

CYBER SECURITY IN NATIONAL PROTECTION OF TURKEY

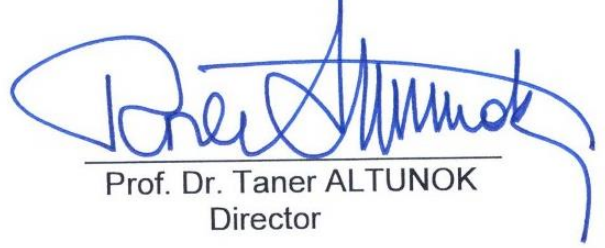
FARUK AYDIN

SEPTEMBER, 2012

Title of the Thesis : **Cyber Security in the National Protection of TURKEY**

Submitted by : **Faruk AYDIN**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University



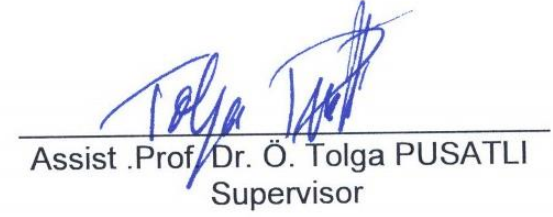
Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.



Prof. Dr. Billur KAYMAKÇALAN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Assist. Prof. Dr. Ö. Tolga PUSATLI
Supervisor

Examination Date:

Examining Committee Members:

Assist. Prof. Dr. Ö. Tolga PUSATLI (Çankaya Univ.)

Assist. Prof. Dr. K. Levent ERTÜRK (Atılım Univ.)

Assist. Prof. Dr. Murat KOYUNCU (Atılım Univ.)



STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by rules and conduct, I have fully cited and referenced all material results that are not original to this work.

Name, Last Name : Faruk AYDIN

Signature : 

Date : 07.09.2012

ABSTRACT

Cyber Security in the National Protection of TURKEY

Faruk AYDIN

M.Sc., Department of Mathematics and Computer Science

Supervisor: Assist .Prof. Dr. Ö. Tolga PUSATLI

SEPTEMBER 2012, 58 pages

Cyber attacks supported by individuals and states are increased by the prevalence of information technologies and usage of these technologies at the critical infrastructure of the states. In this study, these cyber attacks and associated impacts are researched. In connection with this issue, evolution of cyber threats from malware such as viruses to weapons is studied by examples. In addition, within this thesis, precautions against these threats are mentioned. Usage of anti-malware applications as prevalent precautions is assessed within this context. National and international standards of information security, information security strategies of EU, USA and some other countries and precautions for cyber security of Turkey are studied.

In the 9th Development Plan of Turkey, building information society is targeted. In this thesis, requirements to reach this target securely are researched. Under this information, it is considered that educated citizens and companies along with public institutions should cooperate to provide a nationwide cyber security. Consequently, it is defended that government should play an affective role to protect, educate, and guide governmental and private companies and citizens about cyber security. Accordingly, this thesis advises that cyber security should be put into the next development plan.

Keywords: Cyber Attack, Cyber Threat, Cyber Army, National Cyber Strategy

ÖZ

Türkiye'nin Ulusal Korunmasında Siber Güvenlik

Faruk AYDIN

Yüksek Lisans, Matematik ve Bilgisayar Bölümü

Danışman: Y.Doç. Dr. Ö. Tolga PUSATLI

EYLÜL 2012, 58 sayfa

Bilgi teknolojilerinin yaygınlaşması ve bu teknolojilerin ülkelerin kritik altyapılarında kullanılmasıyla birlikte bu altyapılara yönelik kişisel ve devlet destekli siber saldırılar artmıştır. Bu çalışmada söz konusu siber saldırılar ile etkileri araştırılmıştır. Bu konuya doğrudan bağlı olarak, tezde, siber tehditlerin virus benzeri kötücül yazılımlardan silaha evrimi örnekleri ile incelenmiştir. Bunlara ek olarak, tez çalışması kapsamında bu tehditlere karşı alınabilecek tedbirler de ele alınmıştır. Yaygın bir önlem olan kötücül yazılım karşıtı uygulamaların kullanımı bu kapsamda değerlendirilmiştir. Bilgi güvenliğine yönelik ulusal ve uluslararası standartlar, A.B. ve A.B.D. ile bazı ülkelerin stratejileri ve Türkiye'de siber güvenlik konusunda alınan tedbirlerin neler olduğu da araştırılmıştır.

Dokuzuncu Kalkınma Planında Türkiye'nin bilgi toplumu olması hedeflenmiştir. Çalışmada bu hedefe güvenli bir şekilde ulaşılabilmesi için yapılması gerekenler araştırılmıştır. Bu bilgilerin ışığında, ulusal siber güvenliğin sağlanmasında, kamusal kurumların yanında eğitimli vatandaş ve firmalar ile işbirliğinin gerektiği değerlendirilmiştir. Buna dayanarak, devletin siber güvenlik konusunda, kamu kuruluşlarını, özel şirketleri ve vatandaşlarını koruma, eğitme ve yol göstermede daha etken bir görev

üstlenmesi gerektiği savunulmuştur. Buna bağılı olarak, bu tezde, Türkiye’de siber güvenlik konusunun, gelecek kalkınma planına konulmasına ihtiyaç olduğu önerilmektedir.

Anahtar Kelimeler: Siber Saldırı, Siber Tehdit, Siber Ordu, Ulusal Siber Strateji

ACKNOWLEDGEMENT

I express my sincere appreciation to my thesis advisor Dr. Tolga PUSATLI for his patience and guidance in building my thesis. I learned a lot from your broad academic knowledge and experience. I couldn't have written this thesis without your contributions.

I am grateful to Mr. H.İbrahim TOKUŞ, for his support and encouragement.

I would like to thank to key informants who have contributed in the validation of the findings; their names are kept as anonymous by their will.

I want to thank my wife and my family for supporting me throughout my studies.

TABLE OF CONTENTS

STATEMENT OF NON-PLAGIARISM	iii
ABSTRACT	iv
ÖZ	v
ACKNOWLEDGEMENT	vii
TABLE OF CONTENTS	viii
LIST OF FIGURES	xi
LIST OF TABLES	xii

CHAPTERS:

CHAPTER I	1
1. INTRODUCTION	1
1.1. CLIMBING IMPORTANCE OF CYBER SECURITY AND DEVELOPMENT PLANS IN TURKEY	1
1.2. SCOPE	3
1.3. PURPOSE	4
1.4. RESEARCH QUESTION	4
1.5. OUTLINE	5
CHAPTER II	6
2. BACKGROUND AND LITERATURE REVIEW	6

2.1.	CYBER THREATS	6
2.1.1.	Hackers	7
2.1.2.	Botnets	13
2.1.3.	Denial of Service (DoS) Attacks.....	16
2.1.4.	Port Scans	17
2.1.5.	DNS Root Server Incidents.....	18
2.1.6.	Malware	19
2.2.	CYBER THREATS AND THEIR TARGETS	25
2.3.	ANTI-MALWARE.....	26
2.4.	SUMMARY	29
CHAPTER III.....		31
3.	RESEARCH METHODOLOGY	31
3.1.	MOTIVATION.....	31
3.2.	PHASES OF THE STUDY	31
3.3.	VALIDATION OF THE FINDINGS.....	32
3.4.	SUMMARY	33
CHAPTER IV		34
4.	CYBER ATTACKS AND STATES.....	34
4.1.	INTRODUCTION.....	34
4.2.	INTERNATIONAL CYBER ATTACKS.....	35
4.3.	CRITICAL INFRASTRUCTURE	38
4.4.	INFORMATION SECURITY STANDARDS	39

4.4.1.	ISO/IEC Standards	39
4.4.2.	Turkish Standards (TS).....	41
4.5.	RESPONSIBILITY OF THE STATE	43
4.5.1.	Cyber Security Strategies	45
4.5.2.	Precautions in Turkey on Cyber Security.....	46
4.6.	SUMMARY	50
CHAPTER V		51
5.	DISCUSSION AND RECOMMENDATION.....	51
5.1.	MILITARY PRECAUTIONS.....	51
5.2.	CYBER SECURITY SUPERIOR COMMITTEE.....	53
5.3.	CYBER SECURITY REGULATION ORGANIZATION	54
5.4.	CYBER SECURITY COMMAND	54
CHAPTER VI		56
6.	CONCLUSION AND FUTURE WORK	56
6.1.	FUTURE WORKS	56
6.2.	FINDINGS	57
6.3.	CONCLUSION	58
REFERENCES		R1
APPENDIX A		A1

LIST OF FIGURES

Figure 2.1 - Typical phases in a cyber attack.....	8
Figure 2.2 - A botnet overview	14
Figure 2.3 - A snapshot view of botnet hosts' locations	15
Figure 2.4 - Overview of the Tinba Trojan-banker Turkish attacks.....	23
Figure 2.5 - Cyber threats and their targets	26
Figure 2.6 - Most vulnerable applications	28
Figure 4.1 - A Web site screenshot from Estonia in 2007	36
Figure 4.2 - State cyber-attacks	37
Figure 4.3 - A Brief Timeline of Selected Information Security Systems	41
Figure 5.1 - Cyber Security Organization.....	53

LIST OF TABLES

Table 2.1 - Examples of insider attacks from	12
Table 2.2 - Example of Virus Infections and Damages	22
Table 2.3 - Anti-malware Brand / Software	27
Table 2.4 - Top 20 Countries web resources seeded with malware.....	28
Table 4.1 - CC evaluation assurance levels.....	43

CHAPTER I

1. INTRODUCTION

With the prevalence of information technologies in most of the industries, hence business, cyber security saves its importance in the modern world and promises to climb to higher priorities in the governmental agenda in many countries. Nowadays, information technologies has been prevalent at many level (personal, institutional, systemic occasion) from individual to cross nations hence to a global level. Thus, cyber security is no longer considered as a subject coincided in personal computer security and / or securing e-mail accounts.

1.1. CLIMBING IMPORTANCE OF CYBER SECURITY AND DEVELOPMENT PLANS IN TURKEY

With the widening and spreading nature of the topic, literature is fed with studies on cyber security at various levels in many countries, hence in Turkey.

Quick examples include Tunisian Report [1] accepted in the World Summit on The Information Society (WSIS) and the 9th Development Plan of Turkey [2].

Basically, Tunisian Report highlights following bullets;

- Information resources and technologies are being used for crime,
- Terrorism uses information technologies effectively,
- For that reason misuse of information technologies should be prevented but human rights should be considered while preventing the misuse.

Transformation of Turkey's society to the information society has been stressed in the Turkey's vision in the 9th Development Plan covers 2007-2013 years of Turkey.

Before we go further, we give brief information on the national development plans in Turkey. Development is defined by multi-dimensional understanding including concepts like growth of economy besides rule of law, information society, international rivalry, sustainable growth and human development. Thus, development efforts are seen as to be kept on by an integrated point of view complied with this definition [3].

First of Turkish development plans which are basic politic documents resulted in requirement of planned development is prepared in 1963. Plans comprise 5-year periods except the ninth one which covers seven years. Government Planning Organization serving as Ministry of Development today has implemented nine development plans until now. Different priorities are determined in every period of development plans. Vision of "transformation into information society" was placed among the targets of 9th period of development plan which covers years of 2007-2013.

Promoting e-government applications is included in this plan (article 314). Providing public services electronically will bring great convenience to our daily lives; however, criminal organizations take advantage of information technology (article 323) and cyber-attacks against Estonia showed that potential problems may occur if adequate security measures are not taken for e-government applications in the future.

The development programs in Turkey are supported by medium term programs. Following the 9th Development Plan, two sections [4] under "Improving the Quality and Effectiveness in Public Services" of "Development Axis in the Programme Period" chapter visit cyber security in an abstract level. Those are sections three and five, enhancing the effectiveness of security and dissemination of e-government applications, respectively:

“Works on developing necessary legal, institutional and technological infrastructure to fight against terrorism and financing of terrorist activities as well as organized, financial and cyber crimes will be continued.”

“In e-government applications, user-focus, customer satisfaction, privacy of personal information, information security, participation and transparency will be ensured.”

Both Tunisian report and 9th Development Plan, as examples, show that cyber security issue is considered as an important area both nationally and internationally.

1.2. SCOPE

Cyber attacks are not only targeting business for brutal entertainment or theft purposes. Such attacks can be parts of extremist actions such as terrorism as well.

For instance, Lucent Technologies, which is a multinational technology company, announced that Unity, a pro—Palestinian group, had attacked its Web site in November 2000. The purpose of this attack was not to steal any valuable information but because the company did business in Israel [5].

Cyber crimes are big threats not only for the world but also for Turkey. According to the 2012 Norton Cyber Crime Report [6] in Turkey more than 10 million people have been aggrieved because of cyber crime in last 12 months. It is stated that the cost of this aggrieve is around 556 million USD.

Hence, the researcher targets cyber attack tools / actions that can be used as “weapons” against corporations as well as countries. In this context, cyber attack tools are studied by examples. Anti-malware solutions are mentioned as precautions against these threats. Also national and international standards and strategies of the states about information security are studied. Related to this frame, we investigate Turkey’s nationwide digital protection.

While drawing the boundaries of the study, the scope of the thesis is limited as follows. Law clauses mentioned in this thesis are limited to inform that there are legislation works in Turkey. Also, we are aware that enforcing organizations to invest on cyber security create discussion on sparing resources; however, we limit our research with the budgeting. While defining overarching targets and priorities in the cyber security, the government agencies should have clear-cut responsibilities and rights which are left to be defined as a follow-up work. This thesis reports its findings based on mainly literature survey and individual observations, empirical work about some subject such as recommendations (Chapter 5) and future works (Chapter 6) which are left out of scope of this thesis.

1.3. PURPOSE

As mentioned in the scope, we aim to study cyber threats, common technological precautions and strategies against them. Within this scope, we try to find out how serious such threats can be for nations, and whether it is too early to speak of serious cyber threats that can put nationwide security in peril, or not.

1.4. RESEARCH QUESTION

Following the scope and purpose of this study, the researcher aims to find an investigated answer to the following research question:

Should state play an affective role in national cyber security? If it has to, what the state has to do?

Apparently, the audience should notice this research question as an open ended question and it is subject to stay in discussion for an undetermined time i.e. it may be asked all the time. Hence, it is approached with limitation.

1.5. OUTLINE

Following chapter (Chapter 2) gives basic background on cyber threats with popular examples from the literature.

During the preparation of the thesis, the researcher has followed a basic research technique as research methods (Chapter 3).

Chapter 4 focuses on cyber threats against nations and current precautions taken by exemplar countries.

Chapter 5 includes recommendations and discussions as precautions that Turkey can consider.

In the light of the findings, the conclusions (Chapter 6) are reported as Turkey needs to develop a cyber security strategy applicable nationwide; hence, its coming development agenda needs to include cyber security in, as a separate chapter.

CHAPTER II

2. BACKGROUND AND LITERATURE REVIEW

As defined in the scope (section 1.2) and purpose (section 1.3) of this thesis, our study includes cyber threats and potential damages. For this reason, we give basic definitions of those threats along with popular examples in the history. The audience is encouraged to re-visit this chapter frequently while reading the rest of the thesis.

As a direct relation to cyber security, this chapter surveys vulnerabilities that may cause cyber attacks to damage. In this thesis, we adopt vulnerability definition from [7] as “a characteristic of a computer system or a network that makes it possible for a threat to occur”. Basically, vulnerabilities are the holes in the security and functionalities of computer systems through which an abuser can have opportunity to intrude into system. These intrusions can be of different types according to their origins, purpose and severity. Law can and does consider such actions and classifies them as illegal actions based on the country of origin; however, being anonymous and ubiquitous in the digital environment lessens the discouragement of law punishment of hacking, stealing information from and harming computer systems. For this reason, for a country, passing an act of law concerning cyber crime in the government can be just one leg in this fight; another one should be eliminating the vulnerabilities of computer systems by understanding types of attacks.

2.1. CYBER THREATS

Cyber threat is an attempt of unauthorized access to data, application or system to corrupt integrity, confidentiality, security or availability as defined in [8].

Cyber threats are of various types and the number of occasions increases every day. Naturally, the threats we review in this chapter are limited; however, we have tried to include important / popular examples to our knowledge.

2.1.1. Hackers

There are several definitions to define the term hacker. Examples include:

...someone who maliciously breaks into systems for personal gain [9].

or in detail:

...a hacker is a malicious meddler in computer systems who is out to deface, replace, or delete data for personal gain, to sabotage a system, to get revenge, or, in a larger scale, to bring down the economic and social well-being of a nation by attacking its highly networked critical infrastructures [10].

With the variety in types of attacks, white hat and black hat hackers are defined because “a person skilled in computer applications to attack computers” remains too generic as argued in [11].

White hat hacker’s aims are usually limited to expose security flaws and they are not to steal or corrupt any data. Still, such actions are against the law in many countries including Turkey as defined in [12].

Black hat hackers are the attackers whose motivations are malicious and destructive. Figure 2.1 shows typical phases used by hackers.

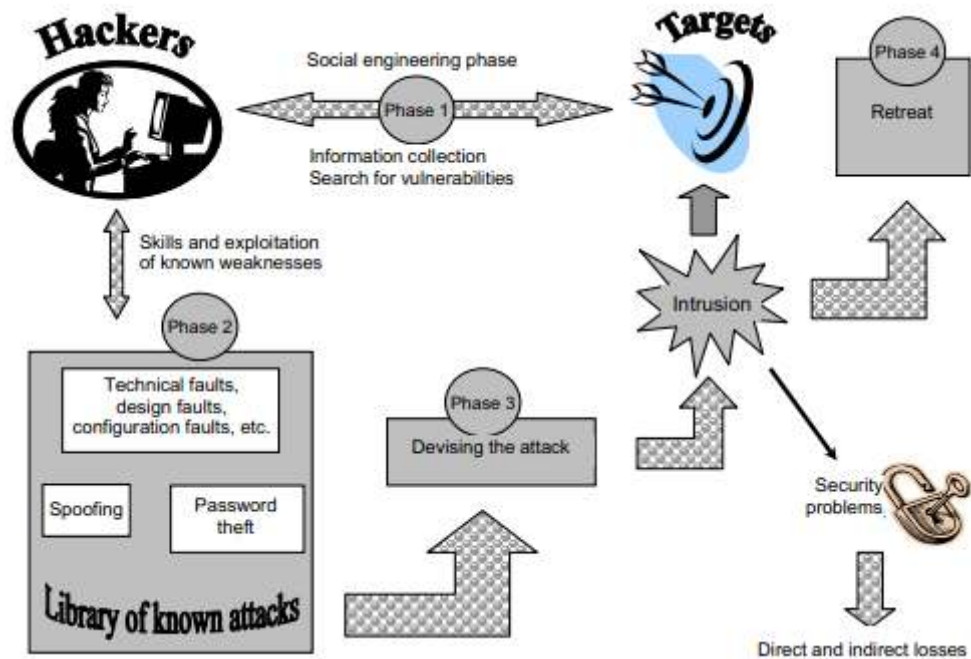


Figure 2.1 - Typical phases in a cyber attack [13]

There are many examples of hacker attacks from penetrating banks to accessing online stores' computer systems and steal credit card numbers. Popular and recent examples include Citibank and Sony cases.

In June 9, 2011, Citigroup was hacked, and 200,000 customer accounts data are exposed as reported in [14]. In the same year, just a couple of months before that, on 27 April 2011, Sony announced that PlayStation network has been hacked and 75 million user accounts are stolen [15].

Those are only two recent examples among lots of black hat hackers and attacks occur almost every day. Another example is Chinese Hackers who hit U.S. Chamber (Nov 2009-May 2010). This is a group of hackers in China, who breached the computer defenses of America's top business-lobbying group and gained access to data stored on its systems. Key informants report that the information stolen includes private data of three million members of the chamber [16].

Recalling that a hacker's attack can be more than one type, more terms are associated with the word hacker. Throughout this thesis, the reader may

find many terms derived from hacker; hence we shall visit them briefly in this section.

2.1.1.1. Hactivist

Some activists are using the Internet as a medium to raise their voices through hacking actions. Hactivist is a term produced by combining hacker and activist to address such person.

RedHack is one of this kind of activist who has hacked 90% of Turkey's police department web site at 29th March 2012 [17]. RedHack claimed that it downloaded all the files of Ministry of Internal Affairs by hacking the Ministry of Internal Affairs' sub website on April 20, 2012 [18].

In abroad, Anonymous group hacked the website of British Ministry of Interior to protest attempts of Theresa May, the British Interior Minister in April 8, 2012. Minister's plans was to keep the Internet accesses under control by holding a complete record of the details of citizens in England [19].

Both groups have assaulted in coordination to the website of ÖSYM, Student Selection and Placement Center of Turkey, on the 17th of July, 2012 and after the web site of ÖSYM was hacked by those groups, prestige of the institute has been undermined and users accesses to the web site have been prevented [20].

These actions have led to a loss of prestige in addition to obstruction of services.

2.1.1.2. Cyber Spies

These intruders are more goal-focused hackers rather than randomly attacking hackers. A computer spy is a person who is hired to break into a computer and / or information system and steal information [11]. Spies may be hired to attack specific computers or systems that contain sensitive information such as critical infrastructure systems' documents. Spies do not try to leave any mark behind them for tracing as their goal is to take information without drawing any attention i.e. they try to act in silence. As

spies are to cover themselves as well as their actions, they are expected to possess more computer skills than other hackers.

The U.S. Department of Defense reports that it is continuously targeted by attackers from China. Among them, one of the most notably series of attacks since 2003 is known as “Titan Rain” which targeted the Department of Defense and resulted in the stealing of classified documents of defense companies.

Another remarkable example is GhostNet which is a malware-based cyber espionage network. As of 2009, GhostNet has infected at least 1,295 computers; this number may appear quite small and insignificant when compared to what viruses do globally; however, 30% of those computers possess high-value diplomatic, political, economic and military information in 103 countries [21]. Hence, the damage is still severe.

2.1.1.3. Cyber Terrorism

The audience may find several definitions for the term. For example, in 2007, researchers from various levels of government agencies and academia have contributed to NATO Advanced Research Workshop Responses to Cyber Terrorism in 2007. In the proceedings of this workshop [22], we find definitions for cyber terrorism. Among them, NATO and FBI define it as follow, respectively:

“...a cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.”

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

This is basically performing a terror action by the means of information technologies, mostly through the Internet.

Cyber terrorism, whether targeting the Internet or conducted by means of the Internet, represents serious threats. Many essential aspects of today's society are considerably dependent upon the functioning of computer systems hence, a terror attack targeting IT infrastructure can easily create panic.

In [23], the authors categorize this threat based on possible legal responses:

(a) Attacks via the Internet that cause damage not only to essential electronic communication systems and the IT infrastructure but also to other infrastructures, systems, and legal interests, including human life;

(b) Dissemination of illegal content, including threatening public, inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; training and recruiting for terrorism; and dissemination of racist and xenophobia material

(c) Other logistical uses of IT systems by terrorists, such as internal communication, information acquisition, and target analysis.

On 14th March 2012, BBC claimed that, a "sophisticated cyber-attack" on the BBC has been linked to Iran's efforts to disrupt the BBC Persian Service [24]. However, no one has claimed the responsibility to our knowledge.

2.1.1.4. Insiders

Another serious threat to organizations may come from its affiliates such as contractors, business partners or "angry" employees who have been reprimanded, demoted or fired; as the name implies, those intruders are insiders in digital environment for sabotage or theft of intellectual property.

In a study of 900 cases of business [25] "data leakage" over 48% of the breaches is reported to relate to insiders who abused their right to access corporate information.

Ciampa [11] argues that insider attacks are usually more costly than an attack from the outside. Examples from different sectors include Table 2.1.

Sector	Incident
Health Care	A California health care worker, disgruntled over an upcoming job termination, illegally gathered health records on celebrities and distributed them to the media.
Government	A Maryland government employee tried to destroy the contents of over 4,000 servers by planting a malicious coding script that was scheduled to activate 90 days after he left.
Commercial	A French security trader lost over 7 billion USD on bad stock bets and then used his knowledge of the bank's computer security system to conceal the losses through fake transactions.
Army	A U.S. Army private in Iraq accessed secret U.S. diplomatic cables and other sensitive documents, which were then given to an international whistleblower who posted them on the Internet.

Table 2.1 - Examples of insider attacks from [11]

A recent and popular insider example appeared with the Wikileaks occasion. A U.S. Army private, Bradley E. Manning [26], downloaded secret files and handed them to Assange's organization which let US government's secrets been exposed to the public.

The insider is not only a technological problem, because it is related more to human than technology. Insider is a person who is or used to be one of the targetted organization hence possesses information about it; so, an insider can harm a company more than a hacker who tries to intrude. For that reason, insider problem cannot be solved by investing just on the technology. Control systems are only as secure as the people who operate them as argued in [27]. Any potential solution should consider technology, standard security management practices such as risk management, management oversight, policies and procedures as argued in [28].

2.1.2. Botnets

Botnets are one of the considerable threats on the Internet; they are mostly silent. These threats can have various purposes from hosting for illegal purposes [29] including phishing, which is directing links to unintended websites on different infected computers, and performing 'brute force' password attacks which are systematically checking all possible keys until the correct key combination is found.

Often, the intruder installs a botnet on a machine which is similar to a worm or a Trojan horse; the botnet runs without informing the user of the machine. The person controlling the botnets is called as the bot herder. A bot herder can command his bots to access to resources stored on the machine. With the botnet, the aim is not always to steal data but also to manipulate data, for example, for a Denial of Service (DoS) attack (section 2.1.3) or to send out spam mail.

An illustration of a simple botnet attack is presented on Figure 2.2. The bot herder sends bulky spam e-mails requesting private information with a fake sender name, eBay. As the popular large companies, such as eBay, have gained trust of its users, the herder's spam e-mail can get responses from recipients who think that the e-mail has been sent from eBay hence it is genuine. The e-mail can also put a Trojan horse to the user's machine which is now referred as a zombie or an agent machine. Such infected computers can logon to a command and control server (C&CS) which is a web or the Internet Relay Chat (IRC) server out of the will of the computer's owner. By this way, the computer can be used as a puppet to send out spam e-mails [5].

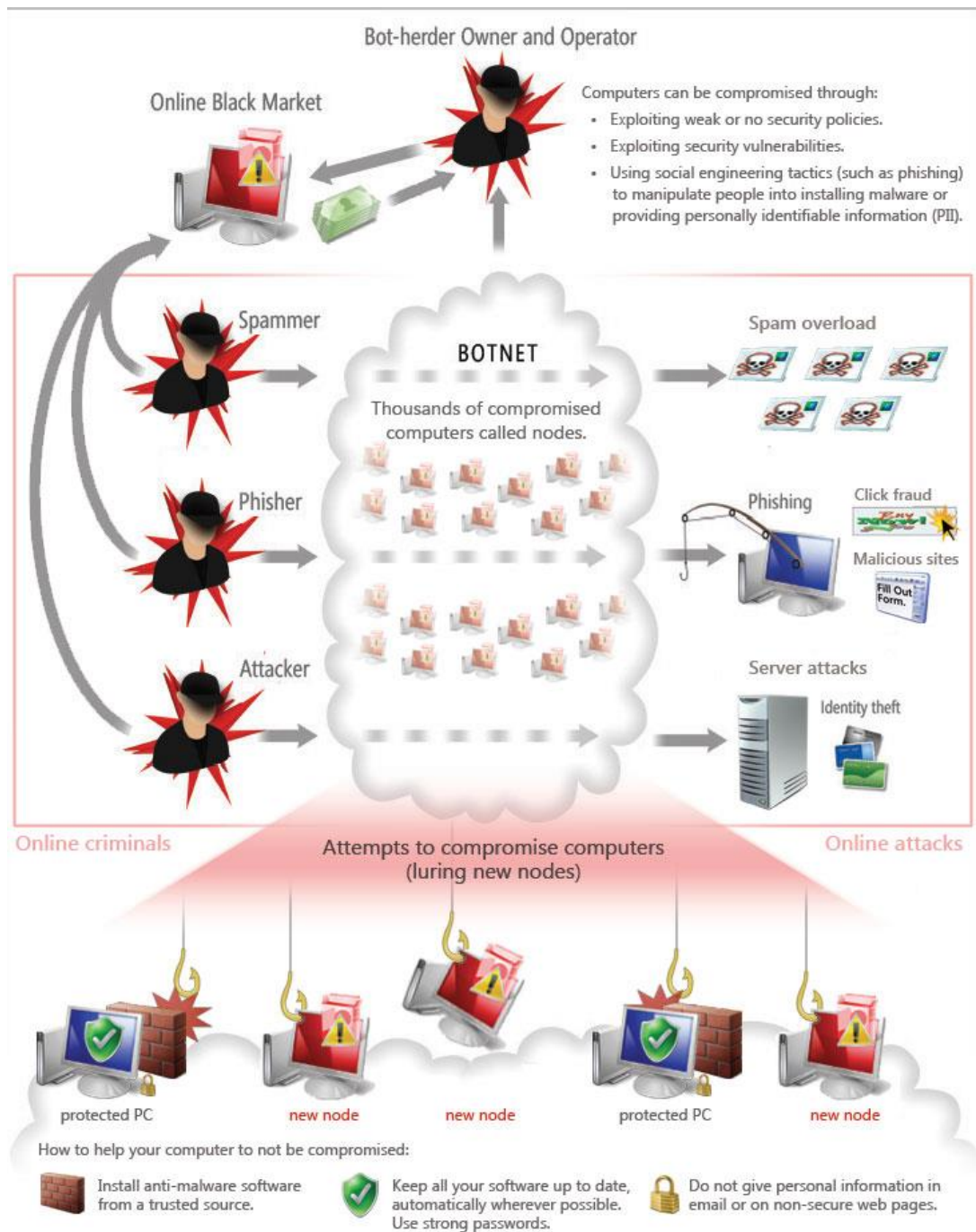


Figure 2.2 - A botnet overview [30]

Bots are getting popular and as they spread globally; Figure 2.3 illustrates the gravity of the problem.



Figure 2.3 - A snapshot view of botnet hosts' locations [31]

According to the Microsoft's report [32] "Progress Made, Trends Observed," bots represent the majority of the disinfection activities. Since January 2005, Microsoft has been delivering the Windows Malicious Software Removal Tool to its customers. At the end of the first 15 months, Microsoft has announced that it had removed 16 million instances of malicious software from almost six million unique computers [33]. However, these numbers cannot be easily used to guess number of bots. For example, a technical director informs that one should gain access to C&CS to have an exact number of botnets and zombie machines [34].

Another example is the Mariposa botnet which was believed that around 100,000 to 200,000 computers have been infected in 2010. However, once the traffic from the C&CS was redirected (via changing the Domain Name System (DNS) record) to the Panda Labs's servers' sinkhole, which approximately 12.7 millions different IP addresses have been connected [35].

As solution, the security firms are deploying C&CS trackers, such as Zeus Tracker [36] which is tracking about 1,000 C&CS of one particular Zeus botnet as at the time of writing this thesis. This operation is not an easy task because IP addresses are tracked separately and they may be too many in

numbers, such as tens of million unique IP addresses to track and trace. It is also guessed a similar number of information-stealing bots.

A botnet can create excessive amount of data network traffic with e-mails and redirection of website links. For example, Conflicker botnet is reported to have 28TB/sec total bandwidth [37].

One of the reasons to encourage botnets is that the spammers make tempting amount of money by renting sessions. iDefence [38], Kaspersky [39], and TrendMicro [40] report huge amount of money gained by this way. Basically, botmasters rent out their botnets for small amount of money to launch large-scale spam campaigns and to automatically ping pay-per-click systems; hence, large companies may use them as middle-men.

Another example of botnet is TDL4. TDL Botnet network, which was revealed by an antivirus software company, uses about 5 million computers as zombies [41]. The administrators ruling the TDL Botnet Network use their own encrypted algorithm and it is almost impossible to solve the system because they update the algorithm, continuously [42]. This feature of TDL indicates that it is not administrated by simple and trivial hackers.

2.1.3. Denial of Service (DoS) Attacks

DoS attacks result in the blocking of a resource to rightful users. They are synchronized attempts to deny services of servers by causing a computer to perform an unproductive task to overload the system so that it becomes unavailable to perform necessary operations.

Examples of such resources include disk space, CPU cycle, memory and bandwidth. For instance, when there is no free space on a disk, accounts of the users may be locked; or when a CPU slows down, services such as DNS, DBMS may be denied. The attacks may come in many forms and different levels of severity and can cost an organization from little annoyances to considerable lost in revenue.

Such attacks may target security and functionality vulnerabilities in software and abuse these flaws to crash or seriously degrade the performance of, for example, servers. These DoS attacks are classified as logic attacks. Counter measures can be taken by fixing the faulty software or by filtering particular packet sequences. On the other hand, flooding attacks are profiled as sending overwhelming requests to the servers to exhaust CPU, memory and network resources. These types of attacks are more dangerous because it may not be easy to distinguish a DoS request from a regular user request in a peak time [7].

As we have mentioned in section 2.1.2, several computers can be manipulated as zombie computers; attackers may direct such machines to send requests to a target to create large number of compromise host. These combined attacks are referred as distributed denial of service (DDOS) attacks [43].

An example of DDOS attack targeted Twitter and put the site offline for an extended period on August the 6th, 2009 [44].

2.1.4. Port Scans

The connected i.e. networked systems, communicate with each other by sending data through points called as ports. These ports are not physical sockets but digitally numerated access and exit points for receiving and sending data, respectively. Protocols and services are given port numbers to send and receive digital signals. For instance, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) use port numbers to provide separate sub-addresses to hardware to distinguish data belonging to different services and applications and the destination and origin of the data is identified.

As the ports are data entry / exit points, attackers can scan them to spot any open one. This action is called port scanning in the context of network security. Scanning ports of a system may be, and usually, is an indication that an attacker is getting prepared to penetrate / attack. This may be to

identify target system or vulnerable services / ports or to locate host system - target enumeration [5].

To achieve such purposes, usually attackers use programs, port scanners that remotely determine open TCP and UDP ports. Advanced Port Scanner, Angry IP Scanner, nmap, and nessus are just some free port scanner programs that everybody can find, download and use. Such programs are used by security staff to test their systems in identifying vulnerabilities hence design proactive solutions.

A port scan does not cause direct damage; however, it can help the attacker to find unguarded ports for various attacks.

2.1.5. DNS Root Server Incidents

As seen in botnet (section 2.1.2) and DDoS attacks (sections 2.1.3), the damages may not be limited to country borders but may create a global impact. This articulation may appear exaggerated; however, there are further examples such as two DDoS attacks on the Domain Name System (DNS) root servers that occurred on October 21, 2002 and February 6, 2007 [45]. Thanks to the over-provisioning of services, the effects were limited; however the attacks demonstrated potential of causing global disruption of the Internet. If those attacks were successful in full scale then they would create a digital chaos in the World Wide Web, globally.

Those examples show that company precautions may not be sufficient to neutralize such attacks; this creates a new discussion that countries should implement mechanisms to protect the national and global critical information infrastructures [46]. We refer to this issue in more detail in Chapter 4.

DNS attacks are not limited to freeze root servers; because the DNS is responsible for managing the resolution of domain names, any replacement of a valid address with an alternate address causes people attempting to access the domain name to visit the channeled TCP/IP address. By this way, an attacker can create a chance to divert the users to another web site that is

shown as a legitimate site. A common purpose is to steal any information by getting between the user and the real site. Alternatively, the attackers can completely take over the apparent role of the real site. The severity of this infringement increases with the abuse of other services such as FTP and e-mail [5].

2.1.6. Malware

Malware term comes from Malicious Software. Every kind of software with a malicious intention are widely known as malware [47].

There are roughly three broad categories of this type of program code, identified as Trojan or Trojan horse programs, worms and viruses.

Trojans

A Trojan or a Trojan horse is a kind of malicious code which infects computers without user permission / knowledge so that hackers can gain access to get into. Trojans are designed to infect their targets off the user awareness so that they can run without any notice. Because of that Trojan hides itself in harmless software and is sent to the target. While this harmless software implements its own function, Trojan infects to the system.

As known, the name Trojan comes from the wooden horse which was used to sneak in and conquer Troy. The name implies similar purpose as Trojans penetrate into the hard disks through by attachments of e-mails or visited web pages. After a Trojan is on the hard disk, it runs in silence. Neither the user nor the operating system can be aware of the malicious code which can send information to the hacker; popular information stealing and damages are as follows: erasing / renaming files as well as copying files to the infected computer, running an application or terminating applications such as anti-malware software, changing the registry, stealing passwords and credentials, keeping a log to hold keystrokes, disabling hardware such as mouse, keyboard or, shutting down the infected computer.

Worms

A worm is another malicious program that originates from a single computer and searches for other computers connected through a local area network (LAN) or the Internet connection so that it can replicate itself onto another computer and spreads in the network by copying itself. A worm continues to attempt to replicate itself indefinitely or until a self-timing mechanism halts the process. Basic damage of a worm is to consume the bandwidth of network [48].

Other types of viruses include boot sector, application and macro viruses.

Boot Sector Viruses

These are often transmitted via a diskette/USB/CD/DVD etc. The virus is written to the Master Boot Record (MBR) on the hard disk, from which it is loaded into the computer's memory every time the system is booted.

Application or Program Viruses

These are executable programs that infect systems when they run. Viruses can also be attached to other, harmless programs; later, when the program is installed, at the same time, the virus also gets installed.

Macro Viruses

We call virus as macro virus that is written in a macro language. Macro language is an embedded language that automates the performance of some task or sequence in a program such as Microsoft Word.

Viruses that are programmed to "go off" (get active) on a predefined date are called time bombs or logic bombs. One of the first of this type to gain worldwide attention was the Michelangelo virus in the early 1990s which attempted to erase the hard disks of the infected PCs on March 6, the birthday of the famous painter. A few years later, a disgruntled ex-employee of Omega Engineering planted a time-bomb virus on the company's network

that resulted in approximately 10 million USD in loss and damage. He was convicted of this crime and sentenced to 41 months in prison [5].

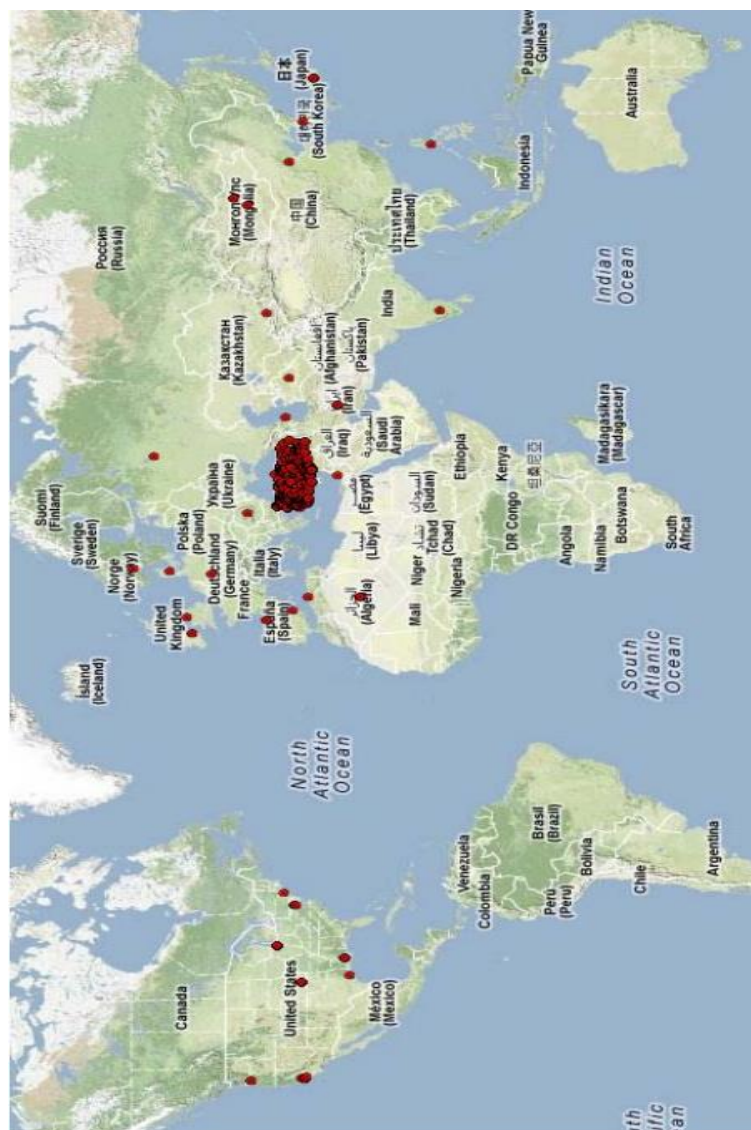
Table 2.2 presents selected big virus infections and damages they have caused.

Malware	Year	Damage
CIH/Chernobyl	In the late 1990s	Damage to business and home computer users. It infected executable files and was spread by running an infected file on a Windows 95/98 machine. There were several variants of CIH; these were "time bomb" viruses that activated on a predefined date (either April 26—the anniversary of the Chernobyl disaster—or every month on the 26th). The virus would overwrite the first 2,048 sectors of every hard disk in the computer thus wiping out the file allocation table and causing the hard disk to appear to be erased. The virus also attempted to write to the BIOS boot block, rendering the computer unbootable. This virus started to show up again in spring 2002, attached on the Klez virus.
Melissa	1999	The first virus to be widely disseminated via e-mail to our knowledge. This macro virus, embedded in Microsoft Word document is activated when the document is opened unless Word is set not to run macros. Sending itself to the first 50 entries in every Microsoft Outlook Messaging Application Program Interface address book, it resulted in a rapid propagation. The virus also made changes to the Normal.dot template of Word which caused newly created Word documents to be infected. Because of the huge volume of e-mail it produced, the virus caused DoS on some e-mail servers. David Smith, creator of the virus, was sentenced to 20 months in prison and was fined 5,000 USD.
Code Red	2001	This self-propagating worm began to infect Web servers running IIS. On various trigger dates, the infected machine tries to connect to TCP port 80 which is used for web services, on computers with randomly selected IP addresses for further infections. Some variations also defaced Web pages stored on the server. On other dates, the infected machine would launch a DoS attack against a specific IP address embedded in the code.

Malware	Year	Damage
		CERT [49] reported that Code Red infected more than 250,000 systems over the course of nine hours on July 19, 2001.
Nimda	2001	This worm infected numerous computers running Windows 95/98/Me, NT, and 2000. The worm made changes to Web documents and executable files on the infected systems and copied itself. It spread via e-mail, network shares, and through accessing infected Web sites. It also exploited vulnerabilities in IIS versions 4 and 5 and spread from client machines to Web servers through the back doors left by the Code Red II worm. Nimda allowed attackers to execute arbitrary commands on IIS machines that had not been patched, and DoS were caused by the worm's activities.
Klez	In late 2001 and early 2002	This e-mail worm propagated through e-mail mass mailings and vulnerabilities in the unpatched versions of Outlook and Outlook Express mail clients. It attempts to run when the message is previewed. When it runs, it copies itself to the System or System32 folder in the system root directory and modifies a Registry key to cause it to be executed when Windows is started. It also tries to disable any virus scanners and sends copies of itself to addresses in the Windows address book, in the form of a random filename with a double extension (for example, file.doc.exe). It is activated on the 13 th day of every other month resulting in files on local and mapped drives being set to 0 byte.
MyDoom aka Norvag worm	2004	This worm set a record as to how fast it was disseminated, and actually managed to slow global Internet performance by 10 %. The worm was spread as an e-mail that appeared to be an error message containing the text "Mail Transaction Failed." When the e-mail is opened the worm spreads by being sent to any e-mail addresses found in address books on the machine. It spread further through shared directories used by the file-sharing program Kazaa. It was estimated that during the first hours the worm was disseminated, one in 10 e-mails sent over the Internet contained MyDoom. It is no longer a threat, because MyDoom was programmed to stop after February 12, 2004.

Table 2.2 - Example of Virus Infections and Damages

Another example is from Turkey, according to the 2012 report of TrendMicro anti-malware company [50], based on the intelligence gathered during a four-month period of close monitoring, a malware named Tinba focused on Turkey. Tinba is a small data stealing Trojan-banker. It hooks into browsers and steals login data, as well as sniffing network traffic. Trend Micro has identified more than 60,000 unique infections in Turkey. This is based on unique IPs, and the numbers may vary. Cyber criminals specifically target financial institutions inside Turkey with the Tinba virus. The infection map on Figure 2.4 highlights that most of the attacks target Turkey.



Figur

This example of Turkey and Table 2.2 are only few examples to show the damage and inconvenience caused by various forms of malicious code.

There are many other malware in the history of digital world; however, they are not limited to attacks launched by individuals but also engineered to cause serious attacks against governments. Popular examples include Stuxnet, Duqu, Wiper and Flame. Because the national cyber security is within the scope of this thesis, we shall visit those viruses in more detail, before Chapter 4.

Stuxnet

Iran's nuclear industry was hit by a virus in 2010 known as Stuxnet, which targeted centrifuges of nuclear facilities, in what was widely believed to be an act of foreign sabotage aimed at slowing Tehran's progress toward building a nuclear weapon. By looking at the aim and the damage it caused, we can say that Stuxnet is an advanced “weapon in the cyber war”.

It was used to deliver a code targeting a specific control system. It is the first industrial control system rootkit. It can self-update even when cut off from C&CS (section 2.1.2). The code is injected into the ladder logic of Programmable Logic Controllers (PLCs), thereafter, it can manipulate the operations of PLC as well as hiding itself by reporting false information back to the human-machine interface which is the apparatus presenting process data to a human operator, and through which the human operator controls the process. It uses system-level, hard-coded authentication credentials that were not publicly disclosed. It signed itself with legitimate certificates manufactured using stolen keys [51].

Duqu

Source code of Duqu Worm, which was detected on 14th September of 2011 firstly, looks like Stuxnet worm and it is considered that it may be developed by the same people who developed the Stuxnet according to Symantec [52]. This worm collected information for reconnaissance instead of blocking the system. Duqu has a fake digital certification just like Stuxnet

and uses Windows zero day exploit, previously unknown vulnerability in the Operating System (O/S) [53].

Wiper

Wiper is believed to be a part of Stuxnet and Duqu series. This malware attack occurred on the Iran's oil sector on 23rd of May, 2012 and spread to other industries [54].

Flame

Flame is one of the most powerful cyber weapon developed within the scope of cyber espionage and it is found in May 2012. The complex nature and the objectives behind the code are considered to have a government support [55] i.e. state sponsored. Virus can manipulate computer equipments such as keyboard, monitor, microphone, storage devices, Wi-Fi, Bluetooth, USB, and even system processors to leak information. With this structure it is more complex than Stuxnet [56]. There are many researchers including [57], who believe that such attacks will increase and will be choices of weapons in cyber wars.

2.2. CYBER THREATS AND THEIR TARGETS

When we look at the nature of cyber threats that are surveyed in this chapter, we can make a coarse classification of the cyber threats according to their nature and targets (**Figure 2.5**).

Basically, such threats are caused by:

- Amateurs / curious people,
- Commercial criminals,
- Hacktivists and
- Attackers supported by states.

Those people target:

- Individuals,
- Organizations (commercial and non-commercial) and
- State organizations / institutions.

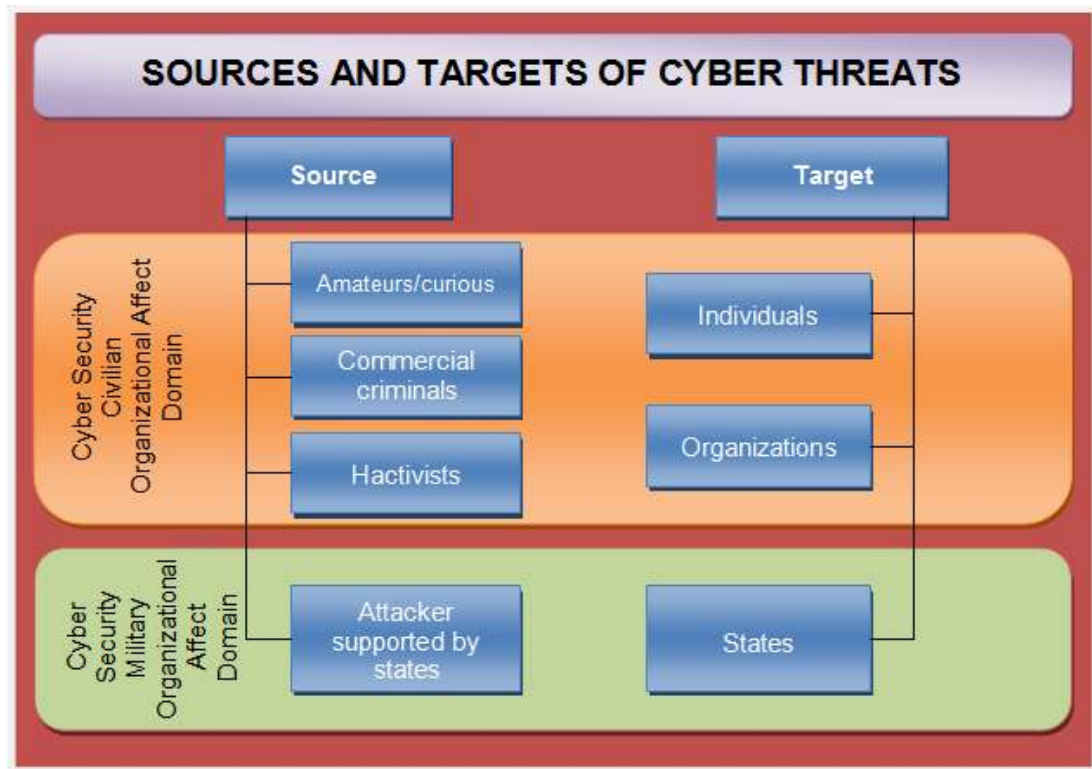


Figure 2.5 - Cyber threats and their targets

2.3. ANTI-MALWARE

Anti-Malware or anti-virus software, as the name implies are the software that guard computers against malware and remove such threats. With the widespread of the malware, anti-malware programs become essential requisites for any computer that process sensitive data or access to the Internet today.

There are many vendors providing such kind of software; hence, institution should (sometimes they do not) carefully examine them for maintenance, after sale support and virus list updates before selecting one. Popular anti-malware vendors are given on Table 2.3 along with the 2012

year average prices for premium services; additionally, most of anti-malware software developers offer free personal usage with limited services.

Anti-malware Brand / Software		Price
	Avast	40 USD
	Avira	26 USD
	AVG	75 USD
	Kaspersky Lab	66 USD
	McAfee	40 USD
	Microsoft Security Essentials	-
	Symantec - Norton	60 USD
	Panda Security	40 USD

Table 2.3 - Anti-malware Brand / Software

Vendors in Table 2.3 publish periodic reports with statistical data on cyber threats. Sample results are given on Table 2.4 and Figure 2.6 about web attacks and vulnerabilities in applications, respectively.

In 946,393,693 web attacks, attackers used 4,073,646 domains. Although malicious codes are detected in 198 countries, 86.4% of them are encountered in the first 20 countries [58].

Rank	Country	Number of attacks	% of all attacks
1	United States	240,022,553	25.4%
2	Russian Federation	138,554,755	14.6%
3	Netherlands	92,652,499	9.8%
4	Germany	82,544,498	8.7%
5	Ukraine	47,886,774	5.1%

Rank	Country	Number of attacks	% of all attacks
6	China	46,482,840	4.9%
7	United Kingdom	44,676,036	4.7%
8	British Virgin Islands	26,336,323	2.8%
9	Canada	19,723,107	2.1%
10	Sweden	15,472,406	1.6%
11	France	14,706,167	1.6%
12	Romania	12,685,394	1.3%
13	South Korea	7,220,494	0.8%
14	Czech Republic	6,009,847	0.6%
15	Latvia	5,371,299	0.6%
16	Spain	5,066,469	0.5%
17	Japan	3,468,602	0.4%
18	Turkey	3,150,767	0.3%
19	Brazil	2,712,440	0.3%
20	Belize	2,660,150	0.3%

Table 2.4 - Top 20 Countries web resources seeded with malware

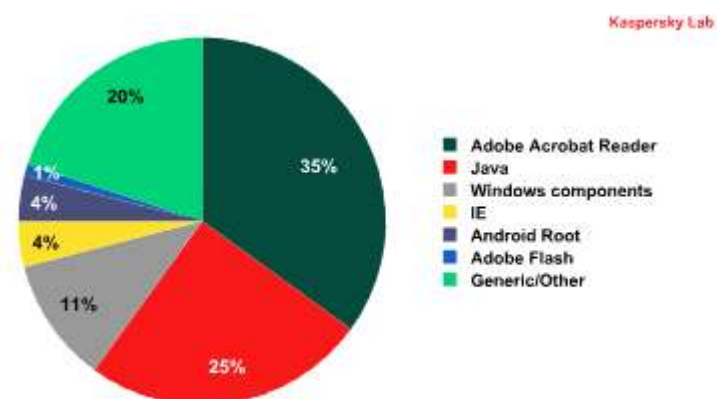


Figure 2.6 - Most vulnerable applications

As seen on the Figure 2.6, Java applications and Acrobat Reader are among the most vulnerability bearing applications for the attackers.

2.4. SUMMARY

Cyber attacks can have severe impacts on the functioning of critical systems both in the public and private sectors. These attacks can be organized rapidly and strike without warning when compared with physical attacks aiming similar damages.

Just by looking at the malware based attacks history, we can easily foresee that number of such attacks will increase in the close future. They are less expensive, can cause physical damage without sending any physical material and / or person to the target.

Additionally, international cyber threats require common responses of multiple countries coordinated at political, economic, legal and technological level as recommended by the ITU [13].

Following is a list of effects of successful cyber attacks, emerged from what we have surveyed in this chapter.

- Provide remote control of systems and collect information to ease further attacks
- Leak sensitive / important / secret information to forge wrong results
- Affect PLC or other type of control systems to damage facilities or equipment's, slow down or stop production, put out of control of the systems
- Cause danger for human life because of malfunctioning system or forged wrong information
- Affect systems to prevent reporting malicious activities
- Lower prestige of institution or country

The literature reviewed informs that there is a variety of threads and anti-malware software products fighting against those threads for both

proactive and after the attack activities. However, relying on software vendors to protect a country's critical infrastructure is open to discussion; hence, we question necessity of having a national cyber security authority and affiliated defense units such as a separate army force, as discussed in Chapter 5.

CHAPTER III

3. RESEARCH METHODOLOGY

This study has been prepared by basic research technique with philosophical assumptions. We have prepared this short chapter for the reader to be informed on the course that the researcher drew an easy-to-follow method to pinpoint the research question and to seek a rational answer to it.

3.1. MOTIVATION

Researcher is employed at the Air Force Command on the information security. He is motivated to study on this topic by the help of his personal experience on the cyber security and his limited interpretation on the requirements of national politics about information security.

In this context, first of all, literature is reviewed about the issue. While the related literature is surveyed, local and foreign books, journals, magazines, conference proceedings, pressed and digital newspapers and websites are reviewed. Additionally, the researcher has interviewed two key informants working in the field of information technologies and security; so technique of observation based on documentation is used [59].

3.2. PHASES OF THE STUDY

At the first phase, threats about cyber security are studied. This research is originated from motivations on learning precautions and threats related to information technologies, mostly, threats on the Internet. Naturally, not every cyber threat has been studied. Popular examples about the issues of cyber security related to these threats are picked up from the incidents and represented in the body-of-knowledge (Chapter 2) of the thesis.

As an outcome of the first phase, it is evaluated that cyber security is a threat not only against individuals and organizations but also against national security. Hence, we have studied possible precautions including nationwide options, at the second phase.

At the third phase, adequacy of the results of this thesis is verified by key informants working on the subject.

At the fourth stage, the researcher has articulated his body-of-knowledge emerged from the literature and drawn knowledge throughout this study as this thesis for reporting.

During the first and second phases of this study various materials have been covered as reported in chapters 2 and 4. Those materials are listed in the References section whenever a researcher's ideas and / or findings have been used in accordance with the statement of non-plagiarism given on page iii,

The researcher's own thoughts are expressed in this thesis including findings, limitations, future research avenues and discussions, and any extra material is not attached to it; however, it is not possible to cover all the literature and there may be unintentional similarities out of our knowledge. Such unwanted coincidences could raise plagiarism discussions regardless the intension of the researcher. The researcher is aware that any illegal use of copyrighted material is seriously emphasized in academic writing guides [60]. As a precaution against such coincidences the thesis is passed through a plagiarism detection software, Urkund, before the final print so that an additional check could be done before the reviewers assess it.

3.3. VALIDATION OF THE FINDINGS

While precautions related to threats are studied, general procedures and internationally accepted standards and practices implemented in other countries are studied. The issue is not handled with technical details; however, procedures associated with precautions at individual levels are

determined; standards at the organizational levels and strategic documents at the national level were required.

As known, creating / improving new viewpoints which are developed by individual experiences are accepted as data sources by the grounded theory [61] in the universe of social reality. In parallel with this point, researcher consulted two key informants working in the sector to validate findings.

While the researcher has consulted key informants, having a written consent is not seen as a necessary procedure as neither audio nor written recording took place. This consultation is limited to validate the findings and does not target to collect information. However, a successive research to obtain empirical data (section 5.2) may and expected to collect information from individuals; hence, written consent will be required as direct quotes can be used to show information sources.

3.4. SUMMARY

In conclusion, the researcher has developed information and knowledge already reported to the literature and validated the drawn knowledge by the additionally literature survey and key informant responses. Such kind of research is named as “basic research” according to [62]. The researcher has taken Çankaya University, Graduate School of Natural and Applied Sciences Thesis Manual [63] as reference in the preparation of this thesis.

CHAPTER IV

4. CYBER ATTACKS AND STATES

As we have covered major types of attacks and attackers in Chapter 2, they may be quite harmful for a state own organization or institution; such an attack may pose more severe damage than a corporation under the same threat. Especially, a cyber attack to a country's electronic government service and / or critical infrastructure can create a new war place other than land, air or sea which are protected by army forces. An intrusion of an army unit to another country without permission can be a reason to declare war. Fortunately, no nation has declared a cyber war to date; however, many governments have spoken out about cyber activities.

This chapter serves to highlight cyber attacks that target government agencies (section 4.2) and national critical infrastructure (section 4.3), information security standards (section 4.4) and cyber security strategies of selected countries (section 4.5.1). The chapter concludes (section 4.6) that Turkey needs to act more rapidly in solidifying a cyber security strategy nationwide.

4.1. INTRODUCTION

About five years ago, ITU made clear that assets, resources including human, financial, technical and information of organizations are within the concern of cyber security; hence, such security should include precaution and guard against the threats as well as restoring damaged services / functions in reasonable time and money [13].

Organizations are commonly utilizing anti-malware solutions and they do not have to spend considerable amount of money for such a guard (Table 2.3). Likewise, the governmental agencies are installing such security

software. Those software solutions offer safety and backup facilities; however, this may not always cover the total cost of a cyber attack as we have seen in Chapter 2. Furthermore, virus libraries are updated and disinfection methods are developed after such attacks occur, naturally. Hence, anti-malware solutions do not provide total security and recovery. NATO underlines that more combined security schemes are seen as necessities as information technologies can be used as asymmetric weapons [64] and they can be state initiated attacks. Consequently, it is known that there are countries developing their cyber weapons capabilities (sections 4.6 and 5.5.1). While NATO took some passive precautions after 2001 Twin Towers Attack, it mentions Cyber Defence 2.0 [65] with radical precautions after the 2007 Estonian Cyber Attacks (section 4.2).

4.2. INTERNATIONAL CYBER ATTACKS

As we have seen structures of some malware (Chapter 2), the countries can use cyber technology to attack each other. Recent examples include the 2007 (possibly Russian) cyber attacks against Estonia. A series of cyber attacks targeted websites of the prime minister, parliament, most ministries, political parties, and big news organizations. There were also attacks to the infrastructure that let the government communication network to slow down. Due to the attacks, members of the parliament could not use e-mail communication for four days. The country's finance sector has also been hit and lots of bank transactions have been compromised, ATMs slowed down, and Hansabank, the largest bank, had to stop its operations on the internet. A hacked web site screenshot is on Figure 4.1.



Figure 4.1 - A Web site screenshot from Estonia in 2007 [66]

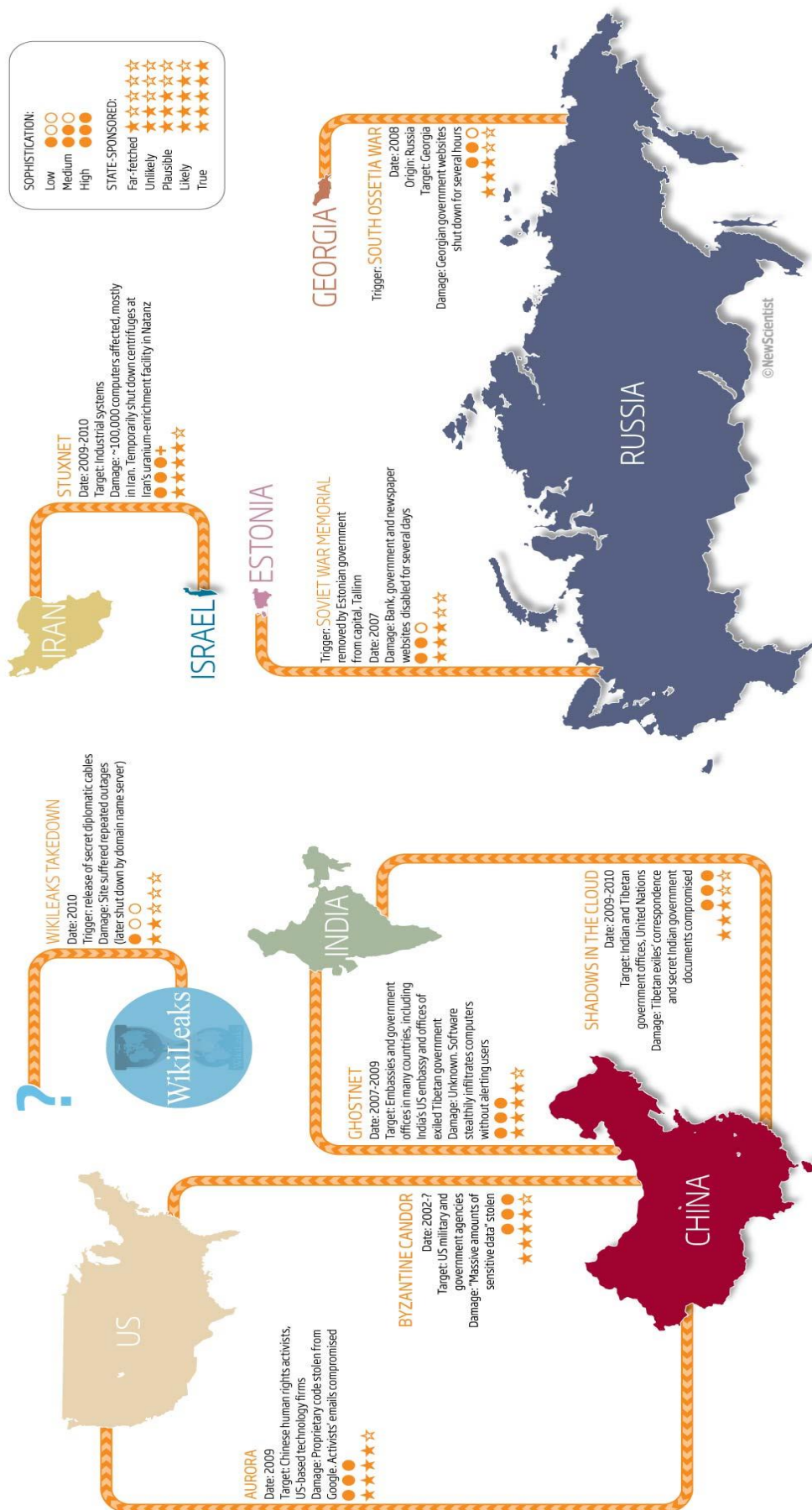
As a temporary solution, Estonia has isolated itself so that no one could get into the country, digitally. This had a consequence that people with bank accounts but outside the country at that time could not access their accounts [67].

After the attack, NATO's Cooperative Cyber Defense Centre of Excellence was established in Tallinn, Estonia [68].

Another attack occurred as a series of Russian assault to Georgia's government agency websites in 2008 as integrated cyber and kinetic attacks by Russia. The attacks were intensive, but their time span was shorter when compared to Estonia case. An average cyber attack lasted 2 hours and 15 minutes, and the longest one went on for 6 hours as reported in [69].

When Russia has declared war to Georgia for the independence of South Ossetia, cyber attacks blocked channels of communication at a strategic time periods. Additionally, 36 main websites are disrupted or suspended hence communication ability of the Georgian government with its public is slowed down just before the start of the war [70].

Both Estonia and Georgia cases involve nation states and call of military actions. Other selective incidents are mapped on Figure 4.2. Most of these attacks have been called criminal acts [71].



The discussion of international cyber attacks accelerated with three successive attacks, Stuxnet, Duqu and Wiper, to Iran as we have visited in section 2.1.6. While the political tension is increasing between Iran and the USA and Israel, it became easier to think that those attacks are planned and are performed by those countries and by using cyber weapons. According to the news on New York Times [73], Stuxnet has deactivated 1000 centrifuges of 5000 in Iran and delayed its nuclear program for 1.5 to 2 years, and this attack was the successor of the cyber attack program started by the Bush government under “Olympic Games” name and accelerated during the Obama government [74].

As of its nature, the cyber attacks target / initiate in software although its damage is not limited to digital environment. Software products, unlike physical structures, may have / need frequent update due to rapidly changing user needs [75] hence a stronger business connection between the user and the vendor can occur. For example, Symantec [76] providing protection against Stuxnet, can be seen as “private army” that guards critical infrastructure of Iran.

Such incidents bring discussions on taking precautions against state targeted cyber attacks.

How can government agencies trust anti-malware companies?

Shall the countries build state own cyber armies?

4.3. CRITICAL INFRASTRUCTURE

As known, some infrastructure such as water treatment and distribution, telecommunication, power and energy distribution are vital for countries. Large scale damage to any of them would create considerable impact on nation not only on human life but also in finance sector and pride of nation. As we have seen in section 4.2, cyber attacks can create physical damage; hence, it is necessary to take precautions to protect such infrastructure facilities against digital attacks in peace and war time. Space Command boss General William Shelton said that it is not easy to even see close future out,

given how quickly the cyber-world changes [77]; thus, it is not possible for states to response against quickly changing cyber space.

Today, we depend on control systems more than we used to in the past; hence, to sustain security, maintain economic operation, protect the public health and safety, and protect the environment countries should keep control systems secure.

Countries are expected to determine their critical infrastructure and Turkey is not an exception.

In USA, following sectors are identified as part of critical infrastructure and key assets sectors [78]: agriculture and food, water, public health, emergency services, defense industrial base, energy, transportation, banking and finance, chemicals and hazardous materials, postal and shipping.

Critical infrastructure sectors of European Union countries are: energy, nuclear industry, information, communication tech., ICT, water, food, health, financial, transport, chemical industry, space, research facilities [79].

In Turkey, there is no any official published documentation about critical infrastructures; however, there is a draft documentation prepared about Cyber Security Strategy. This document offers some sectors as a critical infrastructure. These are: information, energy, finance, health, food, water, transportation, defense, public security, nuclear-biologic-chemical facilities [80].

4.4. INFORMATION SECURITY STANDARDS

There are national and international boards which produce standards in information technologies against cyber threats.

4.4.1. ISO/IEC Standards

As known, International Electrotechnical Organization (IEC) and International Organization for Standardization (ISO) publish standards both in commercial an electro-technical areas, internationally. Both organizations' standards are accepted internationally.

When we have a glance to the history, we see that studies on information security are started by British Standards Institute (BSI) before ISO/IEC (Figure 4.3) to our knowledge. BSI concentrates on the continuously updated threats, tracking security exploits occurring on hardware or software and how to control human factor.

At the end of the studies first part of the BS7799, BS7799-1 were issued in 1995 and second part BS7799-2 was issued in 1999 by BSI.

BS7799-1 was accepted in 2000 by ISO as ISO/IEC-17799 after minor modifications and adaptations; consecutively, it has become a globally accepted standard. In 2002, BS7799-2, which is the second part of BS7799, was issued by BSI second time as English standard after additions and modifications. In 2005, ISO made further changes on ISO/IEC-17799 standard and it is issued again as ISO/IEC-27002:2007 in 2007.

The commonly known ISO/IEC:27001 has been published after BS7799-2 of BSI in 2005.

ISO/IEC:27001 is a mentor prepared for installing, performing, keeping on and updating the information security management system. It is different than the published standards till 2005, because it includes information security checks and information security intrusion management. These additional features are considerably important in taking required precautions to dodge attacks hence, infections and events related to information security.

Although it is argued, for example by [81], that implementing ISO/IEC 27000 standards cannot guarantee organizations' information alone, this standard involves recommendations on information security management.

Issue times of standards focusing information security management systems are given on Figure 4.3 as a history line.

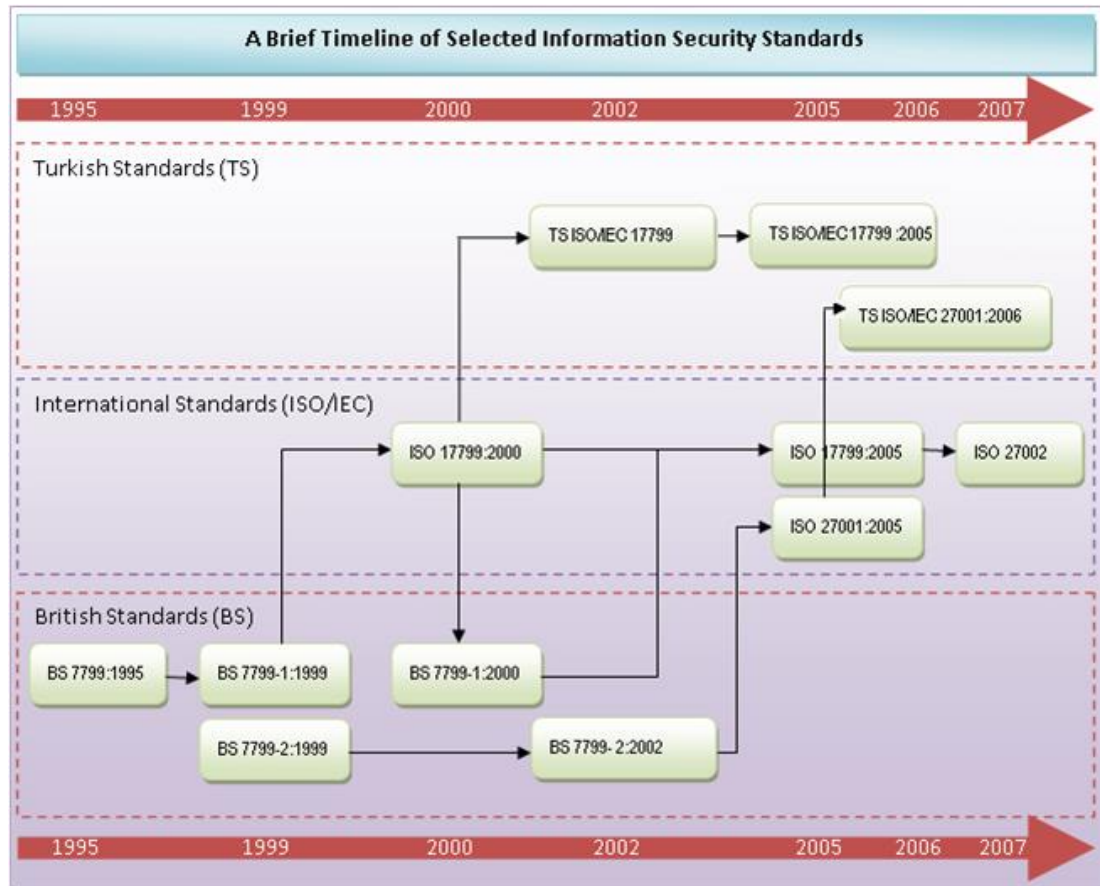


Figure 4.3 - A Brief Timeline of Selected Information Security Systems

While the second part of BS-7799 defines how to install information security management system, the first part of BS-7799 guides how to check information security system. This standard is designed to provide a model for managers and personnel to install and manage effective information security management systems. In this model, plan, implement, check and review steps are defined.

Another English standard related information security management systems is prepared as BS7799-3:2005, Information Security Management Systems Risk Management Rules, in December 2005. In 2006 an update is published as BS7799-3:2006.

4.4.2. Turkish Standards (TS)

In Turkey, studies and documentation on information security standards are performed by Turkish Standards Institute (TSE). As seen on the Figure

4.3, Turkey is not among the pioneers in the information security standards. Hence, the institute takes standards that have already been accepted internationally and publish them in Turkey. Likewise, TS ISO/IEC 17799, Performing Principles for Information Security Management, is accepted as Turkish standard after TSE technical commission interpreted ISO/IEC 17799:2000 standard in 2002. TS ISO/IEC 17799 includes advices about information security management which initiates carries out information security structure of organizations and provides continuity.

For the purpose of documentation of information systems security management, TS ISO/IEC 27001:2006, Information Technology-Security Techniques-Information Security Management Systems-Necessities, is accepted in 2006; this standard is an interpretation of ISO/IEC 27001:2005.

This standard is a milestone both in the world and in Turkey, because BS7799-2 standard was the base for documentation and adaptation of institutional information security management system until 2005; ISO/IEC 27001 is more adopted, thereafter.

Another standard is TS ISO/IEC 15408 the Common Criteria for Information Technology Security Evaluation, in short, Common Criteria (CC). CC include basis for evaluating the security specifications of IT software, hardware and systems. With the assessment the product is determined whether to provide the required safety standard or not [82]. CC certificate is given by a limited number of countries including Turkey. CC evaluation assurance levels (EAL) are listed (Table 4.1) below:

Level	Assurance Level
EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested, and reviewed

Level	Assurance Level
EAL5	Semi-formally designed and tested
EAL6	Semi-formally verified, designed, and tested
EAL7	Formally verified, designed, and tested

Table 4.1 - CC evaluation assurance levels [83]

Product categories evaluated in CC:

- Access Control Devices and Systems
- Biometric Systems and Devices
- Boundary Protection Devices and Systems
- Data Protection
- Databases
- Detection Devices and Systems
- ICs, Smart Cards and Smart Card
- Key Management Systems
- Multi-Function Devices
- Network and Network-Related Devices and Systems
- Operating Systems
- Products for Digital Signatures
- Trusted Computing

4.5. RESPONSIBILITY OF THE STATE

The state possesses considerable responsibility for making physical security within its borders. However, as we have reviewed cyber attacks in section 4.2, digital security should be within the concerns of a nation's defense because an attacker may create physical damage by cyber attacks. This damage is not only limited to causing waste of money on changing expensive equipment or shutting down government websites. While we compare cyber weapons to other weapon systems, Cyber Force emerges as a pretty humanist system besides advantages of cost, effect, and range.

However, a cyber weapon more sophisticated than Stuxnet may cause more damage than a missile with warhead.

The ITU [13] argues that each state has responsibilities other than encouraging research and conferences in cyber security such as creating a cyber security culture in conjunction with information society. This includes law, finance, industry and social cooperation with other countries' bodies affiliated with the cyber security and coactions of public and private organizations for national strategies.

Same argument continues that responsibilities and right in ensuring privacy and security in information sharing, reporting and publishing should be defined at the strategic level while best practices in risk management and security are clarified.

Those actions are far beyond passing few act of law in the parliament. As building an information society is one of the national targets [2], it is essential to provide education, information and training in information processing and communication technologies to construct awareness of cyber security hence a cyber code of conduct. As a natural consequence, civil-defense authorities, emergency services, armed forces and security forces would be given not only tactical but also limited operational role against cyber threats to protect, prosecute and recover after an attack.

A discussion can easily start in this point that armies have to have both of defensive and offensive capabilities. For that reason, also Cyber Armies have to have defensive and offensive capabilities and develop these capabilities to get over the capabilities of possible cyber threats. As a consequence, a cyber command to be founded in the structure of Turkish Armed Forces (TAF) can protect not only the infrastructure of TAF's information technologies but also critical infrastructure systems of the country. Because of that, cyber command should have information and capability to prevent cyber attacks before time of crisis and aggression; hence, it should have authority to coordinate cyber security issues with civilians.

As interpreted from ITU, it is necessary to structure and develop strategy documents that define priorities and precautions in cyber security. This includes developing policy for the information society for protection and the struggle against cybercrime. Following section gives examples from selected countries which put effort in developing national cyber security strategies.

4.5.1. Cyber Security Strategies

The countries leading the world politics need to take strategic precautions which modern era requires for progressing and not losing their position. The report of United Kingdom Cabinet Office 2009 prepared as “Cyber Security Strategy of United Kingdom” [84] indicates this requirement by this statement:

“...Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space...”

Developed Countries started to build up strategies for information securities as they have understood the importance of this issue. The European Union members are exchanging information and experience through conferences to promote their cyber security strategies even at the time of writing of this thesis. Examples include 1st International Conference on Cyber Crisis Exercises & Cooperation. This conference is organized for sharing of experiences and enhancing cooperation among the participants.

USA, UK, Germany and France have considerable effort in structuring national strategies on cyber security.

USA National Strategy Document was issued in 2003 as “The National Strategy to Secure Cyber Space” [85]. It highlighted that providing the security of cyber space is possible only by efforts and cooperation of federal and states’ governments, every individual and especially private and public sectors. Main responsibility to provide the cyber security is given to the Department of Homeland Security by strategic document. Another strategic

document is prepared in 2008 in which there are directives for protecting military, civilian and governmental computer network and systems and critical infrastructure and strategies to follow in a cyber war [86]. We give a figure from USA just to underline the importance given to cyber security; Defense Advanced Research Projects Agency (DARPA) increased its cyber security research budget 50 % increasing to 208M USD [87].

Cyber Security Strategy of United Kingdom defines the cyber threat as the very first risk of the 21st century and in this scope, it determines that international coordination, installing a central cyber security office and defining flaws not only in technology but also in doctrinal, legal and politic regulations are needed [84].

German government stresses protection of critical information infrastructure and security of national public system; hence, they have agreed that it is necessary to establish a National Cyber Security Council and National Cyber Intervention Center [88].

France is another country which defines protection of critical infrastructure and ensuring the security of cyber space as national strategic targets [89].

To our knowledge, there is no strategic concept as seen in the countries mentioned so far; however, it is assessed that a document like a road map for the studies is necessary as the document published by ISA [80], which has been published at the writing of this thesis.

4.5.2. Precautions in Turkey on Cyber Security

Countries mentioned in section 4.5.1 have already structured their road maps in cyber security i.e. their governments provide information for organizational security targets.

As these examples show, cyber security should be considered not only from a technical perspective but also organizational and individual i.e. user dimension as well.

As we mentioned before (section 2.1), weaknesses in cyber security create threats not only in the private sector and on the individuals but also in the public sector. The armed forces (army and police) are responsible of the security of the public. As a natural consequence, the police and the army are supposed to have ability to fight against illegal actions in cyber environment hence threats. However, this right to use power is not limited to proactive solutions such as taking precautions for defense but also counter attack capabilities.

Currently, the precautions in Turkey are limited to separate strategies of the organizations. For example, having a penetration test is just an option for the organizations and it is not so widely conducted.

Among the other efforts about the issue are the Cyber Security Exercises in Turkey. First National Cyber Security Exercise was performed by the participation of 41 different institutes / companies between 25th and 28th of January 2011. At the time of writing this thesis, the Second National Cyber Security Exercise is planned to be performed by more participant, in 2012.

As section 4.4 stated about the information security and background of international standards, TSE has adopted such standards since 2000s. To our knowledge, adopting these standards, such as TSE 27000, are not obligated for the businesses. However, there is slow inclination in the public sector to comply with the cyber security standards; for example, FATİH, a nationwide project concerning all the private and public schools, is initiated by the Ministry of Education, and the ministry has put EAL4+ of TS 15408 restriction to the contractor companies for gateway switches.

There are legislation precautions such as following act of law in Turkey [90]: article 243, intrusion to information system; article 244, preventing the system, impairment, damaging or alteration of the data; and article 245, misuse and abuse of bank accounts and credit cards.

Also by the “Electronic communication law” numbered 5809, responsibilities including the following items are appointed to Information Technologies and Communication Institute:

- Protecting confidentiality of information security and communication,
- Providing counter system against unauthorized accesses,
- Adopting standards and specifications including serving quality and
- Taking precautions ordered by the legal regulations for implementation of national security in the electronic communication sector, public order and services

Precaution against cyber treats is a relatively new topic and there is a considerable room for discussion and proposals for research. These include but not limited to the following items to be read in conjunction with section 5.5.

- Establishing a national warning mechanism managed by the state

Such a guard should be formed by considering cyber critical network infrastructures, as mentioned in section 4.3, precautions defined in the peace time, and national standards for determined sectors.

As a preliminary work, security methods for the critical infrastructure should be defined including national, commercial and non-commercial encryption algorithms and hardware as well as usage of certified software and hardware.

- Designing a non-military structure of cyber defense

In this structure, governmental agencies can evaluate specialists and approve their positions for digital forensics, cyber crime investigations and penetration testing. Additionally, software and hardware certification can be developed. In this scope, encouraging and / or enforcing the usage of national – if not open source code – software is another point of discussion

as we think of series of attacks against critical infrastructure (section 4.3). Government should support research and development projects for national products; however, it cannot exercise pressure on the developer for they should expose source code of their products; nevertheless, a black box software can always rise a question of “how can we be certain that security vulnerabilities are not there on purpose?”

- Educating users in cyber security in conjunction with information society

One of the vulnerabilities in cyber security is the human factor. For instance, the Botnets (section 2.1.2) are based on the enslaved computers of unconscious users. For that reason, training schemes would be beneficial in the institutions to promote the awareness of the personnel. In this scope, precautions to be taken by the individuals for cyber threats include using firewall, keeping software, especially anti-malware software, updated, restricting users accounts, hence leaving full authentication only to the administrative staff, being aware of danger associated with web links and electronically transferred files, such as e-mail attachments, using only controlled software and being aware of social engineering attacks, hence using strong passwords.

- International coordination and cooperation

Such partnerships can promote individual power of Turkey to a cross border capability in fighting against international threats. As the origin of the attack can well be off the target country, international cooperation bears vital necessity.

- Distributing cyber security responsibility

Considering the difficulties to provide the cyber security in the way of public institutions, instead of separate precautions, it should be considered to take advantage of technologies such as cloud computing. However,

administration and protection by central attack detection and prevention systems should be considered.

4.6. SUMMARY

Although there are discussions in the literature such as [81], adopting information security standards are seen to provide advantages to organizations. Those advantages include guidance on information security management. Still, we should be cautious to say that cyber security can be guaranteed by adopting standards. We should remember that, systems are only as secure as the people who operate them. Hence, creating awareness in the society should be an overarching national target. For this, leaving this security issue to the IT personnel is no longer a complete solution for the organizations. Organizations should have cyber security documents that dictate principles on digital precautions and what to do in case of an attack. Additionally, users should be trained to adopt such principles. As we have mentioned in this chapter, organizations are somehow following this line; however, this should be arranged by the government so that organizations' principles are directed by a national cyber security strategy.

As found in this chapter, the developed countries have already started to shape their national cyber security strategies and Turkey has a considerable way to cover the gap.

Directed attacks on public institutions or vital corporations have potentials of damaging a country. For this reason, for example in USA, Pentagon has declared that any state sponsored computer sabotage can constitute an act of war which may lead USA to respond by traditional military force. Similarly, [91] informs that that cyber attacks targeting places such as public institutions will be considered as a reason to declare war. Consequently, USA established Cyber Command on 23 June 2009. China and Iran also have their cyber armies.

CHAPTER V

5. DISCUSSION AND RECOMMENDATION

We reviewed type of cyber threats and damages in this thesis. We discovered that developed countries give great importance to cyber threats such as terrorism and they are developing strategies against cyber threats. Examples mentioned in (sections 2.1.6 and 4.2) indicate that individual precautions such as firewall, anti-malware and security standards are not enough. An early conclusion remarks that while dealing with cyber threats we should notice their impacts on the countries with infrastructures dependant on IT; hence, this aspect should be taken into consideration as priority.

While discussing what is done and what can be done in Turkey (section 6.2) we have found that cyber security promises many research avenues including future works we presented in section 6.1.

In addition to them, there are many other potential works as already given in section 4.5.2; however, we limit our list in this thesis. Nevertheless, this section is dedicated for we can make quick recommendations emerged from our studies.

5.1. MILITARY PRECAUTIONS

Countries constitute armies and intelligence organizations against threats from other countries to assure their survival. Even though “counter attack” does not sound a peaceful term, a cyber army constituted against cyber attacks with the same purpose of conventional armies against armed threats can be started at peace time. Some other countries (Chapter 4) have similar attempts; for instance, USA is a good example at this issue. In the structure of USA Armed Forces, there is a cyber force at the level of an army established in 2009. While thinking the space as the forth force, cyber has

already proven itself as the fifth force after army, navy, air and space in the military literature.

In 2009, a virtual criminology report prepared by McAfee [92], informs that countries including China, Russia, USA, Israel and France are not only collecting information about cyber space activities but also developing cyber attack techniques; also North Korea, Iran, Taiwan, Brazil and India are known to have cyber attack programs.

Such attempts of those countries open discussion topics on accommodating a cyber force in the structure of the armed forces to ensure that all the armed forces are ready for any type of cyber attack 24/7. To make such a body possible, there are many regulation works including legal, political, social, financial and public administrative projects.

As the human holds one of the primary roles in the cyber security, training and recruitment schemes should be prepared with the cooperation of the universities and the industry; security administrators, chief information officer (CIO), chief privacy officer (CPO), IT managers, cyber criminal investigator and encryption specialists are some quick examples.

Building such a structure in the armed forces requires extensive preliminary works for the limitations, rights and responsibilities should be defined clear-cut.

Malware codes are considered as digital / cyber weapons that can create physical as well as digital damages (section 2.1.6). They can be installed in or attached at digital documents and easily spread over by using security holes in hardware and software. Hence, preferring national software and hardware in critical infrastructure, armed forces and public sector has been a hot topic of discussion most of the time as the IT is getting used in most of the strategic institutions (section 4.3).

As seen in Figure 5.1 in section 5.5.2, it is considered that building an organization to confront cyber threat can be structured as civil and military origins. Based on that, an overarching committee (section 5.2) with

consultants from the academia, experts from the industry, members of parliament, military and civilian bureaucrats, to manage regulations (section 5.3) and commands (section 5.4) can be open to discussion (Figure 5.1).

5.2. CYBER SECURITY SUPERIOR COMMITTEE

This committee's task and responsibilities are to be discussed to seek dynamic solutions to the following list:

- Preparing and updating the cyber security strategy documents,
- Coordination between cyber security regulation organization and cyber security command,
- Assistance in the preparation / amendment of legal regulations,
- Evaluating activities of cyber security regulation organization and cyber security command.

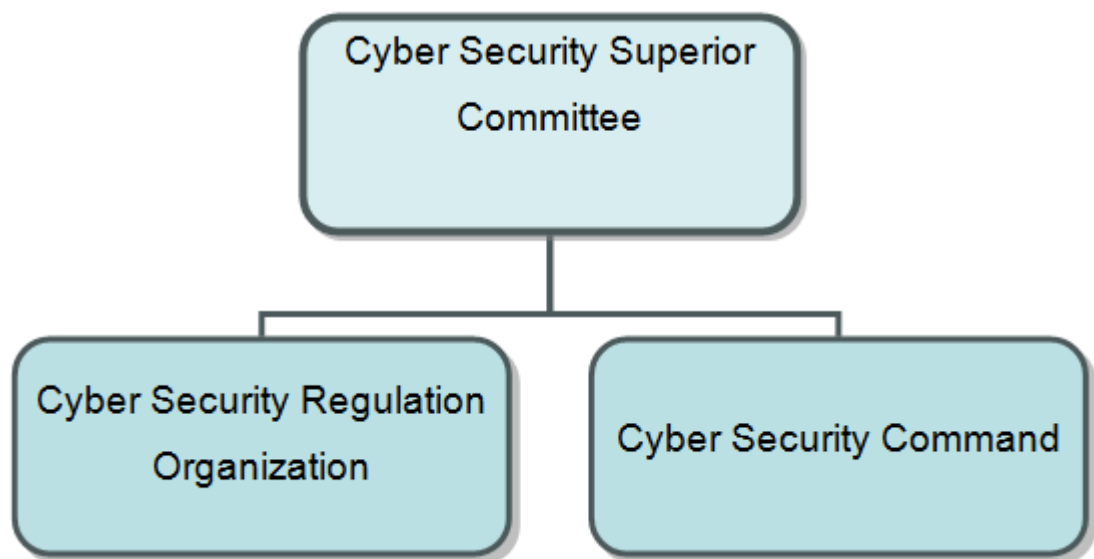


Figure 5.1 - Cyber Security Organization

5.3. CYBER SECURITY REGULATION ORGANIZATION

The existence of such an organization may be discussed to ensure:

- Defining and checking precautions which should be taken by governmental and private sectors according to cyber security strategy document,
- Keeping a national warning system,
- Planning for development of national software and hardware

Widely used applications and systems, are more open to have vulnerabilities. Beside this, methods used in big organized attacks as Stuxnet, Duqu (possibly supported by a state) mentioned in Chapter 4 and zero day exploits increased the doubts of which all these exploits are established consciously and on purpose. Because of this, software developed and certified nationally should be used as much as possible to clear such conspiracy theories.

This would keep the discussion of having national software especially for the systems given as follow:

- Operating Systems,
- Anti-malware / Antivirus,
- Firewall,
- Office applications.

5.4. CYBER SECURITY COMMAND

Such a command office can have following rights and responsibilities open to discussion:

- Coordination of the separate activities of command forces (air, navy and army) by being organized under General Staff.

- Defining the military standards in conjunction with the ISO, European Norms (EN) and TS standards,
- Developing software, hardware considering the requirements of other command forces or contracting / outsourcing to develop,
- Meeting the expert requirements of command forces or developing precautions to meet expert requirements,
- Certificating IT of new and current weapon systems adopted by TAF,
- Confronting cyber attacks against the country in a coordinated way with the cyber security regulation organization,
- Applying the cyber precautions against enemy in the period of aggression and crisis.

CHAPTER VI

6. CONCLUSION AND FUTURE WORK

In the previous chapters we have seen that, cyber threats are not only annoying malware infects in computer that disrupt files, or send advertising e-mails. This thesis reports that cyber threats target commercial secrets or secrets of states and are able to paralyze daily life by breaking down the infrastructure of IT which countries are depended on. Moreover, cyber threats are able to cause physical damages to the critical infrastructures of countries.

This conclusion chapter compiles the findings to respond the research question (section 6.3). Future works should be read in conjunction with discussion and recommendations (Chapter 5).

6.1. FUTURE WORKS

The thesis emphasis that state should be given responsibility to draw national strategy in cyber security. Follow-up research topics, such as surveillance and detection of potential threats related bearing cyber crime risks, are expected to emerge. For this, privacy of the individuals and organizations, reliability and accountability of the government agencies should be studied carefully; hence, collaboration between IT, law and public administration professionals are encouraged.

Empirical works such as semi-structured interviews and / or questionnaires can yield qualitative and quantitative results on anti-malware software usage and organizational behavior on cyber security. Such a research instrument can be constructed by itemizing cyber security concerns by questions which emerge from literature review. Later, those questions can be aligned via discussions with key informants in the industry.

Once the scope of the national strategy is drawn feasibility works can be initiated in the public and private sector as pilot initiatives.

6.2. FINDINGS

(1) Anti-malware software and standards are not enough to guarantee digital security

Using anti-malware software is a common practice for almost anyone doing work with computer; for example, Windows 7 O/S offers Microsoft Security Essentials as default; however, there are lots of examples in which computer systems are hacked although anti-malware software are installed on them.

(2) Organizational and mostly individual level security measures are dominant

With the support of the finding (1) and the conclusion drawn in Chapter 4, leaving the cyber security totally to the IT personnel is a poor approach to secure computer systems.

Obviously, technology should be a part of the solution; however, an integrated approach with the technology, organization and human dimensions would yield more security as concluded in section 5.6. Currently, there is no state guidance in securing companies computer systems in Turkey; hence, the organizations are developing their solutions and precautions in isolation.

Parallel information exists in open sources that even though TAF does not have any cyber security structure as US Cyber Security Command, Command Forces have precautions individually and Chief of Staff have some directives which arrange the cyber security issues.

(3) National strategy in cyber security is required

As the finding (2) informs, the organizations are not guided by the government. Putting the government as a stakeholder in this security issue

will help the development of a national strategy in the cyber security. Hence, the state should provide a road map to both public, private sector as well as individuals.

Even though there are already main regulations in Turkey (section 4.5.2), these are far away from meeting the requirements today; to meet the requirements about cyber world; further work should be done on defining sanctions about responsibilities of persons, commercial and public institutions and intrusions in this area so that legal framework can house cyber crimes in a more comprehensive way.

At the end of thesis research, it is assessed that cyber security should be put in the pot of the major targets in the 10th Development Plan. 10th Development Plan guide of special expertise commissions [93] has already launched hence time, human and financial resources should be managed carefully and without wasting time.

6.3. CONCLUSION

Coming back to the research question, “Should state play an affective role in national cyber security? If it has to, what the state has to do?” our answer is quite positive i.e. Turkey needs to develop a cyber security strategy applicable nationwide; hence, the development agenda needs to include cyber security in, as a separate chapter.

This issue should be kept in greater importance with short and mid-term targets, performance measures and workshops.

REFERENCES

- [1] **WSIS.** (2005). *Report of the Tunis phase of the World Summit on the Information Society (WSIS)*. Tunis: WSIS.
- [2] **Devlet Planlama Teşkilatı.** (2006). *Dokuzuncu Kalkınma Planı (2007-2013)*. Devlet Planlama Teşkilatı Web site: <http://ekutup.dpt.gov.tr/plan/plan9.pdf>
- [3] **Resmi Gazete.** (2012, 06 05). *Onuncu Kalkınma Planı Hazırlıkları*. Retrived 07 15, 2012, from T.C. Resmi Gazete: <http://www.resmigazete.gov.tr/eskiler/2012/06/20120605-7.htm>
- [4] **Ministry of Development.** (2011, 10). *Orta Vadeli Program (2012-2014)*. Retrived 07 30, 2012, from Kalkınma Bakanlığı Web Site: http://www.kalkinma.gov.tr/DocObjects/View/13636/OVP_2012-2014_Baski.pdf
- [5] **CROSS, M., & SHINDER, D. L.** (2008). *Scene of the Cybercrime 2.Ed.* Burlington: Syngress.
- [6] **Norton** (2012). 2012 Norton Cybercrime Report. Retrieved 07 09, 2012, from Norton Web Site: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
- [7] **NEWMAN, R. C.** (2009). *Computer Security: Protecting Digital Resources*. USA: Jones and Barlett Pub.
- [8] **United States Computer Emergency Readiness Team (US-CERT).** (2010, 03 18). Privacy Impact Assessment for the Initiative Three Exercise. USA: Department of Homeland Security. Retrieved from Department of Homeland Security
- [9] **BEAVER, K., & MCCLURE, S.** (2010). *Hacking For Dummies, 3rd Ed.* Hoboken, NJ, USA: Wiley Publishing Inc.

- [10] **SCHELL, B. H., & MARTIN, C.** (2006). *Webster's New World Hacker Dictionary*. Indianapolis, IN: Wiley Publishing, Inc.
- [11] **CIAMPA, M.** (2009). *Security+ Guide to Network Security Fundamentals*. ŞEHİR: Cenagae Learning.
- [12] **TBMM.** (2004, 09 26). Türk Ceza Kanunu (Kanun NO:5237, Madde NO:243). Ankara, Turkey.
- [13] **ITU.** (2007). *Cybersecurity Guide For Developing Countries*. Geneva, Switzerland: International Telecommunication Union.
- [14] **CBSNEWS.** (2011, 06 09). *Citigroup hacked, customer data exposed*. Retrieved 04 05, 2012, from CBSNEWS Web Site:
http://www.cbsnews.com/2100-500395_162-20070251.html
- [15] **NTVMSNBC.** (2011, 04 27). *PlayStation: Kullanıcı bilgileri de çalındı!* Retrived 04 05, 2012, from NTVMSNBC Web Site:
<http://www.ntvmsnbc.com/id/25207123/>
- [16] **GORMAN, S.** (2011, 12 21). *China Hackers Hit U.S. Chamber* . Retrieved 04 05, 2012, from The Wall Street Journal Web Site:
<http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html>
- [17] **CNNTÜRK.** (2012, 03 29). *RedHack'ten emniyete büyük eylem* . Retrived 04 05, 2012, from CNNTÜRK Web Site:
<http://www.cnnturk.com/2012/bilim.teknoloji/teknoloji/03/29/redhackten.emniyete.buyuk.eylem/655156.0/index.html>
- [18] **MİLLİYET.** (2012, 04 21). *İçişleri 'bizi seviyor musun' diye 'hack'lendi* . Retrived 22 05, 2012, from MİLLİYET Web Site:
<http://siyaset.milliyet.com.tr/icisleri-bizi-seviyor-musun-diye-hack-lendi/siyaset/siyasetdetay/21.04.2012/1530889/default.htm>
- [19] **YAŞAR, E.** (2012, 04 08). *Anonymous'tan İngiltere Saldırısı*. Retrived 07 03, 2012, from SDN - ShiftDelete.Net:
<http://shiftdelete.net/anonymoustan-ingiltere-saldirisi-36232.html>

- [20] **Cumhuriyet News Portal.** (2012, 07 17). *ÖSYM'nin sitesi çökertildi.* Retrived 07 20, 2012, from Cumhuriyet Gazetesi: <http://www.cumhuriyet.com.tr/?hn=352600>
- [21] **The SecDev Group & Citizen Lab.** (2009). *Tracking GhostNet (Investigating a Cyber Espionage Network).* Ottawa-Canada: The Information Warfare Monitor.
- [22] **Centre of Excellence Defence Against Terrorism, Ankara, Turkey.** (2007). *Responses to Cyber Terrorism.* Ankara, Türkiye: IOS Press.
- [23] **Council of Europe.** (2007). *Cyberterrorism: the use of internet for terrorist purpose.* Strasbourg: Council of Europe Publishing.
- [24] **BBC.** (2012, 03 14). *Cyber-attack on BBC leads to suspicion of Iran's involvement.* Retrieved 04 05, 2012, from BBC News Web Site: <http://www.bbc.co.uk/news/technology-17365416>
- [25] **Verizonbusiness.** (2011). *2011 Data Breach Investigations Report.* Verizonbusiness.
- [26] **DENVER, N.** (2012). *Private: Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History.* Chicago: Chicago Review Press.
- [27] **USA-DHS.** (2004). *Personnel Security Guidelines.* Idaho, USA: USA Department of Homeland Security.
- [28] **MILLS, R. F., PETERSON, G. L., & GRIMAILA, M. R.** (2009). *Cyber Security and Global Information Assurance (Threat Analysis and Response Solutions).* (K. J.Knapp, Ed.) New York, USA: Information Science Reference.
- [29] **Techradar.** (2010, 09 30). *Botnets Explained.* Retrieved 04 05, 2012, from Tecradar Web Site: <http://pcplus.techradar.com/2010/09/30/botnets-explained/>
- [30] **Microsoft Safety & Security Center .** (2012). *How to better protect your PC with botnet protection and avoid malware.* Retrieved 04 05, 2012, from Microsoft Corporation Web Site: <http://www.microsoft.com/security/pc-security/botnet.aspx>

- [31] **Microsoft Research.** (2012). *An IP-Intelligence Framework*. Retrieved 07 10, 2012, from Microsoft Web site: <http://research.microsoft.com/en-us/projects/s-gps/ipintelligence.aspx>
- [32] **BRAVERMAN, M.** (2006). *MSRT Progress Made, Trends Observed*. Microsoft.
- [33] **SCHILLER, C. A., BINKLEY, J., HARLEY, D., EVRON, G., BRADLEY, T., WILLEMS, C., & CROSS, M.** (2007). *Botnets: the killer web app*. Burlington: Syngress.
- [34] **PcPlus Computer Magazine.** (2010, 09 30). *Botnets Explained*. Retrieved 07 02, 2012, from PCPlus: <http://pcplus.techradar.com/2010/09/30/botnets-explained/>
- [35] **Panda Security.** (2010). *Annual Report PandaLabs 2010*. Pandasecurity.
- [36] **FERGUSON, R.** (2012, 03 26). *Beginning of the end for ZeuS/SpyEye?* Retrieved 04 09, 2012, from TrendMicro Web site: <http://countermeasures.trendmicro.eu/beginning-of-the-end-for-zeusspyeye/>
- [37] **İnternetin büyüyen tehlikesi botnetler.** (2011, 05 06). Retrived 07 02, 2012, from Chip Online: http://www.chip.com.tr/makale/korkutan-botnet-gercekleri-mariposa-ve-conflicker-botnet-leri_26557_3.html
- [38] **Verisign.** (2012). *DDos Mitigation*. Verisign Inc.
- [39] **Kaspersky Lab.** (2011, 06 27). *Promotion of TDSS Botnet in US Costs Cybercriminals 250000 Dolars in Three Months*. Retrieved 07 01, 2012, from Kaspersky Lab: <http://www.kaspersky.com/news?id=207576367>
- [40] **BALTAZAR, J.** (2011). *MORE TRAFFIC, MORE MONEY*. Retrieved 07 03, 2012, from TrendMicro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_koobface-draws-more-blood.pdf
- [41] **Kaspersky Lab.** (2011, 03 11). *What is the value of your leaked data?* Retrieved 07 02, 2012, from Kaspersky Lab: http://www.kaspersky.com/about/news/virus/2011/What_is_the_value_of_your_leaked_data_

- [42] **MATHEWS, L.** (2011, 06 30). *TDL4 botnet: smarter, more sophisticated, and not for use in Russia*. Retrieved 07 03, 2012, from Extreme Tech: <http://www.extremetech.com/internet/88770-tdl4-botnet-smarter-more-sophisticated-and-not-for-use-in-russia>
- [43] **SCHILLER, J.** (2010). *Cyber Attacks & Protection: Civilization Depend on Internet & Email*. USA: Jon Schiller.
- [44] **Twitter.** (2010, 08 06). *Ongoing Denial of Service Attack*. Retrieved 04 05, 2012, from Twitter Web Site: <http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack>
- [45] **RAGHAVAN, S. V., & DAWSON, E.** (2011). *An Investigation Into the Detection and Mitigation of Denial of Service (DoS) Attacks*. New York: Springer.
- [46] **MOORE, T.** (2010). *Critical Infrastructure Protection IV*. Tulsa, OK, USA: Springer.
- [47] **CALDER, A., & WATKINS, S.** (2012). *It Governance: An International Guide to Data Security and Iso27001/Iso27002*. London, United Kingdom: Kogan Page Publishers.
- [48] **ERBSCHLOE, M.** (2005). *TROJANS, WORMS, AND SPYWARE A Computer Security Professional's Guide to Malicious Code*. Burlington, MA, USA: Elsevier Inc.
- [49] **DANYLIW, R., & HOUSEHOLDER, A.** (2012, 01 17). *CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL*. Retrieved 05 06, 2012, from CERT Web site: <http://www.cert.org/advisories/CA-2001-19.html>
- [50] **TrendMicro.** (2012). *Threat Report: W32.Tinba (Tinybanker) The Turkish Incident*. Retrieved 07 09, 2012, from TrendMicro web site: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf
- [51] **KNAPP, E. D.** (2011). *Industrial Network Security*. Waltham, MA, USA: Syngress.

- [52] **Symantec Security Response.** (2011, 10 24). *W32.Duqu: The Precursor to the Next Stuxnet*. Retrieved 07 03, 2012, from Symantec: http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet
- [53] **HALTAŞ, F.** (2011, 11 14). *Duqu: Yeni Nesil Keşif Uçağı*. Retrived 07 03, 2012, from Ulusal Bilgi Güvenliği Kapısı: <http://www.bilgiguvenligi.gov.tr/zararli-yazilimler/duqu-yeni-nesil-kesif-ucagi.html>
- [54] **FAUCON, B., & FASSIHI, F.** (2012, 04 23). *Iran Says Virus Has Hit Oil Sector*. Retrieved 04 24, 2012, from Wall Street Journal Web Site: <http://online.wsj.com/article/SB10001424052702303978104577361972375454022.html>
- [55] **GOSTEV, A.** (2012). *What is Flame?* Retrieved 07 12, 2012, from Kaspersky Lab Web Site: <http://www.kaspersky.com/flame>
- [56] **sKyWlper Analysis Team.** (2012). *sKyWlper (a.k.a. Flame a.k.a. Flamer) : A complex malware for targeted attacks*. Budapest: Laboratory of Cryptography and System Security (CrySyS Lab). Retrieved from <http://www.crysys.hu/skywiper/skywiper.pdf>
- [57] **GEERS, K.** (2011). *Strategic Cyber Security*. Tallinn, Estonia: CCD COE Publication.
- [58] **NAMESTNIKOV, Y.** (2012, 03 01). *Kaspersky Security Bulletin. Statistics 2011* Retrieved 25 05, 2012, from Security (Kaspersky Lab): http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
- [59] **DUVERGER, M.** (1990). *Metodoloji Açısından Sosyal Bilimlere Giriş*. (Ü. OSKAY, Dü.) Ankara: Bilgi Yay.
- [60] **BELL, J.** (2010). *Doing your research project 5th edition*. Berkshire, England: Open Universty Press.
- [61] **BAŞ, D., & AKTURAN, D.** (2008). *Nitel Araştırma Yöntemleri*. Ankara: Seçkin Yayıncılık.
- [62] **ÜSTDAL, P., & GÜLBAHAR, D.** (1997). *Bilimsel Araştırma Nasıl Yapılır Nasıl Yazılır*. İstanbul: Beta Basım Yayım Dağıtım.

- [63] **Çankaya University.** (n.d.). *Çankaya University Graduate School of Natural and Applied Sciences Thesis Manual*. Retrieved 08 15, 2012, from Çankaya University Web site:
http://fbe.cankaya.edu.tr/tr/yonetmelik/tez_klavuzu.pdf
- [64] **NATO.** (2012, 08 02). *NATO and cyber defence*. Retrieved 08 19, 2012, from North Atlantic Treaty Organization (NATO):
http://www.nato.int/cps/en/natolive/topics_78170.htm
- [65] **THEILER, D.** (2011). *New threats: the cyber-dimension*. Retrieved 08 15, 2012, from North Atlantic Treaty Organization (NATO):
<http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm>
- [66] **F-Secure.** (2007). *2007 Threat Summaries*. Retrieved 07 04, 2012, from F-Secure Web site:
http://www.f-secure.com/en/web/labs_global/2007/h1-threat-summary
- [67] **House of Lords** (European Union Committee). (2010). *Protecting Europe against large-scale cyber attacks (5th report of session 2009-10)*. London: Parliament of UK (European Union Committee).
- [68] **GILL, T. D., & DIETER, F.** (2010). *The Handbook of the International Law of Military Operations*. New York: Oxford University Press.
- [69] **NAZARIO, J.** (2007, 05 17). *Estonian DDoS Attacks – A summary to date*. Retrieved 07 04, 2012, from Arbor Sert (Security Engineering & Response Team): <http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>
- [70] **FELS, E., KREMER, J.-F., & KRONENB, K.** (2012). *Power in the 21st Century: International Security and International Political Economy in a Changing World*. New York: Springer.
- [71] **ANDRESS, J., & WINTERFELD, S.** (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA, USA: Syngress.
- [72] **GILES, J.** (2010, 12 16). *Are states unleashing the dogs of cyber war?* Retrieved 04 23, 2012, from New Scientist Web page:
<http://www.newscientist.com/article/mg20827915.100-are-states-unleashing-the-dogs-of-cyber-war.html>

- [73] **ASA, N.** (2012, 08 09). *Cyberattacks on Iran — Stuxnet and Flame*. Retrieved 08 21, 2012, from The New York Times Web site: Cyberattacks on Iran — Stuxnet and Flame
- [74] **SANGER, D.E.** (2012, 06 01). *Obama Order Sped Up Wave of Cyberattacks Against Iran* 06 13, 2012, from New York Times Web site: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all
- [75] **REGAN, B. G., & PUSATLI, Ö. T.** (2012). A Model to Assist the Maintenance vs. Replacement Decision in Information Systems. In Z. BELKHAMZA, & S. A. WAFA, *Measuring Organizational Information Systems Success: New Technologies and Practices* (pp. 137-157). IGI Global Snippet.
- [76] **SHEARER, J.** (2010, 09 17). *W32.Stuxnet*. Retrieved 07 13, 2012, from Symantec Web site: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
- [77] **EWING, P.** (2012, 03 22). *The cyber war after next*. Retrieved 04 05, 2012, from DoD Buzz Web site: <http://www.dodbuzz.com/2012/03/22/the-cyber-war-after-next/>
- [78] **LEWIS, T. G.** (2006). *Critical infrastructure protection in homeland security: defending a Networked Nation*. Hoboken, New Jersey: John Wiley & Sons Inc.
- [79] **THE EUROPEAN UNION.** (2006,12 12) The European Programme for Critical Infrastructure Protection (EPCIP). Retrived 12 05, 2012, from [Europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477](http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477)
- [80] **Information Security Association (Bilgi Güvenliği Derneği).** (2012). *National Cyber Security Strategy (Ulusal Siber Güvenlik Stratejisi)*. Ankara: Information Security Association.
- [81] **VURAL, Y., & SAĞIROĞLU, Ş.** (2008). Kurumsal Bilgi Guvenligi ve Standartlari Uzerine Bir Inceleme. *Gazi Universitesi Muh.Mim.Fak.Der.*, 23(2).
- [82] **MERKOW, M. S., & BREITHAUPT, J.** (2004). *Computer Security Assurance Using the Common Criteria*. Canada: Cengage Learning.

- [83] **STEWART, J. M., CHAPPLE, M., & TITTEL, E.** (2011). *CISSP: Certified Information Systems Security Professional Study Guide*. Sybex.
- [84] **Cabinet Office.** (2009, 06). *Cyber Security Strategy of the United Kingdom*. Retrieved 06 04, 2012, from www.cabinetoffice.gov.uk: <http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf>
- [85] **US-CERT** (part of the Department of Homeland Security). (2003, 02). *The National Strategy to Secure Cyberspace*. Retrieved 05 15, 2012, from US-CERT Web site: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
- [86] **The White House.** (2008, 01). *The Comprehensive National Cybersecurity Initiative*. Retrieved 06 04, 2012, from www.whitehouse.gov: <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>
- [87] **DUGAN, D.** (2012, 03 12). *DARPA Director Speaks of Offensive Capabilities in Cyber Security*. Retrieved 07 07, 2012, from Defense Advanced Research Projects Agency (DARPA) Web Site: <http://www.darpa.mil/NewsEvents/Releases/2012/03/12c.aspx>
- [88] **Federal Ministry of the Interior.** (2011, 02). *Cyber Security Strategy for Germany*. Retrieved 06 04, 2012, from www.cio.bund.de: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
- [89] **The French Network and Information Security Agency.** (2011, 02). *Information systems defence and security France's strategy*. Retrieved 06 04, 2012, from www.enisa.europa.eu: http://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf
- [90] **T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği, Türkiye Barolar Birliği cooperation.** (2012). *SİBER GÜVENLİK HUKUKU ÇALIŞTAYI-2012. Siber Güvenlik Hukuku Çalıştayı Sonuç Bildirgesi*. Ankara: www.iscturkey.org.
- [91] **SIOBHAN GORMAN, J. E.** (2011, 05 30). *Article: Cyber Combat: Act of War*. Retrieved 04 24, 2012, from Wall Street Journal Web Site: <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>

[92] **McAfee.** (2009). *Virtual Criminology Report 2009*. Santa Clara: McAfee Inc.

[93] **Ministry of Development.** (2012, 07). *Onuncu Kalkınma Planı (2014-2018) Özel İhtisas Komisyonları El Kitabı*. Retrived 08 01, 2012, from Kalkınma Bakanlığı Web Site: [http://www.xn--kalknma-ufb.gov.tr/DocObjects/View/14324/Onuncu_Kalk%C4%B1nma_Plan%C4%B1_%C3%96zel_%C4%B0htisas_Komisyonlar%C4%B1_El_Kitab%C4%B1.p](http://www.xn--kalknma-ufb.gov.tr/DocObjects/View/14324/Onuncu_Kalk%C4%B1nma_Plan%C4%B1_%C3%96zel_%C4%B0htisas_Komisyonlar%C4%B1_El_Kitab%C4%B1.pdf)
df

APPENDIX A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: AYDIN, Faruk

Nationality: Turkish (TC)

Date and Place of Birth: 12 October 1976, Van

Marital Status: Married

Phone: +90 505 622 04 76

Mail: farukaydin1@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
MS	Çankaya Univ. Information Technology	2012
BS	Anadolu Univ. Faculty of Business Administration	2006
TC	Uludağ Univ. JTC Computer Programming	1995

WORK EXPERIENCE

Year	Place	Enrollment
1996-Present	Turkish Air Forces	Officer

FOREIGN LANGUAGE

Intermediate English