized modification of web pages of a small number of users (for example cooperatives, fan pages, etc.). Web pages were taking over and content swapped with bronze soldier's pictures, etc. According to Priisalu during the attack period there were also anonymous persons, who “walked along the web and cleaned it up” – the example of volunteering.

No country is protected from similar attacks as attacks did not focus on security vulnerabilities other than capacity. Ottis points out that the effectiveness depends on size mismatch between the attacker and defender which makes similar attacks possible in every country, but he admits that attacks may not be as effective in some places – the threat depends of technical capacity issues.

Estonia's Bronze soldier's related cyberattack in April and May 2007 can be considered as the first known incidence of such an assault on a state. Mägi and Vitsut (2008) have pointed out that before Estonia's case similar attacks have been classified as hooliganism, criminal or nationalistic. Mägi and Vitsut also say that Estonia's case there are clear signs of a nationalistic attack which is special because of the range of the attack, also by variety and diversity of targets and clear visible links to the orientation against Estonia which is the reason why those attacks attracted the attention of many worldwide cyber security professionals. Here it is important to stress out that Estonia did not consider it as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty (Ottis 2011). The attacks were simply regarded as individual cybercrimes (Nazario 2007; Tikk, Kaska, and Vihul 2010 via Ottis 2011) or "hacktivism" as established by Denning (2001 via Ottis 2011).

Despite the fact that cyberattack was considered as against a country, since no significant losses did not occur, there is widespread belief among experts that the attackers did not achieve anything special. Even more, experts believe that Estonia as the target of the attack won from it.

In Ottis opinion, the attackers failed in 2007:

> *There were no serious or critical effects on the population or the economy as a result of cyberattacks. The attackers lacked legitimacy and overreacted on the Bronze soldier issue. As a result, Estonia got a "diplomatic victory" in an event that could otherwise have been interpreted in various ways by the Western media.* Rain Ottis

Same is expressed by Jüri Kivimaa, currently working as a scientist at CCD COE, before, including year 2007, Kivimaa worked as information security expert at SEB Estonia. In Kivimaa's opinion, Estonia won more from cyberattack than lost: it is impossible to figure out better advertisement for the NATO cyber security center, he said.

Kivimaa also is well aware why Estonia succeeded in quickly and decisively responds to cyberattacks. Accordingly to his knowledge Hansapank [now Swedbank] had its first DDoS attack before 2007 and the bank was down for a few days. Due to the past experience, in 2007 the bank managed to start the work again in few hours. So they already had the experience of very large and organized attacks in the past which allowed to response in 2007 quickly and decisively. Jaan Priisalu agrees that the cooperation was at really good level; if there was not such a good cooperation the attack would have the impact for weeks. But he also stresses out that preparation and practice are essential in order to defend effectively from the attack – this is the reason why cooperation is needed before the attack itself.

Ottis emphasizes that there is no reason to underestimate the cyber threat.

> *Let me remind you that in 2007 we saw one of the most primitive attack scenarios imaginable, which was only using brute force. A clandestine, well targeted and executed attack could have serious consequences for a state.* Rain Ottis

This is also pointed out by Reet Oorn, who was working as an analytic in Estonian Information System's Authority in 2007. Oorn admitted (2007) that if at first it felt like attacks in cyberspace were not as dangerous as riots on streets at that time then looking back actions on the Internet greatly exceeded dangerously what was on the streets. Oorn proposed that those attacks should be considered dangerous because they were directed to a relatively small country which has great dependence on information and communication technology.

But communication technology is not the only possible target and experts believe that the next time would not be as easy as the attack in 2007. Kivimägi lists other potential targets:

> *I'm sure our eastern neighbors' have the plan how interfere our electricity or water production, transport and air traffic. However, despite there is currently no war going on, does not mean these plans are not implemented.* Agu Kivimägi

But he also stresses out the principle of proportionality – although some countries have nuclear weapons, they do not use them because it is not reasonable. In his opinion the same principle is used for cyber weapons, too, but still it is important to take into consideration of such threats and to be ready for them. Ottis also believes that the attack on year 2007 will not repeat in exactly the same way, therefore it is essential not to plan for the last conflict. Still, planning the cyber defense is necessary – just because we were attacked five years ago does not mean that we will never be attacked again, he says. Same is stressed out by Jüri Kivimaa – attacks cannot be prevented, if someone wants to attack, then he attacks, what is important is to be ready for it.

5 Cyber security in Estonia after the cyberattack

5.1 Overview

After the attack in 2007 several actions were carried out in order to be better prepared next time. As following it is given an overview of changes after cyberattack in 2007 in three levels – framework, organizations and education on the area of cyber security.

Framework's level

In 2007 The Government approved an Action Plan to Fight Cyberattacks[15]. Plan was established by the Government upon the proposal of the Ministry of Economic Affairs and Communications (2007). The plan was implemented in co-operation of the Ministry of Justice, Ministry of Defence, Ministry of Economic Affairs and Communications, Ministry of Finance, Ministry of Internal Affairs and Ministry of Foreign Affairs and the director of security coordination of the State Chancellery.

The action plan's aim is to be prepared for cyberattacks in a way that attack could not paralyze normal daily activities. Plan has three main objectives. First, the action plan seeks to improve the processes of preparing for emergencies in light of the cyberattacks. Secondly, the action plan emphasizes the importance of information security of the state information systems. Third, the action plan seeks to improve the legal framework and create a strong legal basis for fighting cybercrime.

In year 2008 Estonian Government submitted Estonia's Cyber Security Strategy for 2008-2013. Strategy was prepared by the Cyber Security Committee which was at that time led bu the Ministry of Defence in cooperation with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs and the Ministry of Foreign Affairs. Since the year 2011 the Cyber Security Strategy Committee is led by the Ministry of Economic Affairs and Communications.

Cyber Security Strategy sets five key objectives in enhancing cyber security policies:

[15] Estonian Information System's Authority. (June 6, 2007) Valitsuskabinet kiitis heaks küberrünnetevastase tegevuskava. [Press release] Retrieved April 30, 2012 from http://www.ria.ee/valitsuskabinet-kiitis-heaks-kuberrunnetevastase-tegevuskava/.

1. The development and large-scale implementation of a system of security measures - development of adequate security measures;
2. Increasing competence in cyber security – educational field connected objective in order to provide high quality and accessible information security-related training in order to achieve competence in both the public and private sectors;
3. Improvement of the legal framework for supporting cyber security – both aligning Estonia's legal framework as also participating in international law-making in the field of cyber security;
4. Bolstering international co-operation – promoting countries' adopting of international conventions regulating cybercrime and cyberattacks;
5. Raising awareness on cyber security.

Cyber Security Strategy gives ambitious principles and guidelines to rely on in proceeding national cyber security policies for Estonia. As pointed before, the cooperation in important. Cyber security should be pursued through public and private sectors as well as of civil society. Co-operation with international organizations and other countries will increase cyber security globally. That's leading to efficient information security – every information system owner should be aware of the responsibilities and therefore should take the necessary security measures to manage the identified risks. But also a general social awareness of threats in cyberspace – every member of the information society is responsible for the security of the network-based instruments or systems in possession. In conclusion - cyber security action plans should be integrated into the routine processes of national security planning. All those proposals are easily applicable to any other state to raise the level of cyber strategy knowledge in government level.

Implementation Plan For 2009-2011 of the Estonian Information Society Strategy 2013 focused main areas on the Information Technology and Telecommunications front. Information Society Policy is under the responsibility of the Ministry of Economic Affairs and Communications and the list of activities is updated frequently. In the Estonian Association of Information Technology and Telecommunications (ITL) Activity plan for 2009-2011 (2009) ITL focused mainly on developing economical areas of information technology, but also on IT education and social problems related to the area (e.g. Internet security).

In ITL Implementation Plan for 2011-2013 (2011) association remained focusing economical areas, but plan also sets the activity of increasing the social responsibility of ICT enterprises through implementation of the project "Increasing the safety awareness of young people for coping in the information society". Also focusing on development of information society in Estonia and education area - bringing the IT Academy initiative to implementation, improving the funding of teaching ICT sector specialties and therefore continue the promotion of ICT specialties in basic and upper secondary schools.

Organizations' level

In May 2008 seven NATO nations and the Allied Command Transformation signed the documents for the formal establishment of Nato Cooperative Cyber Defence (CDD) Centre of Excellence (COE) in Tallinn, Estonia.

It seems like this event is connected to Bronze Soldier' case, but actually negotiations for the establishment of CDD COE had been going on since 2004 (Kaju 2008). In 2006 confirmed the conception for organization and the work started by renovating the suitable building and recruitment of the expert group. Still obviously cannot rule out cyberattacks as a consequence of the positive effects of political role in this decision, cyberattacks in spring 2007 definitely enhanced cyber security a priority.

The aim of CDD COE was established in order to enhance NATO's cyber defense capability. It is and International Military Organization and fully accredited by NATO's North Atlantic Council. Its mission is to develop a strategy to prevent cyberattacks; it is not CERT, military base for hackers, intelligence body or any kind of cyber security alliance. In 2012 Estonia will be hosting the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

Estonia had from it significant benefits – increased and strengthened ties with NATO, accelerated development of structures in the field of cyber defense, economic, educational and scientific areas, cannot be left unchecked Estonia's international political prestige. (Estonian Information System's Authority)

Cyberattack in year 2007 showed the need for facility staff at the defense level. The work in order to create the cyber defence league started immediately after the attack and in 2010 the Cyber Defense League was formally established. The actual action in entity started years before. Cyber Defence League is a volunteer organization operating under the Estonian Ministry of Defence. Cyber Defence League is comprised of IT security experts, programmers, lawyers and management specialists from the nation's top IT companies, banks, ISPs and defense forces. The basic objectives of cyber defence league are:

- Creating the network which brings together public and private sector's expertise in cyber environment related crisis situations;
- Increasing the level of cyber security in critical information infrastructure through increased awareness and dissemination of best practices;
- Training members in cyber security field.[16]

In October 2009 was established the Department for Critical Information Infrastructure Protection (CIIP) at Estonian Information System's Authority. CIIP's tasks are to protect public and private sector information systems that are relevant for the functioning of the state. But also analyzes risks on the field related to critical information infrastructure and development and supervision of the security measures and initiated methods.[17]

The Estonian Police and Border Guard also have their own Cyber Crimes Unit, to investigate and prosecute online criminal activity.

Educational level

As stressed out in the Cyber Security Strategy, at the end of 2007, there were no public or private universities in Estonia providing in-depth training in information security at the Bachelor's, Master's or Doctoral levels. Practical expertise in information security was built up in the private sector, particularly in banks. Cyber Security Strategy set the objective that in Estonia's educational field there should be more contributing in cyber security issues. In year 2009 University of Tartu and Tallinn University of Technology started the joint programme

[16] Cyber Defence League's webpage http://uusweb.kaitseliit.ee/et/kuberkaitse-uksus accessed April 28, 2012.
[17] Estonian Information System's Authority's webpage http://www.ria.ee/CIIP/ accessed April 28, 2012.

on cyber security master program, other curriculas were revised and added courses in area of cyber security if needed.

Qualified specialists are also concern of NATO. NATO's Strategic Concept and the 2010 Lisbon Summit Declaration recognized that the growing sophistication makes the protection of the Alliance's information and communications systems an urgent task for NATO. In 2011 NATO Defence Ministries approved a revised NATO Policy on Cyber Defence which set a focus on preventing cyberattacks and building resilience. One out of four of the principal cyber defence activities are research and training. NATO accelerates efforts in training and education on cyber defence through existing schools and the cyber defence center in Tallinn.[18]

5.2 Analysis

Viira (2008) have brought out that the Estonian Government's strong political statements and actions on the cyberattacks brought the issue to the wider political arena and made the international community to pay more attention to topics related to network security and threats posed by cyberattacks in general. Same is stressed out by Kivimaa who says that after the attack, the problem of cyber security rose to the international center and attack perhaps was a very good trigger to tackle this challenge.

In Jaan Priisalu's opinion Estonia raised the leading country in topics related in cyber security and defence, but the advantage is slipping away.

> *In 2008 our Cyber Security Strategy was new in world. The world's most powerful state* [U.S.] *copied it and if the world's most powerful country is copying you that mean you are in top of the world.* Jaan Priisalu.

Unfortunately, the economic crisis caused a situation where it was not possible to fully carry out all activities stated in Cyber Security Strategy and in Priisalu's opinion this have influenced the position of Estonia in cyber security topics in world. It is so not because other countries have passed, but because the rapid development of cyber world:

[18] NATO homepage http://www.nato.int/cps/en/SID-2CD9B70B-541E1AA2/natolive/topics_78170.htm? Accessed April 29, 2012.

> *In 2007 attack was associated phenomenon, in 2008 in Georgia there were coordinated cyberattacks starting at the same time as the military action, in 2010 in Tunisia the riots on streets were caused by the cyber activity. The trend shows that in 2007-2011 was a transition in society when the cyber-based become the main tool for the attacks.* Jaan Priisalu

The essentiality of cooperation has been stressed out many times in this study and it is clear that combating cyber risk needs the cooperation in levels of businesses, organizations, ministries and states. As discussed by Tikk and Kaska (2010) both the environment where cyber activities take place, and the activities themselves by nature disregard national boundaries. This factor by itself makes the cyber realm especially sensitive to the efficiency of international cooperation in criminal matters. In their opinion, politically motivated cyberattacks are a persistent trend which means that nations are more and more dependent on other jurisdictions' ability and willingness to cooperate in criminal proceedings. Internet has not only created borderless virtual world, but also scattered real world's national borders. In order to perform investigation beyond their jurisdictional boundaries therefore have no effective way to prosecute perpetrators without assistance of other nations and international organizations, Tikk and Kaska have emphasized.

Tiirmaa-Klaar (2009) highlights specially the importance of cooperation between public and private sector IT security managers. Both the providers of vital public and private sector services depend on the business continuity of information systems. Ensuring the smooth operation of critical information systems under normal circumstances and minimum business continuity in a crisis situation is actually what cyber security is about. And in addition, action and recovery plans are needed to restore the functioning of information systems as soon as possible after a cyberattack. Kaju (2008) also points out that since most of the network is managed by private sector the cooperation is extremely important – ensuring cyber security in civilian infrastructure the key role is played by private sector.

The cooperation between private and public sector was the key on combating cyberattack in 2007. As Kivimaa explains, filters were put to the internet service providers on a way which made impossible to carry out more attacks from outside Estonian perimeter. The reaction itself was quick because the earlier same kind DDoS attacks against banks the contacts and agreements between authorities had already been done and therefore the response to attacks in 2007 was performed in hours. He stresses out that the main difficulty is the collaboration – between the service providers, internet service providers, server service providers, the object of attack and others. Cooperation must be prompt enough and it must have already been prescreened, so the results are in much better level. Kivimaa also points out important fact about the DDoS attacks – they are expensive for an attacker. Renting botnets is the more expensive the longer it lasts. In case of Estonia internet service providers put filters in first incoming routers to prevent attacks from outside; severe internal attack can not be done because in Estonia there is not large enough for big botnet. It appears that the small size of Estonia have created a good strategy of defence in case of cyberattack from outside.

In Kivimaa's opinion the most important act after 2007 is the creation of voluntary cyber defence union. Holding cyber security experts consistently on the public purse is not feasible; therefore the voluntary alliance is an ideal solution which provides fairly substantial capability of defence, Kivimaa states. Although there was cyber security community before the year 2007, the creation of official National Cyber Defence League offers the highly skilled IT professionals' help in case of emergency. Cyber Defense League has also raised awareness of cyber security issues.

Although it may seem like after 2007 every politician in Estonia is aware of the nature of cyber threats, it is not so. According to Priisalu, politicians are still asking whether we can deliver the cyber law. Reality is that cyber world is not going away, it is in everywhere and this is the reason why there cannot be one law for cyber world, but all laws must be changed so they are legislative also in cyber issues.

6 Summary

This chapter has provided an analysis of the data and findings obtained from the study. It explored what are the main lessons Estonia gained from the 2007 cyberattack.

As the societies are increasingly Internet-mediated the concern of cyber security issues is also increasing. As Lipson (2002) brings out the key concepts related to cyber security are based on the environment itself:

- The Internet environment is anonymous and its cross-border nature makes cybercrime or attack hard to track and investigate.
- Internet was designed on a robust way to make it resistant to external physical attack or accident; there was no concern with regards to the possibility of internal attacks by users.
- As attacks often cross multiple administrative, jurisdictional and national boundaries and there are no universal technical standards or agreements for performing the monitoring and record keeping necessary to track and investigate the attacks.

Rattray stated that as starting with 1986 the hacker phase started and in early 2000s begun the criminal/commercial phase of attacks. In mid 2000s begun even more advanced and dedicated phase. At the same time as in early 1990s attacks were conducted by amateurs and perhaps benevolent hackers, in early 2000s raised new money-motivated criminal and commercial phase attackers along with attack incident number – accordingly to Computer Emergency Response Team/Coordination Center (CERT/CC), the incident trend started rise rapidly in years 1999 and 2000 and have multiplied since then. It is also seen that if in early hackers' time the hacker was rather intelligent and the attack as it was not aggressive did need a specific knowledge in the field, but the attacks remained quite simple. Now conducting the attack does not need a special knowledge from the attacker, attacker can even outsource the service of an attack, but attacks have become more complex and aggressive. Priisalu said in his interview that the first difficulty, when attacked, is to determine that is attack not just a system failure or user error.

As attacks at early 1990s were carried out by hacktivist often in order to prove hacker's cleverness, the attacks were not remain secret, but rather was intended that attacked party could see that he is vulnerable, and probably the hacker also wanted to expose his/her identity to gain glory and fame in hackers' world. Now attacks are focused mainly on three core principles of information security: confidentiality, integrity and availability – principles of security are at the same time system's vulnerabilities and therefore threats (Gelbstein & Kamal 2002). When attacking those principles, at least at the beginning of the attack the victim often do not know of being under attack; the actual attack seems to be rather a system malfunction of user error.

In opinion of Jaan Priisalu attacker must obtain the position where the attack can be carried out continuously. This is the reason why the major attacks against system would not be the best idea from the viewpoint of an attacker – the attack would be identified easily and the countermeasures implemented quickly. Priisalu's opinion the more feared attack would be, for example, the attack against integrity and confidentiality and cause many little problems so it would take time until the attack is noticed and at the meanwhile, attacker can do more harm.

The key characteristics in Estonia's cyber security before 2007 attack were:

- At framework's level in year 1998 entered into force the Principles of the Estonian Information Policy which was the first document of the information society in Estonia. At first all frameworks focused on development of information society, but in year 2004 the policy was approved in where security concerns were first outlined – Principles of Estonian Information Policy 2004-2006.
- Private sector was more aware and had more knowledge in field of cyber security than government. On the level of government there was not so much concern of cyber security matters before the year 2007 as attack against state or public services, but against private sector businesses. At the same time major banks in Estonia were quite used to dealing with cyber threat, but the law enforcement capability was still relatively weak. Perhaps that the private sector had more experience in field of cyber security, from the beginning the private sector was greatly involved in developing the information society and every framework and policy underlined the importance of cooperation.
- At organizational level the most important act was the establishment of the Computer Emergency Response Team (CERT Estonia) in 2005. Also it is noteworthy that there already had started the process of establishing CCD COE in Estonia.
- At educational level in order to ensure education in field of information technology the Estonian Information Technology College (IT College) was founded in year 2000.

The major cyber security issues at Estonian Government level before the attack were:

- In year 2004 the Principles of Estonian Information Policy 2004-2006 policy was the first document where the security concerns were outlined.
- Private sector was more aware and had more knowledge in field of cyber security than government. Banks in Estonia were quite used to dealing with cyber threat, but the law enforcement capability was still relatively weak.
- Perhaps because the fact that the private sector had more experience in the field of cyber security, from the beginning the private sector was greatly involved in developing the information society and every framework and policy underlined the importance of cooperation.
- In 2005 the Computer Emergency Response Team (CERT Estonia) was established.

At 2007 Estonian Government and other institutions' like other governmental agencies, banks, media agencies, schools, Internet Service Providers, etc. suffered mostly under cyberattacks directed to the web sites. The three-week-long attack was carried out with political reasons in order to protest against moving the Soviet-era Bronze Soldier's statue. In order to combat the malicious traffic originated from outside the Estonia, some banks temporarily cut off all foreign traffic while remaining accessible for clients in Estonia (Ottis, 2008). Same was done later in order to protect Estonia's internal web. Goodman (2010) states that Estonia's response to the attacks proved effective – initially were Estonia's network closed off for some international traffic and states with numerous clients, but few attackers were slowly permitted back onto Estonian networks.

So far only one person has been convicted of carrying out cyberattacks in the spring of 2007. It is stressed out by Ottis (2008) that this conviction was possible only because he committed the attacks from Estonia and therefore enough evidence could be collected. As Russia did not agree to cooperate with Estonia in the investigation of attacks, the opinion was caused that attacks were either coordinated or at least approved by Russian government. However, there is no state-level common understanding or decision that Russian government had a leading role in this case, but Russia's behavior and legal decision not to assistance Estonia in investigation of cyberattack shows how difficult is to investigate those types of crimes and indicates the need of cross-border cooperation in the area. Goodman (2010) have stressed out that although cyberspace may be a stateless domain, the international law and domestic criminal laws should be updated and improved to hold states responsible, make them liable, or at least encourage mutual assistance in fighting cyberattacks that originate in their territory.

The major lessons learnt at Estonian government level after cyberattacks in 2007 are:

- After the attack in 2007 and lacking field specialists at educational level there was carried out several activities in order to revise the IT curriculas and if needed added courses in area of cyber security.
- As the government was not concerned of issues of cyber security before the attack in 2007, without the help of private companies who had already suffered under the attacks before and had the experience, the attack would have last for weeks with no solution.
- As the private companies who already had the needed contracts and agreements were cooperating in order to counter attacks, the solution of how to come over the attack was developed and implemented fast.
- As attack showed the importance of cooperation between private and public sector, the establishing the official National Cyber Defence League in basis of cyber security community. The volunteer-based league is supported by Estonia; it cooperates with different organizations in Estonia as well as other states in order to raise awareness of cyber security.

The practices implemented after attacks in 2007 were:

- In order to enhance cyber security policies' develops and implementations the Cyber Security Strategy sets the key objectives of cyber security. This document became the fundamental for every other policy document or framework in the field. The common understanding and approach to cyber security was developed and implemented.
- The establishment of official National Cyber Defence League which is voluntary-based institution for connecting high-skill-level specialists in Estonia in order to practice thru and therefore be ready for possible next attacks.
- In order to make sure that in educational level students get the necessary knowledge of field of cyber security there were carried out several activities in order to revise the IT curriculas and added courses in area of cyber security if needed.

Problems and challenges

The investigation of year 2007 cyberattack was difficult because of its cross-border dimension which prevented the identification of attackers. Although the attack is investigated so far, there is no certainty that the attackers will be identified. Estonia's case of cyberattack underlines the importance of cross-border cooperation in criminal investigation on cybercrimes. It also shows that how powerful and full of opportunities is the environment the Internet and other environments connected to it. It demonstrates that each country must consider the possible risks in terms of cyber security as also be prepared to protect themselves and deter the possible attacks. As cybercrimes often are not carried out in one single country, the international cooperation is essential in order to ensure cyber security for every country.

At the same time as the cross-border dimension of cyberattack blocked the investigation, it created a good opportunity in means of protection – restricting the international connection ended the attack from outside. As in Estonia there is no big botnets there remained no significant offensive capability for attackers. However, the fast reaction to attacks was possible only because there were contacts and agreements between authorities in public and private sector from earlier.

As Viira (2008) have brought out that the Estonian Government's strong political statements and actions on the cyberattacks brought the issue to the wider political arena and made the international community to pay more attention to topics related to network security and threats posed by cyberattacks in general. But in Jaan Priisalu's opinion Estonia raised the leading country in topics related in cyber security and defence, but the advantage may be slipping away as the economic crisis caused a situation where it was not possible to fully carry out all activities stated in Cyber Security Strategy and in Priisalu's opinion this have influenced the position of Estonia in cyber security topics in world. Not because other countries may have passed, but because the rapid development of cyber world. The trend shows that in 2007-2011 was a transition in society when the cyber-based become the main tool for the attacks, Priisalu admitted.

The key learnings

The key learnings from the 2007 cyberattack were:

- Need for the field of cyber security specialists.
- The government was not concerned of issues of cyber security before the attack in 2007, luckily private companies had already the experience and needed contacts and agreements in order to come over the cyberattack
- As attack showed the importance of cooperation between private and public sector, the establishing the official National Cyber Defence League in basis of cyber security community.
- Need for cross-border cooperation in investigating the crimes and attacks as also creating the law enforcement in terms of cyber related issues.

In conclusion, the time before the year 2007 developments were focused on developing new products and services and creating the suitable framework for economic dynamics; mostly activities were engaged in supporting and creating information society. At the same time private sector had to deal with cyber threats as banks, for example, was already suffering from attacks. Cyberattack in 2007 was a trigger to start fast changing of the field cyber security in Estonia. As there were actually needed people with specialist knowledge in private sector, the fast development of cyber security in Estonia was not difficult to achieve. After the 2007 the developments fastened at the area of cyber security – many frameworks were implemented and organizations created.

Although attack against Estonia was not too sophisticated or well-coordinated the nature of the attack was special - politically motivated cyberattack against Estonia (perhaps coordinated by the great eastern-neighbor), the first-time attack against country, some even called it the cyber war. Attacks in 2007 created for Estonia a unique opportunity to take the place among the world’s greatest – the area of cyber security was immediately taken by Estonians. In terms of cyber security Estonia was and is still one leading country among U.S. and others.

Chapter 4. Conclusion

This final chapter of the thesis presents conclusions about the findings of this research. It summarizes the key findings from data analysis. It focuses on the main issues learnt from the study which has been done by answering the research questions in a summarized form as well as pointing the implications of this research and possible future research ideas.

1 Main findings

This study gives an overview of how Estonia’s society has reacted to comprehensive long-term political cyberattacks at time when politically motivated cyberattacks were not so common. In this study have presented the lessons from cyberattack in year 2007 and provided an overview of the current situation in the field of cyber security in Estonia.

In order to bring out the lessons and changes in the field of cyber security in Estonia author has analyzed the developments in field before and after year 2007 cyberattack. Author believes that it is important to map the developments on the field to understand the changes and present the changes in a way which on one hand allows to see how Estonia have reached the point where it is a leading country in cyber security issues and on the other hand draws out the main shortcomings of the existing and possible problems in future in the field of cyber security.

The major lessons learnt at Estonian government level after cyberattacks in 2007 resulted from the attack and the issues on which there was expression of lack during the attack:

- Most important issue was the lack of knowledge in government level. As the government was not concerned on the issues of cyber security before the attack in 2007, without the help of private companies who had already suffered under the attacks before and had the experience, the attack would have last for weeks with no solution. And as the private companies had already the needed contracts and agreements the cooperating in order to counter attacks was carried out quite easily and the solution in order to come over the attack was developed and implemented fast.
- As government was missing specialists in the field, the revision of the IT curriculas was carried out and added courses in area of cyber security if needed.
- As attack also showed the importance of cooperation between private and public sector, the establishing the official National Cyber Defence League in basis of cyber security community. The volunteer-based league is supported by state; it cooperates with different organizations in Estonia as well as other states in order to raise awareness of cyber security. The establishment of official National Cyber Defence League which connects highly skilled specialists in Estonia in order to practice through and therefore be ready for possible next attacks.

In order to overcome the problems mentioned above, the Government established the Cyber Security Strategy 2008-2013 which sets the key objectives of developing cyber security in Estonia. Also the establishment of official National Cyber Defence League which is voluntarily-based institution for connecting high-skill-level specialists in Estonia in order to practice thru and therefore be ready for possible next attacks.

2 Implications of the research

The implication of this study is that the results can be used for assessing the current situation and developing a framework to national cyber security. In this study in given an overview the cyber security field in Estonia before 2007 cyberattacks and dynamics of changes after.

Understanding Estonia's major learnings from the year 2007 attacks and how they are implemented and the procedures that were followed in this process, might be very useful to others to support creating framing of cyber security policies.

3 Future research ideas

This study focused on the security aspects of Estonia and on procedures what were implemented in Estonia after cyberattacks in 2007. That study does not map all of the problems in field of cyber security. The future research ideas could be linked to political attacks focusing on the development of the dynamics of the attack.

Kokkuvõte / Summary in Estonian

“Küberjulgeolek Eestis: 2007. aasta küberrünnakute õppetunnid” on magistritöö, mis annab struktureeritud ülevaate Eesti poliitikas ja avalikkuses toimunud muutustest seoses küberrünnakutega aprillis ja mais 2007. aastal.

Käesoleva magistritöö uurimisküsimused on:

1. Mis olid suurimad õppetunnid Eesti valitsuse tasandil 2007. aastal toimunud küberrünnakust?
2. Millised tegevused viidi läbi pärast 2007. aastal toimunud rünnakut?

Nendest uurimisküsimustest tulenevalt on töö peamiseks eesmärgiks:

- Mõista põhimõisteid, mis on seotud küberjulgeoleku ja selle infrastruktuuriga.
- Mõista 2007. Aastal Eesti infrastruktuuri vastu toimunud küberrünnakute spetsiifikat.
- Analüüsida peamisi küberjulgeoleku küsimusi Eesti valitsuse tasandil enne ja pärast rünnakut.
- Mõista, mis olid peamised õppetunnid 2007. aasta küberrünnetest ja välja tuua muutused, mis võeti ette Eesti küberjulgeoleku edendamiseks.

Põhilised õppetunnid, mis rünnakutest tulenesid, olid järgnevad:

- Küberturvalisuse probleeme ei oldud valitsuse tasandil teadvustatud. Eraettevõtete abita võinuks rünnakute tagajärjed 2007.aastal olla laiahaardelisemad, aga kindlasti kestnuks rünne kauem. Kuna eraettevõtted olid juba varem kokku puutunud küberrünnetega, oli neil ka vajalik kogemus rünnetega toimetulemiseks. Samuti, varasemate rünnete tõrjumisest oli eraettevõtetel usaldus üksteise vastu ja sõlmitud vajalikud kokkulepped, mis oluliselt kiirendavad ründele reageerimist lubades kiirelt hakata tegelema kaitseplaneerimise ja -elluviimisega, selle asemel, et sõlmida kokkuleppeid.
- Kuna valitsusel olid puudu küberjulgeoleku spetsialistid, analüüsiti pärast 2007. aasta rünnet olemasolevaid IT-erialade õppekavasid ning vajadusel lisati küberjulgeoleku ja küberturvalisuse alaseid kursuseid.

- Rünnak näitas, kui oluline ja vajalik on koostöö era- ja avaliku sektori vahel. Kuigi juba enne 2007.aastat erialaspetsialistid omavahel suhtlesid, alustati aktiivselt ka riigi tasandil tööd loomaks Küberkaitseliitu. Vabatahtlik organisatsioon koondab küberturvalisusega tegelevaid spetsialiste Eestis ning tehakse koostööd mitmete rahvusvaheliste organisatsioonidega ja teiste riikidega. Samuti viiakse läbi harjutusi olemaks valmis võimalikuks ründeks Eesti riigi, selle kriitilise infrastruktuuri või muude osade vastu.

Selleks, et ületada eelpoolnimetatud probleeme, kehtestas valitsus Küberjulgeoleku strateegia 2008-2013, mis toetab küberjulgeoleku arengut Eestis. Samuti loodi Küberkaitseliit, mis ühendab kõrge oskusteabega spetsialistid Eestis ning pakub Eestile tuge küberrünnete tõrjumisel.

Töö on kirjutatud inglise keeles.

Bibliography

Aro, P. (2008) Computer Protection 2009. Information Technology in Public Administration of Estonia. Yearbook 2008. Retrieved January 15, 2012 from http://www.riso.ee/et/et/pub/2008it%20.

Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing. Retrieved May 1, 2012 from http://www.cloudsecurityalliance.org/csaguide.pdf.

Bryman, A. (2006) Integrating quantitative and qualitative research: how is it done? Qualitative Research 6(1), 97-113.

Carr, J. (2009) Inside Cyber Warfare. Mapping the Cyber Underworld. Retrieved January 10, 2012, from http://www.security-gurus.de/papers/cyberwarfare.pdf.

CSIS Commission on Science and Security. (2002) Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories. A. Witkowsky (director). Retrieved April 5, 2012 from http://csis.org/files/publication/020425_Hamre_ScienceSecurity_web.pdf.

Cyber Security Strategy Committee Ministry of Defence (2008) Cyber Security Strategy. Retrieved April 26, 2012 from http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

Czosseck, C., Ottis, R. and Talihärm, A.M. (2011) Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. In Proceedings of the 10th European Conference on Information Warfare and Security, Tallinn, Estonia, 7-8 July. Reading: Academic Publishing Limited, July, 57-64.

Denning, D. E. (2000) Statement of Dorothy E. Denning. Retrieved April 11, 2012 from http://www.fas.org/irp/congress/2000_hr/00-05-23denning.htm.

Department of State Information Systems of the Ministry of Economic Affairs and Communications. (2005) Estonian IT Interoperability Framework. Abridgement of version 2.0. Retrieved April, 24, 2012 from http://www.riso.ee/en/files/framework_2005.pdf.

Estonian Information System’s Authority (RIA). (December 14, 2007) Kooperatiivse Küberkaitse Kompetentsikeskus (K5) [Slideshow] Retrieved March 28, 2012 from http://www.ria.ee/public/CERT/K5_briif_avalik.pdf.

EUROPOL Public Information. (2011) Threat Assessment (Abridged). Internet Facilitated Organised Crime, iOCTA. Retrieved Januari 12, 2012 from https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P. (2011) Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural. *IEEE Technology and Society Magazine*, Spring 2011, 28-38.

Gelbstein, E., Kamal, A. (2002) Information insecurity: A survival guide to the uncharted territories of cyber-threats and cyber-security. New York: United Nations.

Goodman, W. (2010) Cyber Deterrance. Tougher in Theory than in Practice?. *Strategic Studies Quarterly*. Fall 2010, 110-114.

Greenberg, A. (2007) The top countries for cybercrime. China overtakes U.S. in hosting Web pages that install malicious programs. Forbes.com Retrieved January 10, 2012 from http://www.msnbc.msn.com/id/19789995/.

Greene, S. S. (2006). Security policies and procedures : Principles and practices. Upper Saddle River, N.J.: Pearson Prentice Hall.

Heath, N. (2008) Nato: Cyber terrorism ‘as dangerous as missile attack’. Software.silicon.com. Retrieved April 10, 2012 from http://www.silicon.com/technology/security/2008/03/07/nato-cyber-terrorism-as-dangerous-as-missile-attack-39170300/.

Howard, J. D., Longstaff, T. A. (1998) A Common Language for Computer Security Incidents.

Hypponen, M. (2012) Crime, computers and security in 2012. NATO Review magazine. Received April 29, 2012 from http://www.nato.int/docu/review/2012/2012-security-predictions/Crime-Computers-Security-2012/EN/index.htm.

Jayashree, S., Marthandan, G. (2010) Government to E-government to E-society. Journal of Applied Sciences. 10: 2205-2210.

Jayawickrama, W. (2008) Cyber Crime – Threats, Trends and Challenges. Computer Security Week 2008. Brisbane.

Johnson, B. C. (2010) Information Security Basics. ISSA Journal, 8(7), 28-34.

Kaju, A. (2008) Küberkaitse – Eesti võimalus ja vastutus. Maailma Vaade. 5. Retrieved April 25, 2012 from http://www.maailmavaade.ee/?d=kuberkaitse0408.

Kumar, V., Srivastava, J., Lazarević, A. (2005) Intrusion Detection: A Survey. V. Kumar, J. Srivastava, A. Lazarević (Editors), Managing Cyber Threats: Issues, Approaches, And Challenges, 5, 24-26.

Laherand, M-L. (2008) Kvalitatiivne uurimisviis. Kirjastus Meri-Liis Laherand.

Layne, K. Lee, J. (2001) Developing fully functional E-government: A four stage mod. Government Information Quarterly. 18 (2), 122-136.

Leeson, P. T., Coyne, C. J. (2005) The Economics of Computer Hacking. Journal of Economic Behaviour and Organization. 57 (2) 241-244

Lin, P., Allhoff, F., Rowe, N. C. (2012) Computing Ethics War 2.0: Cyberweapons and Ethics. Communications of the ACM, 55 (3) 24-26.

Mägi, H. Vitsut, L. (2008) Infosõda: visioonid ja tegelikkus. Tallinn: Eesti Ekspressi Kirjastuse AS.

Ministry of Economic Affairs and Communications Department of State Information Systems. (2006) Information Technology in Public Administration of Estonia Yearbook 2005. R. Randver (Editor). Retrieved April 22, 2012 from http://www.riso.ee/en/pub/yearbook_2005.pdf.

Ministry of Economic Affairs and Communications. (2007) Cabinet Approves Action Plan to Fight Cyber-attacks. [Press release]. Retrieved April 26, 2012 from http://www.mkm.ee/304845/.

Moon, M. J. (2002) The Evolution of E-Government among Municipalities: Rhetoric or Reality? Public Administration Review. 62 (4) 424-433.

Oorn, R. (2008) “Cyber War” and Estonia: legal aspects. I. Odrats (Editor), Information Technology in Public Administration of Estonia Yearbook 2007. Tallinn: Vali Press OÜ.

Ott, A. (2004) ICT Development in the Public Administration of Estonia. I. Odrats (Editor), IT in Public Administration of Estonia Yearbook 2004. Tallinn: Piltkiri OÜ

Ottis, R. (2008) Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. In Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth. Reading: Academic Publishing Limited, 163-168.

Rattray, G. (2010) Emerging Cyber Security Risks: A Multi-Level Challenge. [Presentation] Retrieved April 11, 2012 from https://www.stmarytx.edu/ctl/pdf/Rattray.pdf.

Rufi, A. (2006) Network Security 1 and 2 Companion Guide. Cisco Press.

Schjolberg, S., Ghernaouti-Helie, S. (2011) A Global Treaty on Cybersecurity and Cybercrime. Second edition. Oslo: AiTOslo.

Siau, K., Long, Y. (2005) Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. Industrial Management & Data Systems. 105 (4), 443–458.

Stauffacher, D., Sibilia, R., Weekes, B. (2011) Getting down to business: Realistic goals for the promotion of peace in cyber-space. A Code of conduct for Cyber-conflickts. ICT4Peace Foundation. December 2001.

Tepandi, J. (2007) Co-operation in the field of information security. I. Odrats (Editor), Information Technology in Public Administration of Estonia. Yearbook 2007. 16-18. Tallinn: Vali Press OÜ.

The Estonian Association of Information Technology and Telecommunications (2009) Activity plan for 2009-2011 Retrieved April 26, 2012 from http://www.itl.ee/?op=body&id=111#Cooperation_with_other_professional_associations.

The Estonian Association of Information Technology and Telecommunications (2011) Activity plan for 2011-2013 Retrieved April 26, 2012 from http://www.itl.ee/?op=body&id=247.

Thomas, R. Martin, J. (2007) The underground economy: Priceless. *;login:*, 31 (6), 7-16.

Thuraisingham, B. (2005) Managing threats to web databases and cyber systems. V. Kumar, J. Srivastava, A. Lazarević (Editors), *Managing Cyber Threats: Issues, Approaches, And Challenges*, 5, 3-17.

Tiirmaa-Klaar, H. (2009) Cyber security: a part of internal, External and economic security. IT in Public Administration of Estonia Yearbook 2008. Retrieved April 25, 2012 from http://www.riso.ee/et/et/pub/2008it.

Tikk, E., Kaska, K. (2010) Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. Paper presented at the 9th European Conference on Information Warfare and Security, Thessaloniki. Retrieved April 28, 2012 from http://www.ccdcoe.org/articles/2010/Tikk_Kaska_LegalCooperation.pdf.

Tisdall, S. (2010) Cyber-warfare ‘is growing threat’. The Guardian.

Traynor, I. (2007) Russia accused of unleashing cyberwar to disable Estonia. The Guardian. Retrieved January 10, 2012 from http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Viira, T. (2008) Cyber attacks against Estonia – overview and conclusions. CIIP MERIDIAN newsletter. 2, 1. January 2008.

Weimann, G. (2004) Cyberterrorism: How Real Is the Threat? United States Institute of Peace, Special Report 119. Retrieved April 11, 2012 from http://www.usip.org/files/resources/sr119.pdf.

Whitman, M. E., & Mattord, H. J. (2004). Management of information security. Boston, Mass.;United Kingdom: Thomson Course Technology.

A Questionnaire

A.1 Questionnaire in English

1. Please characterize the Estonian cyber security situation before attacks in 2007.
    a. In your opinion, why the attackers succeeded in the 2007 attack?
    b. What were wrong or missing and therefore made attacks possible?
2. What happened in 2007?
    a. What were the biggest lessons learnt from the attacks?
    b. What was done to overcome of the attacks?
3. What were the changes after?
    a. What were/are the main developments in area of cyber security?
    b. What were/are the biggest obstacles or places of thought?
    c. What was done in order to overcome these obstacles?

A.2 Questionnaire in Estonian

1. Palun kirjeldage Eesti küberturbe maastikku enne 2007.aasta aprillis ja mais toimunud küberrünnakut.
    a. Miks ründajad 2007.aastal Teie hinnangul õnnestusid?
    b. Mis oli valesti või puudu, mis tegi rünnakute õnnestumise võimalikuks?
2. Palun kirjeldage lühidalt, mis juhtus 2007.aastal.
    a. Mis olid suurimad õppetunnid 2007.aasta rünnakust?
    b. Mida võeti ette rünnakute tõrjumiseks?
3. Millised olid muutused pärast 2007.aastat?
    a. Mis olid/on suurimad muutused küberturbe/küberkaitse valdkonnas?
    b. Mis olid/on suuremad raskused, mida tuli/tuleb ületada saavutamaks väga heal tasemel küberturvet?
    c. Mida on tehtud selleks, et eelpoolnimetatud raskustest üle saada?

B Transcripts of interviews

B.1 Interview with Rain Ottis

1. Please characterize the Estonian cyber security situation before attacks in 2007.
The Estonian cyber security situation was undergoing several key developments at the time. The CERT-EE had just been established, and CCD COE was in the process of being established. Estonia had implemented a national ID card and numerous services that could use it (including internet voting, which was done on a local level in 2005 and for parliamentary elections about a month before the cyberattacks of 2007).

In practical terms, the primary perceived cyber security risk at the time was criminal in nature (attacks against banks and their customers). The major banks in Estonia were quite used to dealing with this type of threat, but the law enforcement capability was still relatively weak.

a. In your opinion, why the attackers succeeded in the 2007 attack?
In my opinion, the attackers failed in 2007. There were no serious or critical effects on the population or the economy as a result of cyberattacks. The attackers lacked legitimacy and overreacted on the Bronze soldier issue. As a result, Estonia got a "diplomatic victory" in an event that could otherwise have been interpreted in various ways by the Western media.

b. What were wrong or missing and therefore made attacks possible?
The type of attacks that were generally used (DDoS) do not exploit security vulnerabilities other than capacity. The effectiveness depends on size mismatch between the attacker and defender. Therefore, these attacks were and are possible in every country, but they may not be as effective in some places.

2. What happened in 2007?
I think that some people (likely numbering in the hundreds, perhaps in the thousands) responded to a one-sided and biased media portrayal of the Bronze Soldier riots by performing (mostly primitive) cyberattacks against Estonian systems. Government role in the event remains unproven, except for the fact that the Russian government refused law enforcement cooperation to investigate the cyberattacks.

a. What were the biggest lessons learnt from the attacks?
Communicate, share information and use personal networks/contacts for quick response.

b. What was done to overcome of the attacks?
International cooperation - cutting off attack traffic closer to the source by filtering traffic or taking down bots in other countries.

Good relations and cooperation between CERT-EE, the Estonian telecommunications companies and banks. Endurance - The attacks came in waves and lasted for about three weeks.

Most attackers got tired of this much sooner. Basically, one can wait them out. White-listing - only allowing communications from "friendly" network segments.

3. What were the changes after?

a. What were/are the main developments in area of cyber security?
See the 2011 article. [Czosseck, C., Ottis, R. and Talihärm, A.M. (2011) Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. In Proceedings of the 10th European Conference on Information Warfare and Security, Tallinn, Estonia, 7-8 July. Reading: Academic Publishing Limited, p 57-64.]

b. What were/are the biggest obstacles or places of thought?

2007 attacks will not repeat in the same way. We must be careful not to plan for the last conflict.

We must not rest on our "laurels". Just because we were attacked five years ago does not mean that we will never be attacked again.

Since there were no critical effects from 2007, many people doubt as to whether cyber is a serious threat. Let me remind you that in 2007 we saw one of the most primitive attack scenarios imaginable, which was only using brute force. A clandestine, well targeted and executed attack could have serious consequences for a state.

c. What was done in order to overcome these obstacles?

This is an ongoing process of awareness raising and education.

B.2 Interview with Jüri Kivimaa

1. Palun kirjeldage Eesti küberturbe maastikku enne 2007. aasta aprillis ja mais toimunud küberrünnakut.

Ma ei ole võibolla kõige õigem inimene sellest rääkima – selle kohta on kindlasti palju kättesaadavat materjali.

a. Miks ründajad 2007. aastal Teie hinnangul õnnestusid?

Üldse on teine küsimus, kas nad õnnestusid või ei. Kas ründajad õnnestusid, on üks asi, aga Eestile oli juhtum mitmes valdkonnas ja mõttes väga kasulik. Paremat reklaami NATO küberkaitsekeskuse jaoks on võimatu välja mõelda. Mõned veebisaidid õnnestus natuke ära solkida, mõned õnnestus maha võtta, pankade tööd õnnestus natuke segada, aga mingeid väga suuri olulisi ebaharilikult tõsiseid asju minu meelest ei õnnestunudki teha. Kui esimene DDoS Hansapanga vastu oli paar aastat enne 2007. aastat, oli Hansapank ikka paar päeva maas. Tänu nendele varasematele kogemustele oli 2007. aastal vaid paar tundi maas. Selle mätta otsast võttes oli palju hullemate tagajärgedega väga suuri ja organiseeritud rünnakuid olnud juba.

b. Mis oli valesti või puudu, mis tegi rünnakute õnnestumise võimalikuks?

Rünnakuid takistada ei ole võimalik – kui keegi tahab rünnata, siis ta ründab. Kas nendega midagi saavutati või mitte, on iseasi. Minu arust mitte ja probleem tõusis väga suurde rahvusvahelisse keskpunkti, oli väga hea *trigger* selle probleemiga tõsisemalt tegeleda. Kuna esimene mitte nii vapustav rünnak põhjustas sellise tõsise tähelepanu teemale, oli võibolla isegi väga hea intsident teema tõstmiseks.

1a. Mis olid suurimad õppetunnid 2007.aasta rünnakust?

Mina ütleks, et üldse küberrünnakute osas on probleem, et selleks, et neid rünnakuid tõrjuda, peab olema tõsine seltskond inimesi koos, kes hakkavad juba internetiteenuse pakkujate juures Eesti perimeetri peale filtreid ette panema. Peab olema suurem grupp inimesi. Selleks, et seda pidevalt koos hoida, oleks vaja väga suurt materiaalset ressurssi ja teiseks ilmselt tekiks Eestis ekspertide puudus, ei ole nii väga küberturbe eksperte, nad on üsna defitsiitsed. Alustati riigi tasemel tõsisemalt selle probleemiga tegelemist – küberkaitse strateegia töögrupid ja nii edasi. Aga mina ütleks, et põhiline oli, et tekkis küberkaitseliit. See on tõsine vabatahtlik organisatsioon ja ainuke reaalne võimalus, kuidas ilma üle mõistuse suuri ressursse kulutamata on võimalik tekitada ja tagada küllalt oluline tõrjevõimekus. Eesti riigi mastaabis oli oluline küberkaitse strateegia loomine ja et alustati küberkaitseliidu loomist. NATO Kompetentsikeskuse ja küberkaitseliidu ideede suureks algatajaks oli Johannes Kert.

2b. Mida võeti ette rünnakute tõrjumiseks?

Põhiline oli, et tekitati filtrid internetiteenuse pakkujate juurde juba nii, et väljas poolt Eestit ei olnud võimalik enam rünnakuid teostada. Eestisiseselt ei olnud isegi panganduses olulisi probleeme ega katkestusi. Rahvusvahelised ülekanded olid küll teatud perioodil raskendatud, aga selliste asjade jaoks on pangad välja töötanud varulahendused, et kui Eesti perimeeter kinni pannakse, tuleb kuskilt ümber nurga see ühendus. Rahvusvahelised ülekanded pole ka väga massilised, 90% -95% pangaülekannetest toimuvad eestisiseselt.

Oma kogemuste põhjal võin öelda, et saadi väga kiiresti hakkama. Kahe tunniga. Ja saadi just hakkama tänu sellele, et seal midagi väga erilist uut ja ootamatut ei toimunudki. Põhiline oli DDoS ja esimesel korral selle tõrjumiseks asutustevaheliste sidemete paikapanek võttis aega paar päeva, aga kuna see oli kõik tehtud, tehti see asi ära paari tunniga. Tänu varasematele kogemustele, kui keegi ikka võtab DDoS-i ette, on see ka ründajale teatud kulu – botnettide teenuse ostmine ja mida pikemalt seda tehakse, seda kallimaks läheb see ka ründajale. Selle vastu midagi ette võtta pole võimalik, kui keegi ikka tahab internetist rünnata, siis ta ründab. Kes nüüd rohkem kahjusid kannab ja kuidas neid tõrjuda, on juba järgmine küsimus. Tõsist sisemist rünnakut ei ole võimalik panga vastu ette võtta, pole lihtsal piisavalt suuri botnette ja see, et Eesti internetiteenuse pakkujad panevad oma esimestesse ruuteritesse filtrid üles ja ei lase väljapoolt ründeid sisse on Eesti jaoks väga hea tõrjestrateegia.

3a. Mis olid/on suurimad muutused küberturbe/küberkaitse valdkonnas?

Hakati tõsiselt riigi tasemel tegelema küberturbega, koostati küberturbe strateegia aastaks 2008. Ja teine väga oluline asi on küberkaitseliit. Ja see on väga tõsist tegevust alustanud. Juba on tekkinud ametlik struktuuriüksus.

b. Mis olid/on suuremad raskused, mida tuli/tuleb ületada saavutamaks väga heal tasemel küberturvet?

Ega põhiraskus ongi koostöö – teenusepakkujate, internetiteenuse pakkujate, võibolla serverteenuse pakkujate ja lõpprünnakuobjekti ja teiste vahel peab olema küllalt operatiivne ühistöö ja see peab olema juba eelnevalt läbi tehtud, nii on tulemused palju paremal tasemel. Õnneks Eestil kõige olulisemalt majanduslikud kahjud olid tulid pangandusest ja õnneks olid seal eelnevalt sellised situatsioonid läbimängitud. See, et räägitakse, et olid miljardilised kahjud, on minu meelest suhteliselt uskumatu – kust see number tuleb? Kui pank kaks päeva ei tööta, võib öelda küll, et kahepäevane kasu jäi saamata, aga need kliendid, kes kahel päeval ei saanud oma pangateenuseid kasutada, teevad siis paar päeva hiljem, raha tuleb nii ehk nii paar päeva hiljem. Pankade suured kahjud on võibolla natuke subjektiivne väide. Kahjusid kandsid nad kindlasti, aga paari aasta pärast saavad nad kahjumid kuhjaga tagasi, see on suhteline mõiste. Mingil hetkel tulevad kahjumid, mis tagavad hiljem suured kasumid.

c. Mida on tehtud selleks, et eelpoolnimetatud raskustest üle saada?

Strateegia loomine ja seal on konkreetsed tegevused paika pandud, mida tuleb teha ja minu meelest kõige olulisem on küberkaitseliit, kuhu on vabatahtlikud kokku korjatud. Sest sellist seltskonda pidevalt riigi rahakoti peal ülal pidada pole mõeldav ja seega on küberkaitseliit ideaalne lahendus – huviliste seltskond on kokku viidud, nende koostöö on tehtud suhteliselt mugavaks. Enne 2007. aastat oli olemas küll täielikult vabatahtlik küberturbe inimeste kooslus, aga nüüd on küberkaitseliidu kaudu ka Eesti riik sellele oma õla alla pannud ja selle võrra on läinud vabatahtlike tegevus mugavamaks ja samuti on ka riigil neid parem niiöelda kasutada.

B.3 Interview with Agu Kivimägi

1. Palun kirjeldage Eesti küberturbe maastikku enne 2007.aastal toimunud küberrünnakut.

Riiklikud struktuurid – CERT oli juba olemas. CERTi ülesanded olid infovahetamine, ei olda korda loov nagu politsei tagab avalikku korda. Ei olnud siis, ega pole ka praegu veel. Enne

2007 riiklikust küberjulgeolekust väga ei räägitud ja ega ka ilmselt meie potentsiaalne kübervaenlane ei käsitlenud seda nii metoodiliselt. See, mis 2007 juhtus, oli veebiteenuste rünne, mis on varasematest eestispetsiifiline. Kui vaadata teenuseid nagu hoogle veebileht, kui see liiklus peaks kogemata Eestisse suunatama, ongi Eestis kõik teenused maas. Eesti andmeside mahud on väikesed, kanalid kitsad, me lihtsalt ei pea sellisele koormusele vastu. Mis tehti – viidi Eesti olulisemad lehed platvormi peale, mis suutis kogu selle ründe ära teenindada. Nüüd on tagasi oma serverites. Ma arvan, et Ameerikas ei kardeta sellist rünnet, nad on juba ärilistel eesmärkidel töötavad suuremaidki voogusid. Mõnes mõttes on selline väike tegija vastu suunatud rünnak, kuna me oleme väike riik. Kriitilised teenused on väikese mahuga. See on Eesti spetsiifika. Need rünnakud, mis julgeolekut ohustasid, näiteks ameerika suunas või iraani tuumajaamade rünnakud, on hoopis teistsugused. Enne 2007 selles kontekstis üldse ei mõeldud, mis see riigi julgeolekut ohustav rünnak on. Pigem sellised asjad, mis Tuneesias [2010] toimusid, on palju kardetavamad, kui need, mis meil siin juhtus meie veebilehtede vastu. Aga sellest nüansivahest ei saa enamus otsustajaid ja poliitikuid aru. Ehk see, mida praegu käsitletakse küberründena, on tegelikult rünne, mis Eesti jaoks on halvav, kuna Eesti võime suuri infomahte töödelda on praktiliselt olematu, aga Hiina näiteks ei paneks taolist rünnet üldse tähele.

Mingid struktuurid olid, aga ei mõeldud selles kontekstis. K5 siiatoomine ja küberkaitseliidu alustamine oli algatatud enne 2007, aga nad olid initsiaatoriteks turvateadlikud inimesed – pankade turbejuhid ja just need, kes turvet vajavad. Turvet osutavad või selles saavad väga palju kaasa aidata ettevõtete teenusepakkujad, aga nemad ei mõtle selles kontekstis samamoodi nagu turbevajajad. Neile on suur liiklus äri, nemad teenivad selle eest raha. Kui turbevajaja neilt midagi tellib, mõtlevad nad lahenduse välja ja selle eest makstakse, aga midagi ennetavat, et näiteks panga suunas liikuvat liiklust kuidagi ära pesta, see ei ole kuidagi nende huvides. Selle tõttu, turbe edendamisega on tegelenud rohkem turbe vajajad, pangad ja teised seda tüüpi asutused. Riiklikul tasandil siin muud polegi kui RIAs on andmeside osakond. Nemad muidugi rolliks on riigi ja võrgu tervist tagada, nemad töötavad välja tehnilisi lahendusi, et tagada riigi teenuste töö.

Aga eks katalüsaatoriks oli ikkagi 2007, enne seda võimekust liiklust niimoodi selekteerida ei olnud. Initsiatiivid olid kõik olemas ja vedasid just turvet vajavad asutused, kes tajusid, et nende äri sõltub sellest, et teenused on *up and running*.

Eks riigil on ka hulk veebilehti ja nende püstioleku ja töötamise eest ka muretseti, aga kindlasti on riigi veebilehe maasolek vähekriitilisem presidendi kantseleile kui pangale. Samas ilma riigita ei saada. Pangad, kui mõnele kurjamile nö jälile saavad, ei saa nad ise midagi teha, käsi raudu panna ega midagi. Nii et pangad tegid väga tõsist koostööd kriminaaluurijatega. Siin on olnud palju edulugusid just sellest koostööst sündinud.

Kompetents on ka politseis olemas, kuidas küberkurjamitega võidelda.

Ega ma praegu ei näegi, milline teine ärisektor kannataks niivõrd rünnakust. Muidugi energiasektor, vesi, aga miks me seal ründeid ei näe, on see, et kriminaalil puudub praegu mehhanism, kuidas raha kätte saada sealt. Ja riiklikult motiveeritud ründajad – ei ole parasjagu sõda käsil. Kindlasti on idanaabri kübersõdijatel mingisugune sõjaplaan olemas, kuidas halvata meie elektri või veetootmist, mis iganes transporti ja lennuliiklust, aga kuna parasjagu sõda ei käi, siis neid plaane ellu ei viida.

Riiklikes konfliktides on selline mõiste nagu proportsionaalsus – kuigi mingitel riikidel on tuumarelv olemas, ei lasta seda käiku, kui on mingi väiksem jagelemine. Ma arvan, et sama ka küberrelvaga. 2007. aasta konfliktis Eesti elektrisüsteemi halvamine ei oleks olnud ilmselt proportsioonis.

2a. Mis olid suurimad õppetunnid 2007. aasta rünnakust?

2007 oli õppetund, näitas ära üldise kuhu uue aja konfliktid suunduvad. Näitas ära ka selles, kuidas uue aja konflikte tuleb käsitleda ehk Eesti vastusammudes oli väga suur rõhk tegelikult

PR kontseptsiooni väljatöötamisel ja elluviimisel. Esiteks sõnumid, mis välismaale saadeti. See kontseptisoon töötati kenasti välja, koosnes kolmest sõnast, mis olid paika pandud ja mida tuli igas võimalikus kohas, kus sõna võeti, korrutada. Ja see kontsept hakkas tööle. Eesti sai ohvri maine, Eesti sai toetuse rahvusvahelise ja välismaise ja siis ka küberriigi kuulsuse.

Kas nüüd võitnud või mitte - ma ei nimeta seda võiduks. Aga Eesti on selles valguses end positsioneerinud, oma niši kübermaailmas võtnud ja oma rahvusvahelise rolli leidnud. Eesti on nüüd justkui rahvusvahelisel tasandil tegija, oma suurusega võrreldes, oleme kübermaailmas olulised. Meid valitakse partneriteks kohtades, kus üldiselt tegutsevad suurriigid. See on meie suhteid ka ameeriklastega tihendanud – küberkaitseliit käib tihedasti ameeriklastega läbi.

Loodi kaks rühma – Tallinnas ja Tartus. Tallinna rühma asutajaliige olin mina. Kui need rühmad olid loodud, loodi kaitseliidu koosseisus maleva õigustes küberkaitse üksus kahe rühma baasil. Tegelevad nagu kaitseliidu roll üldiselt on – ettevalmistus. Seaduses on kirjas, et kaitseliit valmistub ette vastavalt kaitseväe plaanidele. Kuna Eesti kaitseväes aga vastavaid õppekavasid või plaane pole, on küberkaitseliit huvitav – sellest võibki saada Eesti kaitseväe küberkaitseüksus. Oleme teinud 2 staabiüksusõppust otsustajate tasandil küberkaitse õppust. Üks siis vabariigi valitsuse kriisikomisjoni staabiüksus. On osaletud ka spetsialisti tasandil õppustel, kus stimuleeritakse mingeid konkreetseid ründeid, mis tuleb ettevalmistatud tootmisüksust kaitsta.

3. Millised olid muutused pärast 2007.aastat?

Alustati küberjulgeoleku strateegia loomisega.

Muutus ka küberkaitseliidu loomine väga konkreetseks. Kui mõtteid oli varem välja käidud, siis hakkas kaitseminister sel teemal sõna võtma. Igasugu muid initsiatiive oli ka – haridusministeerium lõi õppekavasid, justiitsministeeriumis käis töö sel teemal, et seal arendada välja küberünnete avastamise ja tõendite kogumise võimekus.

CERT kasvas ja loodi veel üks osakond – kriitilise infoinfrakaitse osakond, mis tegeleb turbenõuete väljatöötamisega. Töötati välja hädaolukorra plaan, hädaolukorra seaduse alusel peavad kõik kriitilise teenuse osutajad plaanid välja töötama ja üks ulatuslik küberrünnak on meil ka sinna plaani pandud.

Esimese küberjulgeoleku strateegia mõtles välja kaitseministeerium, hiljem andis selle majandus- ja kommunikatsiooniministeeriumile üle. RIA muudeti täitevvõimu asutuseks. Tal peaks olema nüüd rohkem volitusi teha järelvalvet küberjulgeolekut tagavate meetmete rakendamiseks. See on ka oluline samm, et julgeoleku tagamine see on tehtud täitevvõimu osaks ja üleandeks. Enne riik ei kohustanud ettevõtteid küberjulgeolekuga tegelema, aga nüüd on asutus, millel on nõudeid seadev ja nõuete täitmist järelvalvav roll. Protsess on ikkagi algusjärgus, ühtegi asutusejuhti ei trahvita, kui ta ei rakenda meetmeid. Aga arvan, et viie aasta pärast rahulikult, kui on nõuded juba tükk aega kehtinud ja näiteks mingi energiaettevõtte juht ei rakenda piisavalt meetmeid, tuleb inspektor ja teeb ettekirjutusi. See on just viidud täitevvõimu roll on tekkinud.

Küberkaitseliit on ka nüüd seadustesse sisse kirjutatud. Küberkaitseliit on selles punktis huvitav organisatsioon – ühendab neid inimesi, kes on võimelised turvet pakkuma, kellel on see roll turvet pakkuda. Erinevalt sõjalisest riigikaitsest ei ole võimalik küberturvet pakkuvat üksust mingit objekti kaitsma. Aga mingid funktsioonid, mis tekivad kriisiolukorraga, selle jaoks spetsialistide ettevalmistamine ja see on KKL ülesanne. Kriisiolukorras on vajalik ju adekvaatne info ja info levitamine ja selle usaldusväärsus, info ei saa olla avalik ja samas peab olema piisav usaldussuhe, et mingisuguseid samme saaks kohe teha. Paljud asjad on ka juriidiliselt keerukad – näiteks on vaja kellelgi netiühendus ära võtta või midagi ümber teha, siis tavaliselt kui see on seotud ärisuhetega, on seal siduvad lepingud. Riigis näiteks, kuidas saaks üks asutus osutada teisele mingit teenust ilma, et direktorid omavahel kokku lepiksid. Tavaolukorras oleks sellist olukorras toimingute tegemine mustmiljon kooskõlastust ja juristi nõuannet. Kriisiolukorras peab käitumine olema teistsugune. Esiteks kui nad tunnevad üksteist ja neil on üksteise vastu usaldus, KKL ongi organisatsioon, kus usaldussuhe tekib ja annab ka väljaõppe. Üheski riigis ei olegi küberkaitse mudelit. Küll on küberründe mudel, kes allub sõjalisele juhtimisele ja viib operatsiooni läbi. Aga sõjalist küberkaitset korraldada on palju keerukam. KKL on eksperimentaalstruktuur riigi julgeolekut tagava küberturbe tagamisel.

Poliitilised ründed üldjuhul maskeeritakse kas huligaanseteks või kriminaalseteks, me väga täpselt ei tea, kes seal taga on. Sellist selgelt meie poliitilisele vaenlasele omistatavat küberrünnet ma ei tea hilisemast. Aga kriminaalne rünnakute voog on pidev ja selle vastu peab kogu aeg suutma valmis olla. Küberkaitseliidul, ma ei ütleks, et eriline roll oleks mingi konkreetse ründe tõrjumisel, küll on olnud roll info vahetamisel. Konkreetne roll näiteks oli e-valimiste ettevalmistamisel. Seal rünnati CERT-i enda palvel e-valimiste keskkonda.

Kuna Euroopa Liidu riigid vahest nii teravalt ei taju seda ohtu, neil puudub ka arusaam ja ka reaalne vajaduse end sellisel tasandil ette valmistada. Me oleme kübersõja rindel, me oleme väga sõltuvad ja seega haavatavad. Teised pole nii haavatavad. Ja teiseks on meil ka selged poliitilised vaenlased erinevalt vanade Euroopa riikidega, kel ei ole konflikti küberründe võimeka riigiga. Võibolla konfliktid Araabiamaades võiksid neid ohustada, eks ole ka mingite endiste asumaade konfliktid. pigem siis juba euroopa riike ohustada meelsusründed. Näiteks mis tekkisid seoses *wikileaks*-iga. Väga hea ettevalmistusega isikute grupp, aga nemad ründasid mitte riike vaid teatud institutsioone – pankasid näiteks. Eks sealt võibolla tajutakse seda ohtu aga kindlasti mitte sellisel määral nagu Eestis.

Ameeriklased võtavad aga väga tõsiselt. Eestil on nendega ka suhteliselt tihedam koostöö. Nemad tajuvad ka enda sõltuvust riiklikust infosüsteemist ja nad on ka tõeliselt arenenud. Eks arendatakse nii rünnet kui kaitset, aga kuna ebasümmeetria on väga suur, kui võrrelda klassikalise ründetegevusega – head kaitsemudelit ei ole näinud. Sõjalisel struktuuril ei ole väga lihtne teha koostööd erasektoriga, aga enamus sektorist, mida tuleb kaitsta, ongi erakätes. See on üks probleem, kuidas sõjalist riigikaitset korraldada objektide suhtes mis on erakätes. Ameeriklastel on samasugune organisatsioon nagu meil on kaitseliit - rahvuskaart. Paar aastat tagasi oli seal kokku umbes 2000 küberkaitsele spetsialiseerunut. Ta on sarnane meie kaitseliidule, muidugi on nad paremini relvastatud – neil on omad lennuväljad jne. Eesti kaitseliit on riigi poolt finantseeritud, aga tema põhi on ikkagi kaitsetahte kasvatamine, kuivõrd tipprelvastuse andmine vabatahtlike kätte. Sama ka kübervallas saab ameerika lubada endale paremat varustust.

c. Mida on tehtud selleks, et võimalikest raskustest küberturbe valdkonnas üle saada?

Nüüd on turbe eest vastutus eraldatud IT vastutusest. 5-10 aastat tagasi oli turbespetsialist IT töötaja. Nüüd peab iga asutus määrama turbe eest vastutava isiku ja sel isikul on järelvalve kohustused, ta ei tohi olla rolli ülesannetes, kus ta järelvalvet teeb.

B.4 Interview with Jaan Priisalu

1. Palun kirjeldage Eesti küberturbe maastikku enne 2007. aasta aprillis ja mais toimunud küberrünnakut.

Küberturvalisuse pärast muretseti ikka, 2006. aastal asutati ametlikult CERT. 1998 algas ka pankade koostöö. Kes turbega olid seotud, ikka mõtlesid sellele. Selge see, et poliitikute jaoks ei olnud see teema tol ajal. Samas arusaadav – internet ei olnud ka poliitikute jaoks teema alguses. Kui mingi asi aga võtab üle 20% inimeste vabast ajast, muutub teema oluliseks.

Spetsialisti tasemel oli koostöö ja juhid lubasid sel juhtuda. Koostöö oli ja seda ei takistatud, samas oluliselt ei soodustatud ka. Samas kindlasti oli olukord Eestis parem kui paljudes teistes riikides.

a. Miks ründajad 2007. aastal Teie hinnangul õnnestusid?

Nii ründaja kui rünnatav võitsid. Aga erinevaid asju. Eesti võitis meedia tähelepanu. Objektiivne situatsioon oli ka selline, et keegi e teadnud midagi ja kõigi tähelepanu koondus siia. Selles mõttes oli see geniaalne PR-lüke. Eesti võitis rahvusvahelise maine ja teema, kus ta suutis end tõestada. Inimesed usuvad täna, et Eesti oskab küberturbes kaasa rääkida. Praegu on nii, et USA ja Inglismaa võistlevad omavahel, et kuidas seda kopeerida.

Venemaa muidugi sai kommunikeerida seda, et Eesti näol on tegemist pisikese vastiku natsiriigiga.

Ja kolmas osapool - *community* – tänu sellele, et Eestis oli piisavalt julgeid inimesi, kes ei häbenenud rääkida, et rünnak oli, see üldse ju avalikkusesse jõudis. Koostöö suurenes edaspidi oluliselt.

b. Mis oli valesti või puudu, mis tegi rünnakute õnnestumise võimalikuks?

Teadlik võrgu arendamine oli enne 2007. aastat puudu. 2007.aastal minu jaoks kõige suurem probleem oli, et puukujuline struktuur, mis loodi selleks, et koordineerida ja kontrollida küberturbespetsialiste – poliitikud kartsid, et nad väljuvad kontrolli alt ja teevad mida iganes. Koordineerimist oli vaja teha, ma olen nõus, aga tulemus oli see, et 2007. aastal jooksis koordinatsioon totaalselt kokku. Neid asju, mis ümberringi juhtus, oli nii palju, et CERT ei jõudnud neid isegi kokku lugeda. Hierarhiline struktuur küberründes ehk totaalses sõjas ei tööta.

Riigi poolt sponsoreeritud rünnak. Ja miks ma nii ütlen – rahuldamata õigusabi. Seal on teisi asju ka, aga just õigusabi andmisest keeldumine tegi selle riigi poolt sponsoreeritud rünnakuks.

2. Palun kirjeldage lühidalt, mis juhtus 2007. aastal.

Kõik räägivad DDoS rünnakutest, aga me ei tea midagi näotustumisest – olid mingid majaühistud ja muud suvalised inimeste ühendused, kellel olid väikese kasutajaskonnaga veebid, mis üle võeti ja sinna riputati pronkssõdureid, Georgi linte ja muud. Me ei tea, kui palju oli neid, kes seda tegid. Samal ajal olid ka inimesed ,kes käisid mööda veebi ja seda koristasid ja korda tegid. vabatahtlikku tegevust oli palju.

Koostööd riigi ja erasektori vahel ikka oli. Aga mis on harjutamata, see ei tööta samal ajal, kui jama käib. Ilma eelnevate kokkupuudeteta ei oleks saanud 2007. aasta juhtum üldse lahenenudki – oleks võinud kesta nädalaid.

Ma arvan, et juba arusaamine, et see oli rünnak, et me olime rünnaku all, see juba oli väga hea – sest kuidas sa saad aru, et sind rünnatakse, see on väga keeruline küberruumis.

3. Mis olid/on suurimad muutused küberturbe/küberkaitse valdkonnas?

Küberkaitse strateegia ja küberkaitseliit.

Aga ükski asi ei ole tõstnud meie turvet rohkem kui krooni kaotamine ja eurole üleminek, minu arust on see meie riigi viimase aja turbesündmus. Venelased imetlevad seda ja kui sa oma vastase lugupidamise võidad, on see oluline asi. Eesti on kahekümne iseseisva aastaga saavutanud selle, et meie taga on Euroopa Liit, NATO, see saadab võimalikule ründajale välja kindla signaali, et me ei ole üksi.

b. Mis olid/on suuremad raskused, mida tuli/tuleb ületada saavutamaks väga heal tasemel küberturvet?

Küber ei ole asi, mille spetsialistid ära teevad – kõik peavad tööd tegema. Ta oli korraks popp, aga selle nimel on püsivalt ja pidevalt vaja tööd teha ja energiat sinna panna. Aga energiat ei jätku. CIIP osakonda oli planeeritud 22 inimest tööle, aga masu [majandussurutis] ajal sinna raha ei pandud.

Küberturbe alane õpe on olemas - Tartu ülikoolis on, tehnikaülikoolis on, IT kolledžis on – viimastes on terve küberkaitse moodul. Tallinna ülikoolis veel pole nii kaugele jõutud, aga küllap jõutakse.

Tegelikult on meil üks asi puudu – turg. Selleks, et turbest kasu oleks, pead sa protsessis osalema. Selleks, et kogemusi saada, on üks võimalus oma tooteid müüa, kui tahad turbes tasemel olla, kakled pidevalt selle nimel, et kogemusi oleks.

Pigem praktiline pool, hariduse poolt on kõik tehtud. Ma arvan, et haridusministeerium on, kui vaadata küberturbe strateegiat, ainuke ministeerium, mis tõesti on teinud kõik, mis ette nähti. Strateegi maht oli 400 miljonit krooni, sinna pole pooltki sisse pandud.

Kui haridus ja teadmine on korras, on see sel alal põhi mis paigas peab olema. Nüüd on ressurss õigesse kohta läinud, küll muu ka tuleb.

Meie riigis on primaarsed elektroonilised registrid. Mis tähendab, et kui mingi kirje ära muudetakse, see tegelikult ka muutub. Mis mina teeksin – ma ründaksin terviklikkust, siis on hästi palju väikeseid jamasid. Inimesed ei usaldaks enam elektroonilist süsteemi läheksid paberile tagasi ja kui nad paberile tagasi lähevad, siis nad kaotavad.

Küberründes tuleb saavutada olukord, et rünne kestaks. Suur rünnak x-tee või id-kaardi süsteemi vastu ei oleks parim – seda märgataks, ründe puhul ei oleks see enam hea. Mina ründaks terviklikkust ja konfidentsiaalsust – tekiksid väiksemad probleemid igal pool, oleks raske kindlaks teha, kas tegemist on rikke või ründega.

Suurimad kahjukannatajad olid börsiettevõtted – rünnak tekitab usalduskriisi. Ja kõige suuremad kahjud ongi kaudsed. Muidugi oli tol ajal osasid kahjusid hea põhjendada, et ütleme et oli küberrünnak. Samas see, et Eesti majanduses hinnati 10% transiidile, see kadus ju täiesti. Iseenesest oli sündmusel endal väga suur mõju, kui palju sel oli küberründel osa, me ei saagi öelda.

2007 oli küberrünnak kaasnev nähtus, 2008 Gruusia oli koordineeritud, küberründed hakkasid samal ajal kui sõjaline tegevus, 2010 Tuneesia oli juba selline koht, kus küberist olid tänavarahutused põhjustatud. Nüüd on toimunud muudatus, kus küber on muutunud peamiseks koordineerimise vahendiks. Trend on selline, et 2007-2011 oli üleminek ühiskonnas küberi kui peamise ründevahendiks ära toimunud. See kaks aastat mil Eesti küberisse korralikult raha ei pandud, maksab meile tagasi, me kaotasime kaks aastat ülemineku ajal. See on oma positsiooni käest ära andmine. Teised on nüüd järgi tulnud, Eesti marginaliseerus. Eesti on nii väike, me ei saa seda endale lubada. Enne olime unikaalse kogemusega riik, nüüd on teised väga kiiresti järgi tulnud, 2008 küberkaitse strateegia oli väga kõva asi, kaevati, et jänkid kopeerisid sealt lõike endale. Kui maailma kõige võimsam riik sind kopeerib, sisi see tähendab, et oledki maailma tipus.

Kübersõda on tegelikult majandussõda. Majandusprotsesside vastu suunatud sõda, kus üritatakse protsesse takistada. Üritatakse leida pudelikaela, et tekitada takistus niimoodi, et takistus oleks jääv ja tõmbaks võimalikult palju protsesse endaga kaasa. Ja jäävad tuvastamise probleemid.

Küber ei kao kuhugi. Poliitikud küsivad, kas me saaksime küberseaduse teha. Küber ja keerukus, informatsiooniline vastasolu on nii suur, et ei saa teha eraldi seadust. Kõik seadused tuleb teha selliseks, et nad küberruumis ka töötavad.