BOSTON UNIVERSITY

METROPOLITAN COLLEGE

Thesis

DIGITAL DARK SIDE: CYBER WARFARE

by

OZGUR OZTURK

U02113904

Submitted in partial fulfillment of the requirements for the degree of

Master of Science in Administrative Studies 2014

Approved by

First Reader _____

Name of First Reader, PhD

Professor of .....

Second Reader _____

Name of Second Reader, PhD

Professor of .....

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

In modern world, computer systems and internet has become very crucial for individuals, businesses, and governments, and it has really huge advantages for all parties. The world has been becoming more and more interconnected via these information technologies that make our lives more comfortable and easier. On the other hand digital security concerns have increased very fast in the last decade especially for governments and societies. Because, the governments have critical infrastructures such as transportation, finance, energy, communications, and such which are computer controlled systems or web based services (e-government services like e-health) for public using. They have been spending billions of dollars to develop, setup and maintenance for these mandatory systems in every year. Moreover, these applications have processed and stored very critical and private information about their citizens. In addition, top secret information, related with military issues, scientific researches and politic/diplomatic issues may be shared via internet between government parties. All of these critical infrastructures are under attacked by the hacker groups, terrorist groups, intelligence services and other states. As a result, in today's world, war means not only physical bombing but also cyber attacking by using malicious codes, malwares and etc.

The cyber warfare is addressed in this study. The thesis will concentrate on the international cyber attacks which are organized by the governments, terrorist groups and hacker groups. In the paper, the basics of the cyber security framework will be explained at first. Some basic definitions of cyber attack types will also be mentioned in the second chapter. Then different types of cyber attacks which are categorized according to the objective and the level of harmful effects will be evaluated in the third chapter. Some examples of international cyber attacks like Stuxnet will also be mentioned in this chapter. Finally, the national and international efforts

fighting against cyber threats will be explained in the fourth chapter. This study will try to analyze the situation in some states such as US and Turkey, and the efforts made for handling this issue by international organizations such as United Nations (UN) and NATO.

CHAPTER 2: TYPES OF CYBER THREATS

In today's world, cyber attacks are becoming more serious problems for both organizations and individuals. Attackers use different types of cyber threats which are identified in seven basic types as shown in the figure, in order to infiltrate and attack to information systems.

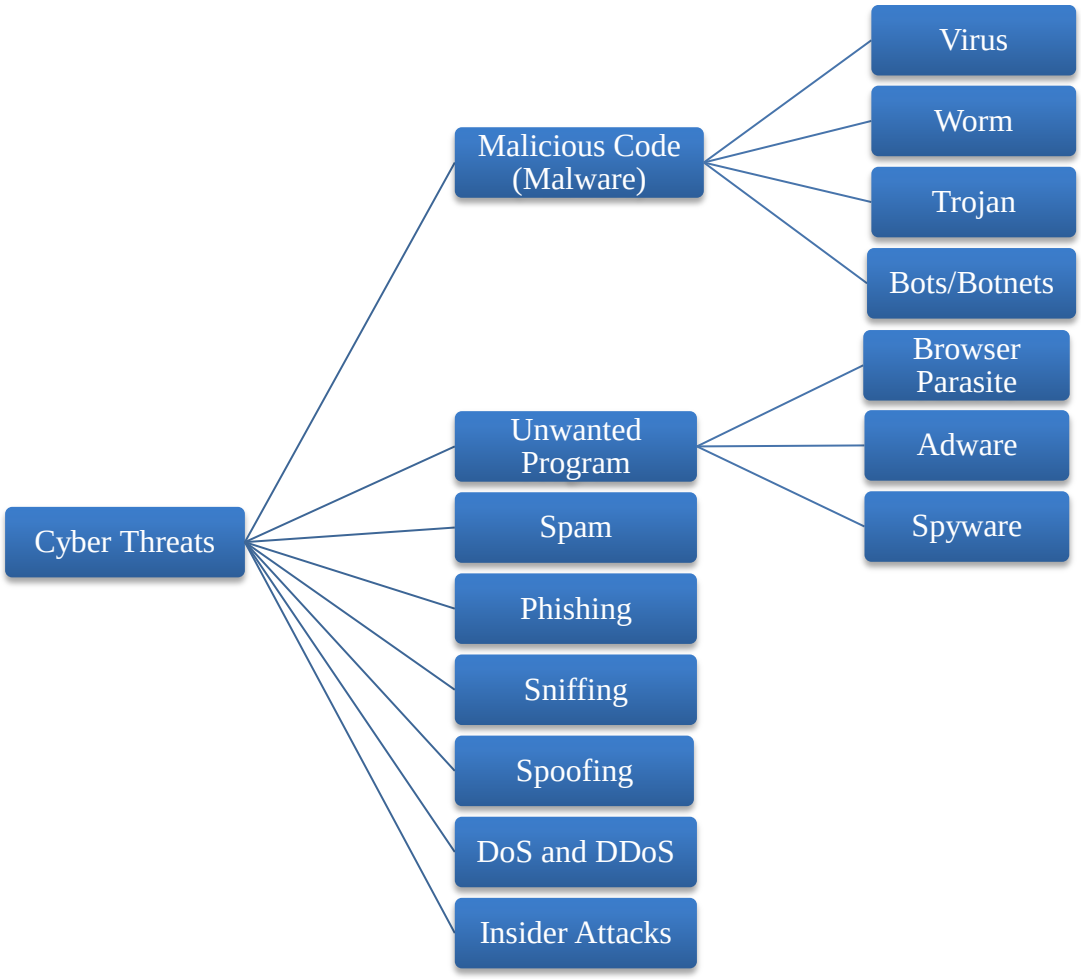


Figure 2.1. Types of Cyber Threats

2.1. Malware:

Malware is the common name of malicious codes such as viruses, worms, and Trojans. These types of malicious codes first infect a computer in a network and then spread out from infected

computer to the other computers in the network. They are designed for causing damages on computer systems and networks, and/or effecting their operations in negative.

2.1.1. Viruses:

Viruses are the programs that attach themselves to the computers by using other programs, files, e-mail attachments and etc. They cannot activate themselves; they need user actions such as clicking a link, opening an attachment or file, or executing a program to be activated. Once they are activated, they can replicate themselves and spread out to other files and computers. Viruses can cause serious damages on computers and systems such as damaging hardware, destroying files, reformatting the computers, or causing the programs to run improperly (Laudon & Traver, 2009). The first known computer virus was a kind of boot sector virus called *Brain* which was programmed against IBM computers in 1986 (Ogun & Kaya, 2013).

There are four main types of viruses: *Boot Sector viruses, Macro viruses, File-infecting viruses, and Script viruses*.

- *Boot sector viruses:* Boot sector is the first sector of a disk and it stores information about how a computer can use the disk. *Boot Sector viruses* on the other hand infect the boot sector of a disk and spread itself to the other hard and removable disks. These viruses cause damages on the disks and run them improperly (Weems, 1998). *Chernobyl* is an example of boot sector virus and more than one million computers were infected by this virus in 1999. It is one of the most harmful viruses ever written which caused more than $250 million in damages (Symantec Security Response).

- *Macro viruses:* Micro viruses are written for the specific applications such as Word, Excel, PowerPoint, or Acrobat Reader. They affect only that specific type of applications

and when the user opens the infected file, macro virus is activated. Then it replicates itself to the other documents on the same application (Laudon & Traver, 2009).

- *File-infecting viruses:* Like micro viruses, these are written for the other specific file types which are executable such as *.exe, *.dll, *.com, and *.drv. After they are activated by executing these files, then virus may replicate itself to the other executable files. These types of viruses can cause damage on files by changing the program codes with their own, or the worse they can destroy the file. Because of this reason they are more dangerous than micro viruses.

- *Script viruses:* Script viruses are another types of viruses developed for script files such as Java Script files (*.js) and Visual Basic Script files (*.vb).

2.1.2. Worms:

Worms are also computer program codes that can infect computers and spread across the network by replicating its own. Unlike viruses they do not need other files to reach other computer, or they do not need to be activated by user actions in order to infect other computers in the network. They can send their copies to other computers via the network communication channels. Then worms can replicate themselves on that computer very fast by using the memory and other system resources. In addition they use network resources such as bandwidth in order to infect other computers. Once a computer is infected then it typically runs much slower than before. Moreover, attackers can take the control of computers by using worms (Canbek & Sagiroglu, 2007).

Modern worms are more complex codes and they have the ability to spread via the network very fast by using more than one method. Moreover these malicious codes are able to bypass security

tools; therefore they cannot be analyzed and/or detected easily. In 2004, one of the fastest spread worms called *MyDoom* infected computers, slowed their internet connection about 10%, and increased the page load times about 50%. This worm caused damage around $38.5 billion. In 2001, another worm called *Code Red* infected 359,000 servers within 14 hours and exploited the Microsoft's Internet Information Server. In this case, estimated damage was $2.6 billion (Fosnock).

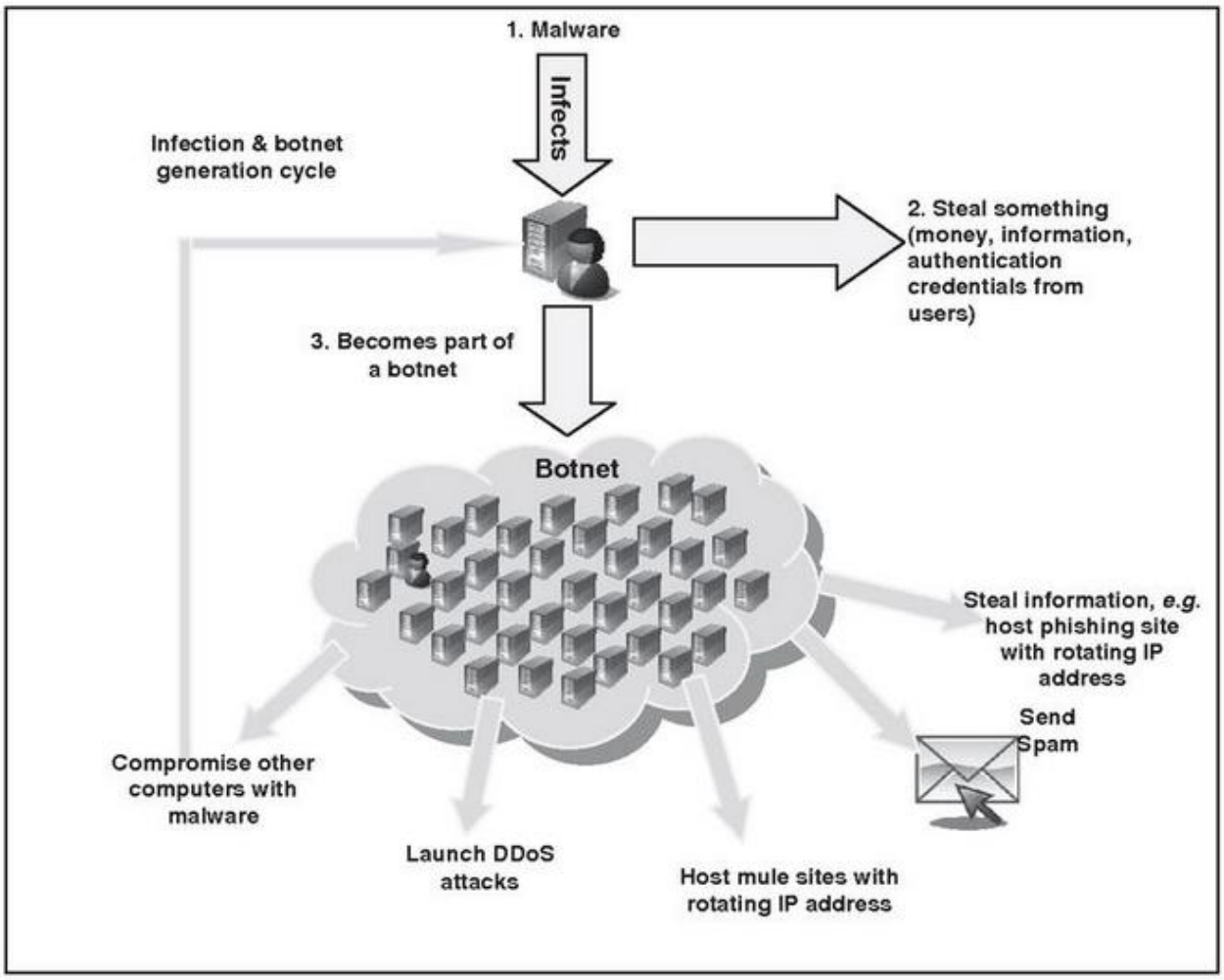
2.1.3. Trojans:

In general, Trojans introduce themselves as good and beneficial programs to the users and they generally bundle with an application which is downloaded from the internet, in order to hide their ectivities. Since a Trojan does neither replicate itself and nor infect other files and computers, these types of malwares are a bit different threats from viruses, and worms. After a Trojan settle in a computer it uses security vulnerabilities of the host and it starts running as a malicious activity. This type of malwares may cause wide range of damages but they are most widely used for information and/or password stealing from the host computer and sending them to the attackers (Kim et al., 2010).

In 2007, a Trojan called *Infostealer.Monsters* suffered computers and web sites, and stole the information in those computers. One of the most affected web sites was the Monster.com that is a very popular and well known job seeking web portal. Only from this portal more than 1.6 million job seekers' personal information such as names, addresses, phone numbers, and e-mail addresses were stolen by this Trojan (Laudon & Traver, 2009).

2.1.4. Bots and Botnets:

Bots (short for robots) are the computers that are infected by cyber threats in order to create unauthorized access for taking the control of the host by the attackers. They are also named *Zombie* computers. Once the computer connects to the internet, attackers first find out the vulnerability and then attack by using malicious codes such as viruses, worms, and Trojans. Since these attacks are invisible, mostly users cannot realize that their computer is under attack. Therefore attackers take the control of the computers and use them for their illegal activities such as stealing private information, spamming to other computers, and organizing the denial of service (DoS) or distributed denial of service (DDos) attacks. Typically attackers capture more than one computer (mostly hundreds of computers) via this method and this collection of bots is named as *botnet*.



Source: OECD, 2009b

Figure 2.2. The Botnet Lifecycle

The first known "bot" was *Eggdrop* that targeted IRC[1] in 1993. But it was not published for a malicious activity; the main purpose behind the "Eggdrop" was to control interactions in IRC chat rooms. On the other hand, in the course of time they were evolved as cyber weapons by the attackers. When we came to the 2011, *TDL-4* infected more than 4.5 million computers according to the reports, as one of the most sophisticated threats. Security researchers have identified it as virtually indestructible (Silva et al., 2012).

[1] Internet Relay Chat (IRC) is a text-based chat-system that organizes communication in channels.

“Botnets” are one of the most dangerous cyber attacks which are used by both individual attackers and organized criminals. Because of this reason, users, organizations, and governments should be aware of them and protect themselves and their computers/systems against these types of attacks that pursue such serious crimes.

2.2. Unwanted Programs:

In addition to malware, computers are also targeted by unwanted programs such as browser parasite, adware, and spyware. These programs install themselves on a computer without the user’s consent. They are generally used for advertising, gathering and analyzing user’s internet traffic, and stealing information.

2.2.1. Browser Parasites:

These are unsolicited commercial software/programs which are mostly developed for making some changes on the browser settings such as changing the home page, and/or changing the search settings. In addition to this, sometimes they are used for gathering information about the visited web pages and sending them to the attacker. Browser parasites are often created as the components of adware programs; for instance *Websearch* is an adware component that changes search settings and default home page of Internet Explorer (Laudon & Traver, 2009). Furthermore detecting and removing this type of unwanted programs from a computer by using anti-virus software can be very difficult.

2.2.2. Adware:

These programs are using for the advertising activities and once they are installed they automatically open the pop-up advertisements when the web browser opens or when certain web

sites are visited. The new versions of these programs are now placed the advertisements on the unused areas of the already opened web pages. An adware can install itself when the user visits an infected web site, or clicking a link on e-mail messages or instant messages. On the other hand, some adware programs have the ability to collect the users' activities (such as most visited web sites, likes and dislikes, shopping habits, and searching behaviors) in internet by using the browser data and send them to the advertisement companies. Like *web parasites*, adware programs are annoying but at least these are not as dangerous as spyware programs or malware programs (Gordon, 2005).

2.2.3. Spyware:

There are some common characteristics of a spyware (Awad & Fitzgerald, 2005) (Aycock, 2011);

- Stealing files and information
- Recording webcams and instant messages, and capturing images
- Changing browser settings, tracking user's behaviors and browser activities, and recording internet traffic information
- Logging keystrokes, and mouse clicks
- Slowing the computers

These unwanted programs are generally bundled with other useful programs and beyond this, users mostly are not aware of a spyware that is already installed. Once a spyware is installed then it is very difficult to uninstall the program on the computer. These programs are seriously dangerous because they can steal user's most critical information such as license keys, passwords, online banking accounts, and online payment information. Cookies, Web bugs, browser hijackers, key loggers, and tarcks/spybots are the main sub categories of the spyware

programs. Some spyware programs are listed and evaluated in the table according to their characteristics (Awad & Fitzgerald, 2005).

Table 2.1. Characteristics Analysis of Some Spyware Programs

Spyware	Advertising	Settings	Slowing	Inconspicuous	Bundled	Uninstall?
Comet Cursor	–	✓	✓	✓	✓	–
Escorcher	✓	–	–	✓	–	✓
Inspexep	✓	✓	–	✓	–	–
SongSpy	✓	–	–	✓	–	✓
Webhancer	–	–	✓	✓	✓	✓

Source: Awad & Fitzgerald, 2005.

2.3. Spam:

Spam messages are mostly used in e-mail services but on the other hand other electronic communication channels/services such as SMS, MMS, instant messaging, search engines, blogs, and VoIP are also suffered by the spam messages. Although there is no widely agreed definition of spam, OECD defines some characteristics of spam messages. According to OECD, spam messages are primarily electronic messages and they are sent for commercial activities. In addition, these are unsolicited messages and they are sent in bulk (Schryen, 2007).

Table 2.2. Characteristics of Spam Messages

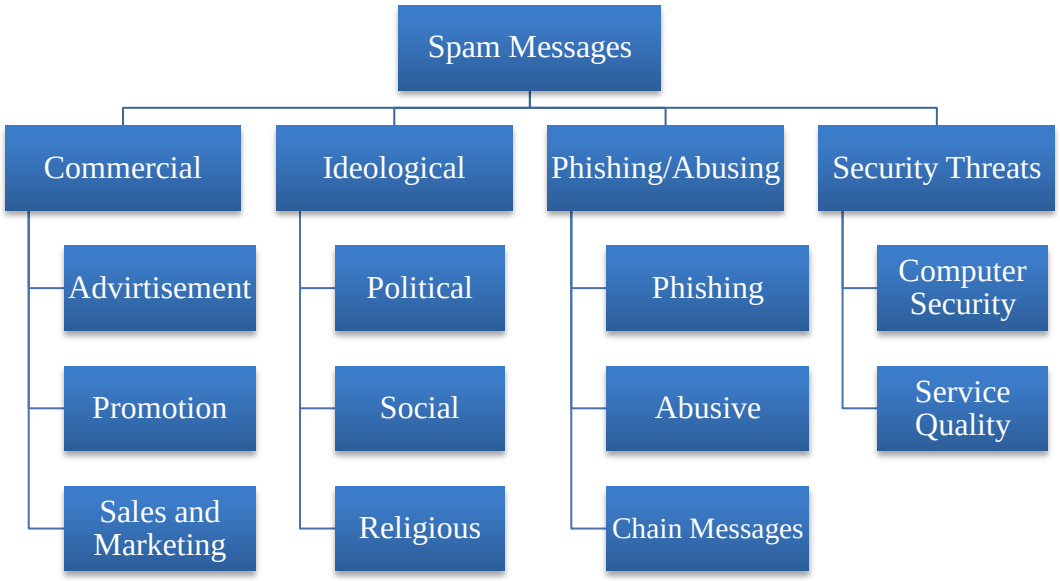
Primary Characteristics	Secondary Characteristics
Electronic message	Use addresses collected without prior consent or knowledge
Sent in bulk	Unwanted
Unsolicited	Repetitive
Commercial	Untargeted and indiscriminate
	Unstoppable
	Anonymous and/or disguised
	Illegal or offensive content
	Deceptive or fraudulent content

Source: Schryen, 2007.

Spam messages are created based on four different main purposes;

- *Commercial:* These messages are just used for advertising, promotion, and/or marketing of a product, service, or a web site. These are not really dangerous but still annoying for the users.
- *Ideological:* These types of spam messages are sent for propagating a political or religious idea.
- *Phishing and Abusing:* This is the more dangerous and criminal related spam messages category since the attackers try to steal user's personal information such as password and username by using phishing methods. Moreover, attackers try to capitalize by selling fake products, or abusing user's feelings by using untrue and dramatic stories and collecting money for helping non-existent desperate people.
- *Security Threats:* These are other dangerous types of spam messages because of their illegal intents. Mostly these spam messages includes malware programs as an attachment

file or a web page link. When user downloads and opens the attachment, or clicks to the link then malware installs itself on the computer and starts its malicious activity.



Source: Ozturk, 2009.

Figure 2.3. Spam Message Categories

2.4. Phishing:

Phishing is a deceptive activity in order to obtain users' confidential information such as social security numbers, and login names and passwords which are used for accessing to financial accounts like bank accounts, mortgage accounts, credit card accounts and etc.

E-mail services, SMS services (called SMiShing), and Voice over Internet Protocol (VoIP) services (called Vishing) are the most frequently used electronic communication channels for Phishing activities. In these types of attacks, third parties (phishers) are pretending as financial institutions or as government agencies so as to deceive the people (OECD, 2009a).

- *E-mail Phishing*: Phishers provide a link in e-mail messages to make the users access to the fake web page. These messages inform the users to go to the web site by using the link

and to fill the form which is placed on the that web page. These web pages are the fake copies of financial institutions' web pages and the phishers collect the confidential information when the user enters them on the form.

- *SMiShing:* This is the second types of phishing methods which uses text messages and mobile phones to reach the people. Similarly, this SMS directs the user to the fake web site and requests them to sign up their account, thus phishers can collect the confidential information.

- *Vishing:* On the other hand, Vishing is a bit different from former types of phishing methods since it uses the phones to steal the information. In this case, phishers send spoofed e-mails which are subjected about making a phone call for some reasons. When the victim calls the fake telephone number then the automated attendant welcomes and requests dialing personal information such as account number, password, social security number and etc.

After collecting confidential information, the phishers use them to steal the money for financial gain, and/or to steal the identity for selling them to the other parties. Especially in recent years, phishing is the most widely used cyber threat and cause much serious financial damages on individuals and societies. Although the certain amount is not known, the estimated financial loss because of the phishing is billions of dollars per year. According to Anti-Phishing Working Group (APWG), the total number of phishing attacks was 30,000 for the first quarter of 2010. This means users come up against approximately 0.7 phishing attacks per minute (Gupta & Pieprzyk, 2011).

2.5. Sniffing:

Sniffing is an eavesdropping activity on computer networks in order to capture the information which is travelling over the network equipments such as routers and etc. By using sniffing, attackers can analyze IP data packets on the network and then extract the information such as e-mail messages, confidential files and reports which are carried. Actually, sniffing can be very helpful to identify the network security vulnerabilities and then to fix them or secure them when a security professional uses this method. On the contrary, it can cause serious damages on computer systems and/or may finalize with publicity of confidential information (Baylor University, 2013).

For different operating systems there are different free packet analyzers (sniffers) which can be downloaded from internet such as *Wireshark* for Windows, and Linux, and *Snoop* for Solaris (IBM, 2013).

To avoid or to prevent sniffing attacks, using data encryption, and setting the connections via secure communication channels and protocol is one of the most beneficial methods although it is not totally sufficient alone (de Vivo et al. 1997).

2.6. Spoofing:

Spoofing is used by the attackers for the purpose of hiding their real identity.

- *IP Spoofing:* Spoofing mostly occurs as *IP Spoofing* on internet which means that attackers show or introduce themselves with the fake IP addresses while they are attacking to a computer or system in order to hide their real IP address. In addition, sometimes hackers use IP spoofing to surpass authentication mechanism by introducing

themselves as a trusted or authenticated source of IP addresses. Once they infiltrate then they begin malicious activities (Harris & Hunt, 1999).

- *DNS Spoofing:* According to the internet standards in order to connect to a website, the host computer should resolve the IP address of the domain name that the user wants to connect. Therefore, a host computer should request the equivalent IP address of the actual domain name from the DNS name server. At this point, if the hackers infiltrate to the DNS name server then the host computer can be redirected to an illegitimate server by the hackers through sending this illegitimate server's IP address to the host. This type of spoofing attacks is called DNS spoofing (de Vivo et al., 1997).

2.7. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:

DoS and DDoS attacks are highly popular in recent years among the hackers. DoS attacks are used for reducing the information systems service quality and making the servers/systems out of service for a limited time period. Hackers generally send large numbers of packets (requests) to the servers at the same time in order to increase the server's response time or totally make it shut down (Chinh et al., 2013), (Gasti et al., 2013).

On the other hand, DDoS is more complicated than DoS attack since it is an organized attack. In DoS attacks, hundreds or thousands of client computers which are infected and controlled by the master (attacker) computer, are turned into zombie computers in a botnet. After this, master lunches the DDoS attack by commanding the zombies to send service requests to the victim system/server in order to create excessive traffic on the server. Then at the end victim system becomes out of service and remains like that throughout the DDoS attack (Tickle et al., 2011).

Although DoS and DDoS are continued for a limited time and don't cause information loss on systems, still they may result in serious effects. As an example, if critical systems such as online banking systems, online payment systems, and e-government services are exposed by a DoS or DDoS attack and if the system cannot provide the service for a long time then the financial loss of companies/organizations, bad reputation on brand names/services, and negative effects on societies may goes into more serious situations (Laudon & Traver, 2009).

2.8. Insider Attacks:

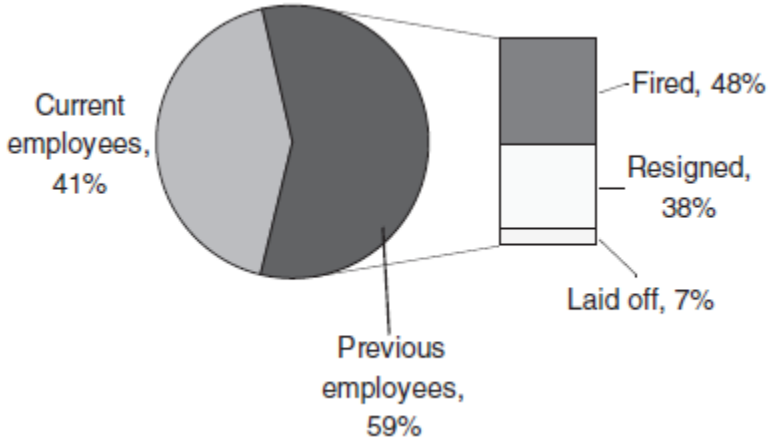
People mostly think that cyber threats/attacks come from outside the organization. But researches and statistics show the opposite of this idea. According to Lynch (2006) 60-70% of total cyber threats organized by the insider attackers. Likewise, according to Laudon & Traver (2009) 70% of the total identity theft has done by the insiders. These researches show that authorized users can find the system security vulnerabilities easier than the outsiders. In addition, they may have the permission to access the system and data, and they may have knowledge about how they can clean their tracks (logs) from the system in order to remain invisible. As a result, an insider can easily and quickly organize an attack to the system, steal the data, and delete access records with making very little effort.

According to Bellovin & Pfleeger (2008), there are some different reflections behind these insider attacks;

- Trying to do something unauthorized without knowing that the action is not authorized.
- Checking the system vulnerabilities or problems, and reporting them at the end.
- Testing the authorized access limits and checking system vulnerabilities or problems without an intention of reporting them.

- Just killing time by viewing data.
- For revenge (especially done by former employees who are fired) or just for fame.

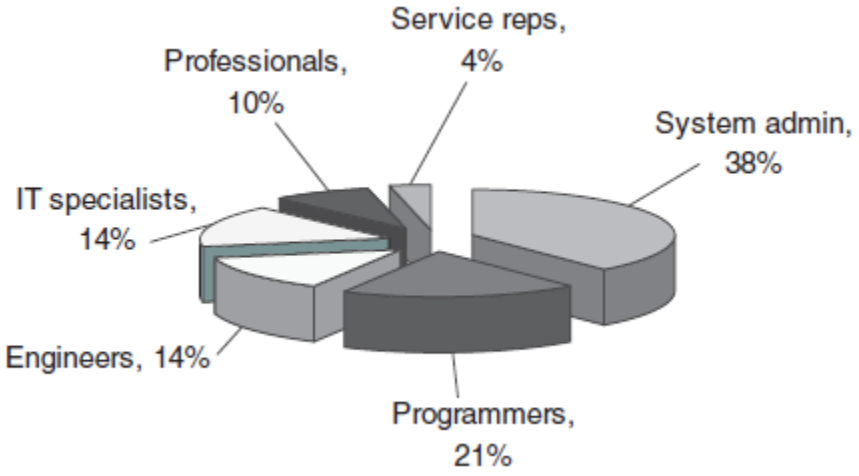
Beyond these reflections, some statistical data shows that 41% of insider attackers are current employees while 59% are former employees who are fired (48%), resigned (38%), or laid off (7%).



Source: Lynch, 2006.

Figure 2.4. Breakdown of Insiders

On the other hand, current employees as insider attackers are almost all IT professionals with 87% in sum, and only 10% of them are professionals and 4% of service reps. Expectedly, since they have more access authorization to the system than the other groups, and also they have expertise on security vulnerabilities, system administrators are the biggest insider attacker group with 38%. Likewise, programmers are the second largest group (21%) probably they may know the software vulnerabilities very well since they involve coding activities, and/or they may add backdoors to the software applications in order to access the data.



Source: Lynch, 2006.

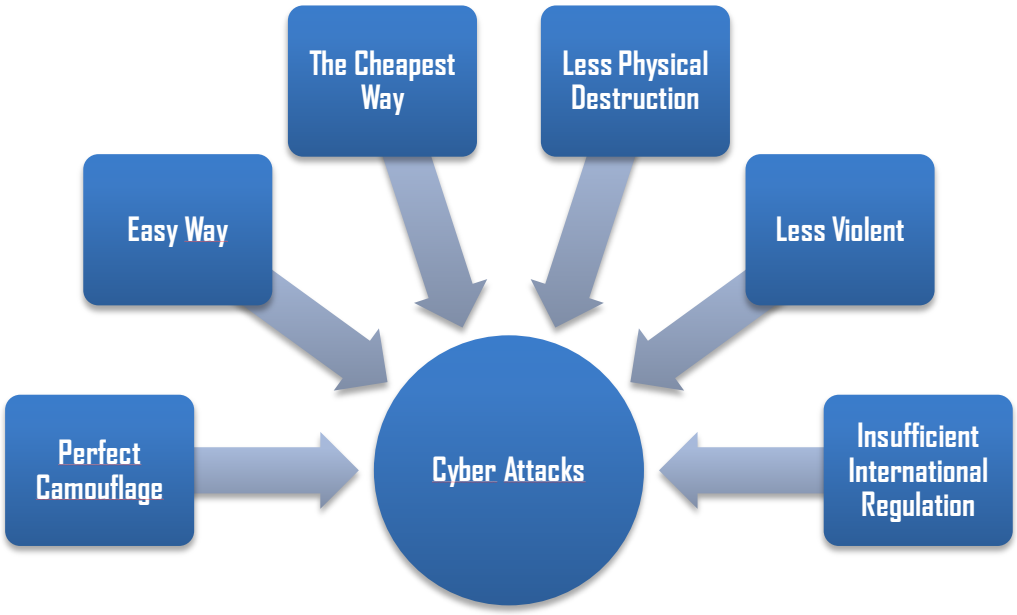
Figure 2.5. Breakdown of Current Employees as Insiders

Insider attacks may cause serious damages like financial loss and publicity of confidential data. As an example, in 2005 an insider stole data such as employees' time and travel expenses, security audits, and encryption software from a data broker company called *Acxiom Corp.* This data theft cost about $5.8 million for the company. In another example, *Card Systems Solutions Inc.* declared that 40 million credit card numbers may had stolen as a result of security incident and unauthorized access (Lynch, 2006).

CHAPTER 3: DIFFERENT ASPECTS OF CYBER WARFARE

3.1. Why Cyber Warfare

Now, with cyber warfare, we have another means of launching attacks in the world, this time with only a keyboard. But why these types of attacks are highly popular in international level? Why the states, terrorist groups, and hacker groups are using cyber warfare for attacking? In reality, cyber space offers huge advantages for attackers and that is why the cyber warfare is getting more and more serious problem in international level.



Figue 3.1. Advantages of Cyber Attacks for Hackers

3.1.1. Perfect Camouflage

In cyberspace, attackers can easily hide their identity and cover their tracks. They generally take the control of other computers around the world by using malicious codes (virus, worm and etc.) and then attack to the target via these zombie computers.

3.1.2. Easy to Find the Software Vulnerabilities

Security issues were not considered as important as other issues such as functionality, availability and ease of use in software development industry until recently. Since the software systems are not secure enough, attackers can easily find the vulnerability of software systems in order to attack. In addition, there are so many scanning security tools are available on the internet and many of them can be downloaded as free for scanning and finding the vulnerability of a system. Finally and obviously it is much easier than producing a nuclear weapon or a rocket which require so many years in order to develop and, very special and advanced expertise.

3.1.3. The Cheapest Way

Cyber warfare is the cheapest way to attack someone. There is no really cost to develop malicious codes, malwares or other types of threats (Farwell, & Rohozinski, 2011). The only necessary steps are finding the vulnerability of the target system, developing the software program (virus, Trojan horse and etc.) and finally spread the digital weapon to the target system. Unlike in physical weapons, attackers do not have to spend billions of dollars to develop the digital weapons.

3.1.4. Less Physical Destruction

Attackers might simply shut off national defense system of a country, explode railways or make the telecommunications systems out of service not by using a missile, rocket or physical bomb but by activating a logic bomb. This means that cyber warfare is less disruptive and it causes less physical destruction (Clark, 2009). Although it causes less physical destruction, it may cause much serious harmful effects on critical IT based services which are required billions of dollars to recover.

3.1.5. Less Violent

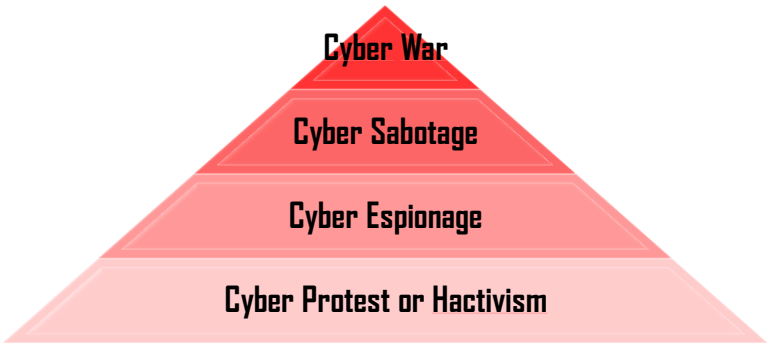
Cyber warfare has never ended up with the kind of death as nuclear or other physical weapons caused. Thus, people categorize these types of attacks less serious and almost innocent. On the other hand, we cannot be sure about that because we have never seen the serious two sided cyber war and its effects yet.

3.1.6. Insufficient International Law and Regulation:

Although some countries and international organizations have intended to do something about cyber warfare, yet there is no sufficient international rule or law to handle the issue. Furthermore, there is no consensus on the definition of the cyber attack, cyber war, cyber espionage and cyber warfare. It is not clear that what kinds of rights have the victims and how they can react against to the attackers in a legal frame.

3.2. Different Motivations of Cyber Attacks

Attackers are using different types of cyber attacks for different motivations. Some of these motivations are less dangerous and they have short term effects on victim systems while others are more dangerous and they may cause more serious damages.



Figue 3.2. Motivations Behind the Cyber Attacks

3.2.1. Cyber Protest or Hactivism

This is the most common and least harmful types of attacks. They are generally managed by the international hacker groups who are organized around a social or political view such as anonymous. They try to receive sensational attention and make the public aware of an actual international issue. This aims modification or destruction of content such as the hacking of websites, or make the victim systems out of service for a while by DoS and DDoS attacks (Cavelty). Such actions are carried on between a couple of hours and a few days, and their effects are temporary. At the end of the attack, the only damage for the victims is suffering their image.

3.2.2. Cyber Espionage

It is a long term activity that attackers try to collect relevant data. They are using back doors, malware and spyware programs, rootkits, Trojan horses and etc. In contrast to cyber protest, attackers try to hide their activities from the victims. Even though attackers don't destroy the data, the collection of relevant data can be very harmful for the victims who may be private companies or government parties. Such actions are mostly attempted for stealing a new private technology, collecting other nation's secret information, or tracking the terrorist groups' actions.

3.2.3. Cyber Sabotage

Consists of unlawful attacks against computers, networks, nations' critical infrastructures (transportation, finance, energy and communications) and the information they store. Since attackers try to destroy the computer systems and their data this is more violent and more harmful than cyber espionage (Cavelty).

3.2.4. Cyberwar

Except the cyber war, cyber attacks are all one sided attacks and the attackers try to cause the damage on victims systems or property. In other words, the victims are in passive and defense mode. On the contrary, there are two sides in a war and in general they publicly declare their objectives and their targets on the other side (the enemy). In addition, a war consists of series attacks managed by each of both sides but not only one time action. Thus we have not seen the cyber war yet we cannot clearly identify it. Although there is no commonly accepted definition of a cyber war, *obviously it refers to the use cyber attacks to disrupt or to destroy the activities of another country, especially deliberate attacks on communication systems* (Cavelty). Finally it is clear that these are the most dangerous and most harmful cyber attacks.

3.3. Most Known International Cyber Attacks

Especially in the last decade nations and private sectors have tried to struggle with dramatically increasing cyber attacks. The most known cyber attacks will be mentioned in this part of this study. Although there was no clear evidence about who were the attackers, international security experts believe that almost all of those attacks were managed by the states. But none of the governments has officially accepted the cyber attack was originated by their country.

3.3.1. Anonymous vs. Israel (Cyber Protest)

In 2012, Israel government stated that 44 million cyber attacks were made by the Anonymous to the government's websites, after the military operation of Israel to Palestinian (Sutter, 2012). Dozens of government websites, even Israeli Ministry of Defense website, were affected from this attack and these remained out of service for a while according to Anonymous (RT Network).

Anonymous group organized this DDoS attack in order to take world's attention to the military operation.

3.3.2. Operation Aurora: China vs. U.S. Technology Companies (Cyber Espionage)

Operation Aurora was one of the most known international cyber espionage activities, targeted the private sector, in the history. In 2009, Google and some other U.S. major technology companies such as Yahoo, Cisco, Juniper, and Adobe announced that they were attacked by the Chinese hackers (Clark, 2011). They also claimed that hackers stole their proprietary information through by using a malware. Hackers were able to copy the source codes of new projects and designs of new products from Google and other companies. According to Grover, it was a well organized Chinese attack and as an example a stolen source code from Google might be used for the Baidu that is Chinese search engine.

3.3.3. Russia vs. Estonia (Cyber Sabotage)

Estonia is a small but the one of the leader countries on developing and using e-government or internet based services. At the same time this leadership Estonia made it as a web-dependent country, with widespread internet access, digital identity cards, 80% usage rate for online banking, electronic tax collection, and remote medical monitoring. In April 2007, the DDoS attacks was started by the Russian hackers first affected the foreign minister's web site, but spread to all government institutions and key businesses, such as banks (Harris). According to the Harris this attack might be organized by the Russian government because it was started several weeks later than a political conflict between Estonia and the Russia.

This is the first cyber attack that affects a whole country in the history and this case is the best example of how negative a cyber attack can affect the countries and people's lives. During this

DDoS attacks Estonia requested the help and assistance of the NATO and this case turned into an international issue.

3.3.4. Stuxnet: U.S. & Israel vs. Iran (Cyber Sabotage)

In fall 2010 a worm called Stuxnet infects Windows computers. The US and Israel together had developed malware, a highly sophisticated computer worm that would damage the nuclear plants in Iran (Natanz plant in particular) (Broad et al., 2011). The idea of the computer worm was to speed up the rotating centrifuges to a level that they would be damaged enmass so that the Iranian nuclear enrichment program will be delayed\sabotaged by years. The computer worm was to be deployed through thumb drives (not internet) and was to find the Siemens chips that controlled the centrifuges. These are small embedded industrial control systems that run all sorts of automated processes: on factory floors, in chemical plants, in oil refineries, at pipelines—and, in **nuclear power plants**. These chips are often controlled by computers, and Stuxnet looks for Siemens chips controller software. The attack would be invisible to the operators and the worm was designed to rest in the system and continuously sabotages the Iranian facility. This was a covert operation for sabotage. However, the Stuxnet worm was discovered when it got outside of the Natanz realm (unauthorized usage by operators of internal resources on personal computers) (Falliere et al., 2011).

The important aspect of this episode is that it has legitimized state sponsored cyber attacks. The notion of malware has been whitewashed by this type of uses, thus giving credence to such activities at all levels of attacks, personal, industrial and political. Then finally we all have to ask a question:

CHAPTER 4: NATIONAL AND INTERNATIONAL EFFORTS

4.1. National Efforts

Cyber power is getting more and more important and complicated for every state in order to create a secure environment for their citizens. Therefore governments have realized that they have to support their physical army based power with the cyber power which is the composition of a state's cyber defense and cyber offense capabilities. Especially the US, Russia, China, Israel, and North Korea are the most active states in cyber space regarding both the defense and offense, and we know that these countries sometimes get involve in cyber offense activities against other states. One another well known reality is that some of these countries such as China, and Russia have performed projects to create cyber armies. On the other hand, other less developed or developing countries are still dealing to create the cyber security policy, strategy and action plans. Although they have limited capability, they are trying to improve their national cyber security.

In this section, the US as one of the most sophisticated and equipped country, and Turkey as one of the developing country who tries to improve its limited capability on cyber defense will be examined more comprehensively.

4.1.1. The United States (US) - National Cyber Defense Approach:

As one of the most exposed countries US deals with cyber threats so seriously and especially in the last decade the country have addressed national cyber defense issues. At the beginning of the last decade national cyber defense strategy plans against cyber threats was developed based on the passive defense issues but in recent years active defense and offensive methods (such as tracing the incoming cyber attacks, finding and deactivating its source) have adopted to the plan.

With the leadership of White House, the responsible government parties have taken some very critical and important steps in order to establish a national coordination - includes the government agencies, and both the public and private sectors - on fighting against cyber threats.

4.1.1.1. Policy Documents:

The US National Cyber Security Strategy: The strategy document was announced under the name of *The National Strategy to Secure Cyberspace* in February 2003. This document takes attention to dramatic increase of cyber threats, potential destruction of those threats on critical infrastructures, and necessity of the cooperation between the government agencies, private sector, and citizens on fighting against those threats. The main objective of the document was declared as creating *"a framework for protecting this infrastructure that is essential to our economy, security, and way of life"*. Right after the announcement of this document the federal government agencies and the private sector initiatives started to the first cooperation in order to take actions for protecting the national critical infrastructures, vulnerable sectors, and large pants (Even & Siman-Tov, 2012).

International Strategy for Cyberspace: The US government issued the international strategy document in May 2011. Besides the national cyber defense, in this document the US emphasizes the importance of global security, creating partnerships with other nations, and global information sharing. Because of global nature of the internet and interconnectivity, the US points out those national efforts are not sufficient with alone in order to create a secure networks and/or infrastructures. Therefore, the federal government declares its international cooperation intent to create secure networks for the US and its Allies. Based on this strategy document the US have made partnerships with other nations and international organizations such as NATO, in order to

share information and expertise on economic, social, political, and security issues (Even & Siman-Tov, 2012).

4.1.1.2. The US Federal Organizations:

The National Cyber Security Division (NCSD): NCSD was created within the Department of Homeland with the duty of implementing the cyberspace strategy. NSCD is working with public, private, and international entities to secure the cyberspace. In this context, this division is conducting National Cyberspace Response System that creates the acting procedures and protocols, and leads the coordination of parties in the case of detecting suspicious cyberspace activities. In addition, NSCD manages and operates the Cyber-Risk Management Program that was developed for figuring out cyber security related risks, and reducing them.

The US Army Cyber Command (ARCYBER): ARCYBER was established within the Pentagon in 2010, is responsible for cyber offence and cyber defense activities in the military. ARCYBER identified its duties as "planning, coordinating, integrates, synchronizing, and conducting activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries" (ARCYBER, 2014).

The US Intelligence Agencies: In the US, the most active organizations on both offensive and defensive cyber security activities are the intelligence agencies such as the FBI, and the NSA. These agencies issued a strategy document in August 2009 and according to this document developing and improving the capability of managing cyber security related activities (offensive

and defensive) is the most important task for the intelligence agencies in the US (Even & Siman-Tov, 2012).

4.1.2. TURKEY - National Cyber Defense Approach:

As a developing country Turkey has a great increase in creating and using information technologies, and internet access. Both the government parties, and public and private sectors have offered so many information systems and e-services. Especially in the last decade information systems for national critical infrastructures and e-government services such as e-health, and e-education are developed and launched for the citizens. In addition, with the increasing scope and quality of the information and communications technologies frameworks people now can access to these services easily and from everywhere throughout the whole country. In the meantime these are some of the main factors that accelerate the development of Turkey in economics, and politics as an emerging country.

Turkey has pointed out the protection of its critical infrastructures and information systems against cyber threats as an urgent and priority task in recent years. Although it is not sufficient yet, the government takes some actions on creating national cyber security strategy. In this context, the government has been cooperating with private sector initiatives, and security experts in order to increase its capabilities in cyber defense and to create a cyber defense system. Turkey is now at the beginning of this journey and therefore has been trying to adopt a passive cyber defense strategy. Although all these actions are admirable, still a responsible national cyber defense institution which the official cyber security defense strategy is assigned to, has not established yet.

4.1.2.1. National Cyber Security Policy:

The National Cyber Security Strategy and the Action Plan for 2013-2014, is the primary national cyber security policy document of Turkey, was established on December 2012 by the National Cyber Security Board. The Board was created on October 2012 in order to set up the policy framework, to coordinate the cyber defense studies, and to follow their results. The goals of the strategy and the action plan are defined as follows (UN Secretary-General, 2013):

- *"To establish an infrastructure that enables the availability of the services, processes and data provided through information technologies by governmental organizations*
- *To ensure the security of information systems used in critical infrastructures that are operated by the Government or the private sector*
- *To determine the strategic cyber security actions to minimize the effects of cyber attacks and shorten the recovery time after attacks*
- *To constitute an infrastructure that facilitates the investigation on cyber crimes by judicial authorities and law enforcement bodies."*

This document points out midterm and long term objectives under some essential subjects;

- *International Cooperation:* Cooperation with other nations, and international organizations such as UN, NATO, EU, and OECD, is emphasized as one of the critical success factors of cyber defense strategy. Turkey should get involved in international events in order to improve its capabilities and share expertise on cyber security issues.
- *Cyber Security Legislations:* According to the action plan, establishment of national cyber security legislation framework plays very important role on fighting against cyber threats.

Therefore, the government should create the necessary laws in order to struggle effectively with cyber attacks and attackers.

- *Assigning Roles and Responsibilities:* Roles and responsibilities of government bodies, public and private sectors, universities, and social organizations should be defined clearly for conducting efficient cyber defense strategy and action plan. New institutions and authorities, responsible for conducting, coordinating, and assisting the cyber defense strategy, should be established urgently.
- *National Cooperation:* Government agencies, public and private sector should cooperate in order to take actions for protecting the national critical infrastructures, and vulnerable sectors.
- *Education and Awareness:* Training and raising awareness of human resources about cyber security is an efficient way in order to create safety and therefore it is emphasized as an essential.

4.1.2.2. Cyber Security Exercises:

National cyber security exercises are organized under the cooperation of The Information and Communication Technologies Authority (ICTA) of Turkey, The Scientific and Technological Research Council of Turkey (TUBITAK), and the Ministry of Ministry of Transport, Maritime Affairs and Communications, to coordinate the government agencies and public private sectors in order to develop the national and international cooperation, to increase the cyber defense capability, and raising the awareness. The first national cyber security exercise was held on January 2011 and the second was held on January 2013. Public, private and non-governmental organizations (involving representatives of the education, information and communications technology, health sectors, finance, defense and various ministries) were getting together in these

exercises. The number of participation was 41 in 2011 whereas 61 different institutions were participated in 2013.

In addition, a *Cyber Shield Exercise* was held on May 2012 under the coordination of ICTA, government body responsible on regulating telecommunications sector in Turkey, with the participation of Internet Access Providers. In this exercises, DDoS attack was simulated against the networks to measure their adequacy.

Moreover an *International Cyber Shield Exercise (ICSE)* was organized on May 2014 in Istanbul, Turkey, under the cooperation of Turkish Ministry of Transport, Maritime Affairs and Communications, ICTA, and ITU, in collaboration with the ITU-IMPACT. Representatives of 19 countries representatives participated to the ICSE 2014. The objectives of the event were launched as follow (ICSE2014, 2014);

- to increase awareness,
- to develop international cooperation on cyber security,
- to enhance capabilities and information sharing to fight against cyber threats ,
- to strengthen the capacity and the role of countries in the field of cyber security.

4.2. International Organizations

Because of the global nature of the cyberspace and becoming of the cyber security as one of the top priority/urgent issues in last decade, international organizations such as the the Council of Europe (CoE), the European Union (EU), the North Atlantic Treaty Organization (NATO), the Organization for Economic Cooperation and Development (OECD), the Organization for Security and Cooperation in Europe (OSCE), and United Nations (UN) have been heavily concentrating on dealing with it. But different organizations address different aspects of the cyber

subjects. As seen on the table below, OECD, EU, and CoE have performed activities about internet governance and cyber crime issues whereas the NATO and the UN focus on the cyber warfare. In addition UN carries studies on all fields of the cyber security while OSCE deals with the cyber crime and cyber terrorism.

Table 4.1. Dimensions of Cyber Security

	EU	CoE	OECD	OSCE	NATO	UN
Internet Governance	✓	✓	✓	–	–	✓
Cyber Crime	✓	✓	✓	✓	–	✓
Cyber Terrorism	–	–	–	✓	–	✓
Cyber Warfare	–	–	–	–	✓	✓

Source: Tikk, 2010.

When we look in more comprehensive manner, it is seen from the table in below, that OECD and EU make efforts on economic issues and data privacy areas of cyber security. On the other hand, since their duties are more related with the international security in military base, UN, NATO, and OSCE are working on cyber armed attacks response, terrorists uses of internet, national security relevant cyber crime. In addition, since the only UN and NATO are dealing with the cyber armed attack response activities their roles in cyber warfare will be detailed in this section.

Table 4.2. Areas of Cyber Security

	EU	CoE	OECD	OSCE	NATO	UN
Data & Privacy	✓	✓	✓	–	–	–
Spam	✓	–	✓	–	–	–
E-Commerce	✓	–	✓	–	–	–
General Network Security	✓	–	✓	–	–	✓
CIIP	✓	–	✓	–	–	–
Cyber Crime	✓	✓	–	✓	–	✓
National Security Relevant Cyber Crime	–	–	–	✓	–	✓
Terrorist Uses of Internet	–	–	–	✓	–	–
Cyber Armed Attack Response	–	–	–	–	✓	✓

Source: Tikk, 2010.

4.2.1. North Atlantic Treaty Organization (NATO)[2]:

NATO is one of the most active international organizations on dealing with cyber warfare. This organization's studies mainly address defending the organization itself and its member countries against cyber attacks. NATO has centered all of these efforts on cyber defense strategy.

NATO's studies on defending against cyber warfare have accelerated especially after the implementation of Cyber Defense Programme was approved in 2002. This program was an action plan that aimed improving the capabilities of NATO about defending against cyber attacks. However in 2007 the Estonia case (DDoS attack on Estonia) was the turning point for the

[2] NATO: *"the North Atlantic Treaty established in 1949 as a political and military Alliance of 28 member countries. NATO's essential purpose is to safeguard the freedom and security of its members through political and military means. NATO provides a unique opportunity for member countries to consult and take decisions on security issues at all levels and in a variety of fields." (Source: NATO - www.nato.int/nato-welcome/index.html)*

Alliance. As a result of these cases cyber warfare become more critical and urgent concern in international level (Hunker, 2010).

Prior to 2007, NATO primarily concentrated on protecting its own information and communication technologies infrastructure and its digital assets. But the Estonia case was the first real cyber attack organized against a whole country and after DDoS attack was begin Estonia requested technical assistance from NATO on cyber defense. In addition Georgia-Russia conflict proved that international organizations should deal with cyber warfare primarily. As a result of these cases NATO decided to extend its cyber security studies and started to develop a new and comprehensive cyber defense policy.

The first cyber defense policy (Policy on Cyber Defense) was adopted in January 2008 and 3 years after that, the second version of the Policy on Cyber Defense approved by the NATO in June 2011. Currently NATO has been working on implementation of the third generation cyber defense policy. This policy concentrated on 5 main topics (NATO, 2014):

- ***Developing the NATO cyber defense capability:*** The NATO Computer Incident Response Capability (NCRIC), created in 2002, responsible for developing the cyber defense capability by taking security actions in order to protect Alliance's digital assets. In addition, NCRIC includes researching, and watching new threats and technologic changes in order to remain up to date and be ready against cyber attacks.

- ***Increasing NATO cyber defense capacity:*** NATO carries out education, training, and evaluation activities on cyber defense in order to improve both Alliance's and Allies' capacity. In addition, NATO conducts cyber defense exercises, such as Cyber Coalition

Exercises, by simulating cyber attacks, and at the end collecting the lessons learned which the Alliance then may integrate them in its cyber defense elements.

The NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE), created in 2003 and accredited by NATO in 2008, conducts research and training facilities on cyber warfare under the sponsorship of Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Slovakia, Spain, Turkey, and United States. (Hunker, 2010).

- ***Assisting allies:*** NATO is assisting member countries on information sharing about protecting their critical information systems against cyber attacks, and improving their national expertise by conducting cyber defense exercises. In addition to this, NATO developed an action plan on cyber defense in order to help member countries during a cyber attack.

- ***Cooperating with other international organizations:*** Since the cyber warfare is a cross border issue NATO works with other international organizations such as United Nations (UN), European Union (EU), and Organization for Security and Cooperation in Europe (OSCE). Alliance believes that fighting against cyber attacks should be handled by universal participation. Besides this, through the cooperation with other organizations NATO aims to avoid waste of time, efforts, and resources because of the unnecessary duplication of work.

- ***Cooperating with industry:*** It is obvious that private sector has played crucial role in the context of technological developments, cyber security, and expertise. NATO believes that fighting against cyber warfare is not sufficient without cooperating with the industry. Therefore, this organization cooperates with the private sector in order to share

information and expertise via the NATO Industry Cyber Partnership (NICP) (NATO, 2014).

Although actively working on defense against cyber attacks, NATO primarily focuses on the passive defense that includes network protection through firewalls and other equipments. On the other hand, active defense includes more aggressive activities such as tracing the incoming cyber attacks, finding and deactivating the source. NATO should make more efforts on active defense in order to provide safer environment for Allies. In addition, clear and official definition on cyber warfare issues should be included in NATO's doctrine. Such as; what is cyber attack?, what the cyber war means?, what is the limits of cyber espionage activities carried by states and secret services?, what is the legal rights of victim states against a cyber attack?, and etc.

4.2.2. United Nations (UN)3:

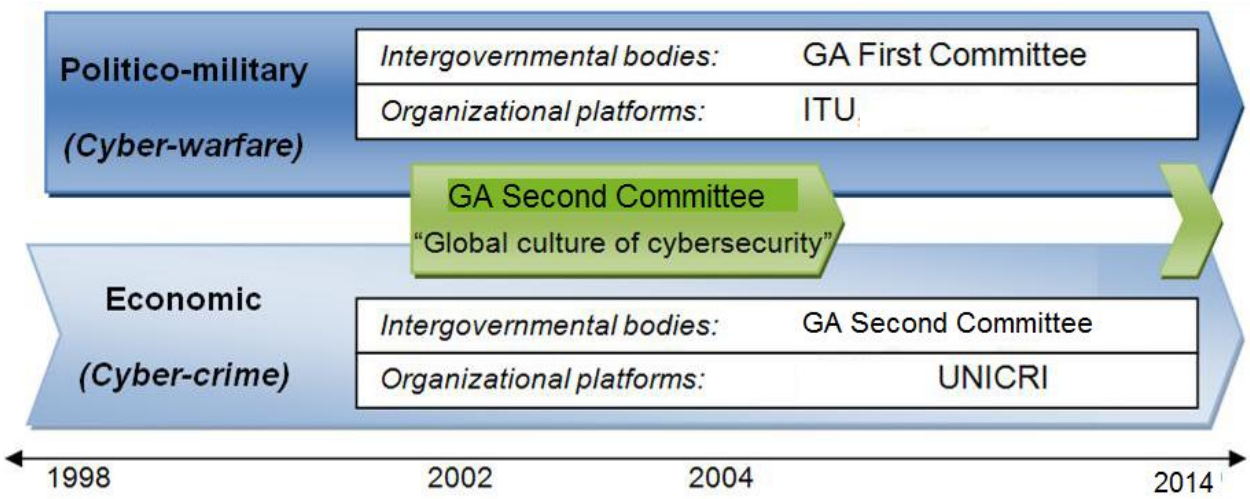
UN has worked on cyber security since 1990 and adopted some Resolutions which address cyber crimes;

- *"In 1990 the UN General Assembly adopted Resolution 45/121 on computer crime legislation.*
- *In 1994 published a manual on the prevention and control of computer-related crime.*
- *In 2000, the General Assembly adopted a resolution on combating the criminal misuse of information Technologies.*
- *In 2002 another resolution tackled the criminal misuse of information technology.*

[3]UN: "*The United Nations is an intergovernmental organization established on 24 October 1945 to promote international co-operation. The organization was created following the Second World War to prevent another such conflict. At its founding, the UN had 51 member states; there are now 193*" (Source: Wikipedia, en.wikipedia.org/wiki/United_Nations).

- *At the 11th UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, in 2005, a Declaration was adopted that highlighted the need for harmonization in the fight against cybercrime.*
- *In 2004, the United Nations Economic and Social Council (ECOSOC) adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.*
- *In 2007, the Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.*
- *The topic was again discussed by the Council in 2009 and a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime was adopted." (HIPCAR, 2012)*

All activities on cyber security are conducted in two main perspectives – *politico military, economic* – through the whole UN organizations. Politico-military studies are primarily concentrating on legislative and technical issues while Economic studies are about the criminal misuse of computer systems. As it is shown in the figure GA First Committee, and ITU are the most active parties who are responsible with the politico-military issues, since GA Second Committee, and UNICRI are most important parties who are responsible with the economic perspective.



Source: Maurer, 2011

Figure 4.1. UN Perspectives on Dealing with Cyber Security Activities

4.2.2.1. General Assembly (GA) Committees:

There are six different committees were created under the management of the General Assembly. The first three committees have worked on cyber security issues and discussed the draft Resolutions which are then sent to the General Assembly's annual session for adoption.

- *The GA First Committee (Disarmament and International Security Committee)*, deals with disarmament and related international security issues;
- *The GA Second Committee (Economic and Financial Committee)* deals with economic issues; and
- *The GA Third Committee (Social, Humanitarian and Cultural Committee)* deals with social and humanitarian issues.

4.2.2.2. The United Nations Interregional Crime and Justice Research Institute (UNICRI):

This institute helps and assists other governments, and also non-government organizations on defining policies and implementing cyber security frameworks, preventing cyber crimes, and criminal justice (Maurer, 2011).

4.2.2.3. International Telecommunication Union (ITU):

ITU is the most active agency of the UN in the context of developing and assisting practical activities on cyber security among other issues such as standardization and development of the telecommunications. This organization has carried out very important activities related with legal and technical fields of cyber security, and international cooperation.

World Summit on the Information Society (WSIS): This includes two phases international conferences held by the ITU with the participation of governments, policy makers, private sectors, and experts from around the world. These parties shared their information, experiences, and ideas about the issues related with internet, information society, and security. The first phase was conducted in Geneva, Switzerland in 2003 and the second phase was in Tunis, Tunisia in 2005. At the end of the Geneva, and Tunis four documents - *Geneva Declaration of Principles, the Geneva Plan of Action*, the *Tunis Commitment, and the Tunis Agenda for the Information Society* - were agreed on as outputs of the phases. Cybercrime related issues such as the importance of international cooperation in fighting against cybercrimes and creating compatible national legislative framework were emphasized on the Tunis Agenda. In addition to this,

responsibility of conducting Action Line C5 of *Geneva Plan of Action* (*Building confidence and security in the use of ICTs*)[4] was taken by the ITU (ITU, 2013).

ITU Global Cybersecurity Agenda (GCA) and Global Strategic Report: In 2007 ITU launched the GCA that included the strategies for the development of cybercrime legislation model as one of the seven goals of agenda. Based on this agenda, ITU announced the Global Strategic Report which covers the overview of some international approaches in fighting with cybercrime. This

[4]**Action Line C5 of *Geneva Plan of Action*:**

Confidence and security are among the main pillars of the Information Society.

a. *Promote cooperation among the governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.*
b. *Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.*
c. *Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy.*
d. *Take appropriate action on spam at national and international levels.*
e. *Encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions including electronic means of authentication.*
f. *Further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.*
g. *Share good practices in the field of information security and network security and encourage their use by all parties concerned.*
h. *Invite interested countries to set up focal points for real-time incident handling and response, and develop a cooperative network between these focal points for sharing information and technologies on incident response.*
i. *Encourage further development of secure and reliable applications to facilitate online transactions.*
j. *Encourage interested countries to contribute actively to the ongoing United Nations activities to build confidence and security in the use of ICTs.(Source: ITU - www.itu.int/wsis/docs/geneva/official/poa.html)*

report focuses on legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation (Maurer, 2011).

Understanding Cybercrime - A Guide for Developing Countries, and ITU Toolkit for Cybercrime Legislation: In 2009 ITU announced these two guides in order to support and assist on creating national cybercrime legislations of developing countries. These documents were developed by a team of policy experts, industry representatives, academicians, attorneys, technical experts, and government personnel from around the world. The *Understanding Cybercrime Guide* aims to create compatible and harmonized legislative frameworks for ITU members (ITU, 2009). Similarly, the *Toolkit* aims the adoption by all countries of appropriate legislation against the misuse of information and communication technologies for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security (ITU, 2010).

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

Information systems are one of the most important assets for the governments, public sectors, and private sectors. Using of these digital assets can be witnessed in everywhere. While systems owners are trying to protect their assets, different types of cyber threats are used by the attackers in order to surpass the security systems. Malware programs such as viruses, worms, and Trojans are traditional threats which have been used since the early stages of the cyber warfare. On the other hand, using unwanted programs is increasing very fast while DoS and DDoS attacks are more organized attacks with their time limited effects. The new versions of these threats are more complicated and more dangerous than their predecessors. More important, in today hackers are using embedded attacks that have more than one cyber attack's characteristics, to cause more damage on the digital assets. Therefore sometimes it can be very difficult to classify a cyber threat as one type, for instance as a worm or a Trojan, since it has some abilities from both types. Moreover, contrary to common belief cyber threats do not come from outside but from inside the organizations. Due to the fact that statistics show more than 60% of total cyber attacks are carried by the insiders, organizations must take account of this reality and take the necessary measures against those attacks.

Since cyber space offers huge advantages for the attackers, cyber attacks are frequently used in international level. States, terrorist groups, and hacker groups are now using cyber warfare for attacking their enemies. Because, organizing a cyber attack is much cheaper and easier than organizing a physical attack. In addition, attackers can hide their real identity and they can also cover their tracks in cyber space. Although there are some other motivations, these three are most important factors behind the dramatic increase of cyber attacks.

Different types of cyber attacks have caused different effects on the victim systems. Some are less dangerous which have short term effects while others are more dangerous and they may cause more serious damages. Cyber protest is the least dangerous one because of its time limited nature and less destructive effects, while cyber sabotage and cyber war are the most dangerous since they are long term attacks and because of their destructive nature. Especially with the Estonia case, and Stuxnet case cyber sabotage has become the biggest concern for states in the last decade. Furthermore, cyber war will be the next step in cyber space if governments and international organizations don't take preventive actions against these types of attacks.

Almost all international organizations are taking the cyber security as a serious issue and conducting some studies. However, they generally concentrate on the data privacy, general network security, and cyber crime issues. The only organizations, dealing with the cyber armed attack response activities, are UN and NATO. They focus on how the legal standards should be created, and how they can support developing countries in fighting cybercrime. Although they conduct so many valuable studies, they have not adopted a comprehensive legal framework on combating cybercrime, and operational framework on active defense strategy.

On the other hand, countries have realized the importance of having cyber power and cyber security. So many countries are dealing with improve their abilities on cyber offense and defense. According to the Laundon & Treva (2012) some countries such as China, USA, Russia and North Korea are in very advanced stages of test and use of a cyber weapon while more than 100 nations have cyber warfare capabilities and programs.

Finally since the cyber warfare is an international phenomenon, it should be handled as universally. International organizations, especially United Nations and NATO should concentrate on;

- identifying a clear definition of cyber attack, cyber war, the legal limits of cyber espionage activities carried by states and secret services, the legal responses and rights of victim states against a cyber attack,
- identifying the human rights, humanitarian, and ethical rules of information warfare on national and international security and
- implementing active defense strategy which include more aggressive activities such as tracing the incoming cyber attacks, finding and deactivating the source.

On the other hand governments also should take the responsibility fighting against the cyber attacks. They should concentrate on;

- creating a national strategy on both the passive and active cyber defense,
- identifying roles and responsibilities of government institutions according to national cyber defense strategy,
- developing disaster recovery plans for their critical infrastructures (transportation, finance, energy and communications services) to make them available under the cyber warfare conditions and,
- developing secure IT systems and software applications,
- working with the private sector and helping them to develop the business action plan for defense against the cyber attacks and
- educating their staffs and the public.

REFERENCES

ARCYBER. (2014). ARCYBER Web Page, Retrieved from www.arcyber.army.mil/org-arcyber.html

Awad, N.F., & Fitzgerald, K. (2005). The Deceptive Behaviors that Offend Us Most About Spyware, *Communications of the ACM, 48 (8),* p. 55-60

Aycock, J. (2011). Spyware and Adware, *Springer.*

Baylor University. (2014). Sniffing (network wiretap, sniffer) FAQ, Retrieved from cs.baylor.edu/~donahoo/tools/sniffer/sniffingFAQ.htm

Bellovin, S.M., & Pfleeger, P.C. (2008). Insider Attack and Cyber Security Beyond the Hacker, Advances in Information Security, *Springer*, p. 1-15

Broad, W.J., &Markoff, J., &Sanger, D.E. (2011). Israeli test on worm called crucial in Iran nuclear delay. The New York Times, Retrieved on December 15, 2013, from http://www.cfr.org/iran/nyt-israeli-test-worm-called-crucial-iran-nuclear-delay/p23850

Canbek, G., & Sagiroglu, S. (2007). Malware and Spyware: A Comprehensive Review, *Gazi University Faculty of Engineering Archives, 22 (1),* p. 121-136

Cavelty, M. D., The Reality and Future of Cyberwar, Retrieved on December 17, 2013, from kms2.isn.ethz.ch/.../Files/.../Reality_and_Future_of_Cyberwar.pdf

Chinh, H.N., & Hanh, T., & Thuc, N.D. (2013). Fast Detection of DDoS Attacks Using Non-*Adaptive Group Testing, International Journal of Network Security & Its Applications (IJNSA), 5 (5),* p. 63-75

Clark., R. (2009). War From Cyberspace, *The National Interest, November/December 2009*, p. 31 – 36, Retrieved on December 17, 2013, from web.clas.ufl.edu/users/zselden/coursereading2011/Clarkecyber.pdf

Clark, R. (2011). China's Cyberassault on America, *Wall Street Journal, June 15, 2011*, Retrieved on December 15, 2013, from belfercenter.hks.harvard.edu/publication/21124/chinas_cyberassault_on_america.html

de Vivo, M., & de Vivo, G.O., & Isern, G. (1997). Internet Security Attacks at the Basic Level, *GIRAS U.C.V.*

Even, S., & Siman-Tov, D. (2012). Cyber Warfare: Concepts and Strategic Trends, Memorandum 117, Institute for National Security Studies, Retrieved from www.inss.org.il/index.aspx?id=4538&articleid=2487

Falliere, N., &Murchu, L.O., &Chien, E. (2011). W32 Stuxnet Dossier, Symantec Security Response, Retrieved from www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War, *Survival, 53 (1)*, p. 23 – 40, Retrieved on December 15, 2013, from www.cyberdialogue.ca/wp-content/uploads/2011/03/James-Farwell-and-Rafal-Rohozinski-Stuxnet-and-the-Future-of-Cyber-War.pdf

Fosnock, C., Computer Worms: Past, Present, and Future, *East Caroline University*, Retrieved from www.hackerzvoice.net/madchat/vxdevl/avtech/Computer Worms: Past, Present, and Future.pdf

Gasti, P., & Tsudik, G., & Uzun, E., & Zhang, L. (2013). DoS & DDoS in Named-Data Networking, Retrieved from named-data.net/wp-content/uploads/2013ICCCN-DOS.pdf

Gordon, S. (2005). Fighting Spyware and Adware in the Enterprise, Retrieved from www.infosectoday.com/IT Today/spyware.pdf

G Grover, A., Cyber War's Final Frontier: Network Centric Warfare Framework, Retrieved on December 14, 2013, from www.itffroc.org/articles/ag_cyberwar.pdf

Gupta, G., & Pieprzyk, J. (2011). Socio-technological Phishing Prevention, *Information Security Technical Report, 16 (2)*, p. 67-73

Harris, B., & Hunt, B. (1999). TCP/IP Security Threats and Attack Methods, *Computer Communications, 22 (1999)*, p. 885-897

Harris, S. (2008). China's Cyber-Militia, National Journal, Retrieved from www.nationaljournal.com/magazine/china-s-cyber-militia-20080531

HIPCAR. (2012). Cybercrimes/E-crimes: Assessment Report, Retrieved from www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR Assessment Cybercrimes.pdf

Hunker, J. (2010). Cyber War and Cyber Power Issues for NATO Doctrine, NATO Defense College - Research Division, Retrieved from www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.ndc.nato.int%2Fdownload%2Fdownloads.php%3Ficode%3D230&ei=uuHdU7ulHtCOyASmv4G4BQ&usg=AFQjCNEFdsSBly3rFQ0EL3Ykf2Gj1JrgbA&sig2=G2hysb7eYs716yFa4CSFkQ&bvm=bv.72197243,d.aWw

IBM. (2014). Sniffers, Retrieved from www-01.ibm.com/support/docview.wss?uid=swg21499365&aid=1

ICSE2014. (2014). ICSE 2014 was performed successfully, Retrieved from www.icse2014.org/content/after-event

ITU. (2009). Understanding Cybercrime: A Guide for Developing Countries, *ITU Publications*, Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

ITU. (2010). ITU Toolkit for Cybercrime Legislation, *ITU Publications*, Retrieved from www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

ITU. (2014). World Summit on the Information Society, Retrieved from www.itu.int/wsis/index.html

Kim, W., & Jeong, O., & Kim, C., & So, J. (2010). The Dark Side of the Internet: Attacks, costs and responses, *Kyungwon University.*

Laudon, K.C., & Traver C.G. (2009). E-commerce: Business, technology, society (5th ed.). *New Jersey: Pearson Prentice Hall*, p. 272-285.

Lynch, D.M. (2006). Securing Against Insider Attacks, Information Security and Risk Management, *Auerbach Publications Inc.*, p. 39-47

Maurer, T. (2011). Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-security, Discussion Paper 2011-11, Harvard Kennedy School, Retrieved from belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

NATO. (2014). NATO and Cyber Defense, Retrieved from www.nato.int/cps/en/natolive/topics_78170.htm?selectedLocale=en

OECD. (2009a). Online Identity Theft, *The Organization for Economic Cooperation and Development (OECD) Publishing*, p. 15-32

OECD. (2009b). Computer Viruses and Other Malicious Software: A Threat to the Internet Economy, *OECD Publishing*, Retrieved from www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page31

Ogun, M.N., & Kaya, A. (2013). Significance of Cyber Security for National Security: A Study Concerning the Necessary Measures, *Journal of Security Strategies (Güvenlik Stratejileri Dergisi), 18-2013*, p. 145-181.

Ozturk, O. (2009). Spam Problem in E-mail Service and Solution Proposals, *ICT Expertise Thesis for Information and Communication Technologies Authority of Turkey*.

RT Network, Anonymous Launches Massive Cyber Assault on Israel, Retrieved on December 14, 2013, from rt.com/news/opisrael-anonymous-final-warning-448/

Schneier, B. (2010). The Story Behind The Stuxnet Virus, Forbes Commentary, Retrieved on December 14, 2013, from www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

Schryen, G. (2007). Anti-Spam Measures Analysis and Design, *Springer*, p. 7-8

Silva, S.S.C., & Silva, R.M.P., & Pinto, R.C.G., & Salles, R.M. (2012). Botnets: A survey.

Symantec Security Response, www.symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99.

Sutter, J. D. (2012). Anonymous Declares 'cyberwar' on Israel, Retrieved on December 15, 2013, from http://www.edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html

Tickle, A.B., & Ahmed, E., & Bhaskar, S.M., & Mohay, G., & Panicphrecha, S., & Raghavan, S.V., & Ravindran, B., & Schimidt, D., & Suriadi, S. (2011). An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, *Springer,* p. 10-11

Tikk, E. (2010). Global Cybersecurity–Thinking About The Niche for NATO, *The SAIS Review of of International Affairs, XXX (2), p. 105-119, The Johns Hopkins University Press,* Retrieved from uofahsmun.files.wordpress.com/2012/06/microsoft-word-globalcybersecurity-2010-09-11-et.pdf

UN Secretary-General. (2014). Developments in the Field of Information and Telecommunications in the Context of International Security, Retrieved from https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/e68ed4bd170321b285257bc70067f864/$FILE/A 68 156 Add1.pdf

Weems, R.P. (1998). Computer Viruses: A Growing Problem, *Library & Archival Security, 14 (2),* p. 51-59.