Cyber Society and Cooperative Cyber Defence

Peeter Lorents[1], Rain Ottis[1], and Raul Rikk[2]

[1] Cooperative Cyber Defence Centre of Excellence, Filtri 12, 10132 Tallinn, Estonia
[2] General Staff of Estonian Defence Forces, Juhkentali 28, 15007 Tallinn, Estonia
{Peeter.Lorents,Rain.Ottis}@ccdcoe.org,
Raul.Rikk@mil.ee

Abstract. Emergence of cyber societies places new emphasis on the protection of information and information services. The paper provides a definition for the concept of information that is based on the concept of knowledge and a definition for cyber society, which encompasses the relationship between a society of humans and a network of computers. Estonia and the cyber attacks of spring 2007 are briefly examined as an example of an early cyber society under cyber attack. Finally, the role and principles of the Cooperative Cyber Defence Centre of Excellence are explained.

Keywords: Knowledge, information, cyber society, cyber attacks, cooperative cyber defence, CCD COE.

1 Introduction

When talking about cyber society and all that it implies (including vulnerability, threats, defense etc.) it is important to clearly define *cyber society*, a term that differs from information society, IT-society, e-society etc. Without diluting our focus by comparing all the various opinions on the subject (although, see [1] for some key points) we identify aspects that describe what could be called a cyber society:

- information's importance is equivalent to traditionally valued concepts, such as energy, money etc.
- information is transmitted, processed, stored etc. on mostly computer-based systems (including universal, specialized, miniature computers etc.)
- computers are used to govern the society.

Based on the above we get to the following definition:

Definition 1. A cyber society is a society where computerized information transfer and information processing is (near) ubiquitous and where the normal functioning of this society is severely degraded or altogether impossible if the computerized systems no longer function correctly.

Following this definition, cyber society is an advanced form of human-computer interaction. This relationship (human-computer interaction) involves not just a single human and a single computer, but encompasses the relationship between a society of humans and a network of computers.

N. Aykin (Ed.): Internationalization, Design, LNCS 5623, pp. 180–186, 2009.

In order to fully understand a cyber society, including its strengths and weaknesses, we must first understand the concept of information. We will begin by defining information and other necessary concepts. Then we focus on the Republic of Estonia as an example of an early cyber society. We will also provide a short overview of the cyber attacks against Estonia that took place in the spring of 2007 and provide some lessons learned from this experience. Finally, we will discuss the principles, structure and areas of activity of the Cooperative Cyber Defence Centre of Excellence, which received its NATO accreditation in 2008.

2 Information and Information Corruption

One of the instruments for understanding various objects and processes in the world is "finding" and formally describing the relationships between them. Unfortunately, relationships come in two categories:

- Relationships that can be defined (including definitions using other relationships)
- Relationships that cannot be defined

The last types of relationships are called *fundamental relationships.*

Example. In set theory (see [2] and [3]) the concept of *being an element of* is a fundamental relationship, which is designated with a stylized "e" or the symbol "$\in$". On the other hand, the concept of *being a subset of* (designated with the symbol "$\subseteq$") is not a fundamental relationship, since it can be defined with the concept of *being an element of,* among other things (one set is a subset of another set, if every element of the first set is also an element of the second set).

In this paper we rely on the fundamental relationship of notation-denotation (see [4]), which is designated by a stylized letter "s" or the symbol "$\int$". If some objects A and B have this relationship, then A is the notation for B and B is the denotation for A. Let us agree that if we have formed an *ordered pair* of A and B, where A is the first element and B is the second element then we write this down as $\langle$A,B$\rangle$.

Definition 2. We call an ordered pair $\langle$A,B$\rangle$ *knowledge*, if A is the notation (symbol) for B and B is the denotation (meaning) for A. [4]

Note. A and B constitute knowledge, if they have the notation-denotation relationship "$\int$" or if A$\int$B.

Often knowledge is represented in text form, but not always.

Example 1. $\langle\pi$, ratio of a circle's circumference to its diameter$\rangle$ is knowledge, because $\pi\int$ *ratio of a circle's circumference to its diameter.*

Example 2. $\langle$the diagonal of a square, a straight line joining the opposite corners of a square$\rangle$ is knowledge, because *the diagonal of a square* $\int$ *a straight line joining the opposite corners of a square.*

Example 3. A red traffic light is the notation for a prohibition for moving forward. This piece of knowledge (where the color of the traffic light is the notation and the corresponding meaning is the denotation) is necessary for anyone navigating city streets.

Example 4. Hoisting the flag upside down signals distress. Unfortunately, not many are aware of this piece of knowledge, where the "wrong position" of the flag is the notation and the emergency is the denotation.

Definition 3. D is data, if there is such an A, where $\langle$A,D$\rangle$ is knowledge, or if there is such a B, where $\langle$D,B$\rangle$ is knowledge. [5]

Example. The question – what is the air temperature in the coming days – is answered by a list of numbers. Therefore, the numbers constitute data that is the *denotation* (meaning) of the words "air temperature in the coming days". The question – what do you call the country that shares a land border with only Latvia and Russia – can be answered as "Estonia", "Eesti", "Viro" etc. Therefore, in this case all these words are a *notation* (symbol) for the same country.

Note. In order to have data it is necessary to have the corresponding knowledge. If, for some X nobody knows, has known and will never know, what is the notation or denotation of X, then X *is not* data!

Definition 4. *Information,* or more shortly *info*, is either knowledge or data.

According to the definition, only one that has knowledge or data also has information. If someone holds some X, which is not knowledge or at least part of knowledge (an object in the form of a notation or a denotation), then X is not information. Following the definition the information can be corrupted by using one or more of the three main options:

- corrupt the notation;
- corrupt the denotation;
- corrupt the relationship between notation and denotation.

Depending what operations are done with the information (see [5]) – for example, transmission, storage, manipulation, systematization, destruction etc. - a suitable method can be found to corrupt the operation (which can bring about, but does not require, the corruption of the information itself). For example, enough extra information can be "pumped into" the information transmission channels that the *transmission speed* of the necessary information becomes intolerably slow. In order to corrupt a database or knowledge base it is enough to corrupt the *system*, which can be realized by deleting the data within. A more sophisticated way to corrupt a system would employ moving the data or changing the relationships between data objects etc.

3 Estonia as an Example of an Early Cyber Society

According to the definition in the introduction, a cyber society is based on ubiquitous computing and that a loss of these computer services directly affects the normal existence of this society. Computing deals with manipulating information (knowledge and data) for the benefit of the user. For example, the concept of money no longer requires a physical entity (coins, bills) that can be passed between transaction parties (from one wallet to another). Instead, the passage of wealth can be represented with a simple change of numbers in the related accounts (stored in computer systems). Therefore, money is accompanied with the knowledge about the ownership of namely this specific wealth. In operations with money, old knowledge changes to new knowledge.

The financial sector in Estonia (which is equivalent to the blood circulation in the human body) is almost fully computerized. The following facts are a good illustration of this claim:

- 98% of all bank transactions are completed via electronic means (on-line payments, credit card use, signing up for new bank services on-line etc). [6]
- 88% of all income tax declarations were entered on-line in 2008 and 17% of those on the first day of the declaration period. In 2009, the number of first day declarations rose 43%. [7]

The exchange of information is also largely facilitated by computer systems:

- major newspapers are represented on-line
- some key information forums are only available on-line
- medical records available to doctors via a national information system
- school grades, homework assignments and messages to and from parents are implemented in an e-school system
- Estonian police and courts use an e-case system, which allows for easy sharing of information about criminals

Leadership and management of the society is strongly reliant on computer systems:

- government holds paperless e-cabinet meetings
- local and state elections offer both manual and an electronic vote option

NB! This is not merely using „electronic gadgets“ but information transmitting, processing, storing etc. with computers in order to ensure the running of critical processes at the national level! Therefore, many (if not all) of these services should be considered critical information infrastructure and any attacks against them should be viewed in the context of national security. In most cases, attacks against these systems have a tangible effect on ordinary citizens, who can no longer get access to the services they need. This illustrates the dangers of over-dependence between human society and computer networks.

4 An Overview of the 2007 Spring Cyber Attacks Against Estonia

In the spring of 2007 many Estonian government and private information systems came under a wide scale cyber attack campaign that lasted for 22 days, from April 27th to May 18th. The attacks were a response to the Estonian Government's decision to relocate a Soviet WWII monument to a military cemetery. The decision met with much criticism by the Russian authorities, as well as the ethnic Russian minority in Estonia. Following two nights of looting and rioting in Tallinn, a campaign of cyber attacks was launched by presumably ethnic Russian activists, located in Russia, Estonia and elsewhere. To this day no official connection has been made to the Russian government. [8]

Majority of the attacks were relatively simple and robust, using well known methods and vectors. Most prominent were the distributed denial of service attacks (SYN flood, PING flood, mass e-mail etc.) which were launched both manually and via botnets. However, the size and length of the attack was unexpected for most targets and therefore various services were either degraded or disabled throughout the conflict. The most prominent target categories were: government web and e-mail servers, on-line banking services, on-line news services, as well as the network infrastructure (DNS servers and network routers) at ISP level. [8]

It is important to note that this was a purely political attack – there is no information about financial motivation among the attackers. And yet, many “civilian“ systems were purposefully targeted, including commercial banks and private news companies. This would indicate that the attackers were interested in damaging the Estonian cyber society in all the relevant categories identified in the introduction:

- targeting the banking infrastructure has serious economic consequences if services remain out of operation for more than a few hours or days
- attacks against news services bring about an (partial) information blockade both nationally and internationally (fortunately alternative media channels were not affected by this attack)
- attacks against government systems diminish the government's ability to properly govern the state.

In this light, the attackers were aiming at critical sectors of the Estonian cyber society, but were fortunately unable to cause serious harm. However, attacks like this are becoming more commonplace and should be addressed at a national level for any country that is in the process of transforming into a cyber society.

5 On Cooperation

An important lesson from these attacks is that the Internet has empowered the people not only by giving them access to information and nearly free communication around the globe, but also by letting people attack any connected target no matter the physical location. While this is usually not a problem, it can become one quickly enough if a critical mass of attackers converges on a target. Simplest denial of service attacks require no training or specialized software, so it is just a matter of finding enough committed attackers and coordinating their effort.

As a result of this relative ease we witness cyber attacks becoming more popular as a tool for political activism. Politically motivated cyber attacks have become commonplace. It is no longer surprising if a military conflict in Israel coincides with hacking on both sides, or if a political row between Russia and its neighbors also escalates into cyber space. In essence, cyber militias are developing in many countries around the world, some of them undoubtedly with the (passive?) support of the interested government. [9]

Since these cyber conflicts lack a clear legal status they usually boil down to technical countermeasures at the service provider and target level. Usually the attacks cross international boundaries, which means that the service providers and incident handlers (computer emergency response teams) need international cooperation in order to stem the tide of the attacks.

6 The Cooperative Cyber Defence Centre of Excellence

Understanding the importance of cooperation in cyber defence, in 2004 Estonia offered to establish and host a multi-national organization focused on developing this aspect within NATO. The Alliance supported this idea and after thorough preparation the Cooperative Cyber Defence Centre of Excellence (CCD COE) was formally established in the spring of 2008 and accredited as an International Military Organization in the fall of 2008. In addition to Estonia, it currently includes six more sponsoring nations: Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain, with a few more in the process of joining the Centre.

The nature of the CCD COE is to develop new concepts, methods, tools, training materials, as well as analytical products. It is by no means intended or equipped as an operations organization, such as the various computer incident response teams etc. Instead, it is designed as a vessel for assisting NATO's transformation process, especially in the matters of cyber defence.

Organizationally the CCD COE is divided into three branches: administrative, research and development, training and doctrine. However, much of the work is done using a virtual matrix structure that "ignores" the official organization chart and uses the necessary manpower as ad-hoc project teams, regardless of the position of the personnel. This allows for a much more flexible approach when tackling complex problems.

7 Summary

As information technology becomes ever more integrated into our daily life, we transform into a cyber society. We have discussed that cyber society is, in fact, an advanced form of human-computer interaction, which encompasses the relationship between a society of humans and a network of computers.

In the preceding sections we have briefly covered the definition of information that is based on the concept of knowledge and main principles to corrupting it. We defined the concept of cyber society, identified Estonia as an early cyber society and examined the cyber attacks that brought this into focus in 2007. Finally, we discussed the principles behind the establishment and running the Cooperative Cyber Defence Centre of Excellence.

References

1. Wiener, N.: The human use of human beings. Cybernetics and society. Doubleday Anchor Books, Doubleday&Company, Inc., Garden City, New York (1956)
2. Fraenkel, A.A., Bar-Hillel, Y.: Foundations of Set Theory. North-Holland Publishing Company, Amsterdam (1958)
3. Potter, M.: Set Theory and its Philosophy. Oxford University Press, Inc., New York (2004)
4. Lorents, P.: Formalization of data and knowledge based on the fundamental notation-denotation relation. In: Proceedings of the International Conference on Artificial Intelligence, IC-AI 2001, Las Vegas, USA. USA, vol. III, pp. 1297–1301. CSREA Press (2001)

5. Lorents, P.: Knowledge and Taxonomy of Intellect. In: Proceedings of the International Conference on Artificial Intelligence, IC-AI 2008, Las Vegas, USA, July 25-28, vol. II, pp. 484–489. CSREA Press (2008)
6. Hiie, I.: Sulgkerged teenuste halduse protsessid. In: ITSMF 2007 conference, Tallinn, Estonia, November 22 (2007), http://www.itsmf.ee/itsmf2007/itsmf_estonia_2007_sulgkerged_protsessid.pdf (last accessed March 16, 2009)
7. Estonian Tax and Customs Board: Press Release (February 16, 2009), http://www.emta.ee/?id=25369&tpl=1026 (last accessed March 15, 2009)
8. Ottis, R.: 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, UK, June 30-July 1, pp. 163–168. Academic Publishing Limited, Reading (2008)
9. Ottis, R.: Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. In: Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon, Portugal, July 6-7, 2009 (accepted for publication)