CYBER SECURITY, TOOLS AND METHODS OF CYBER THREATS, DIMENSION OF CYBER THREATS AT THE PRESENT TIME AND CYBER ARMIES

MEHMET ALI GEZKAYA

Turkish Air Force Academy
E-mail: 1825gezkaya@harbiyeli.hho.edu.tr

Abstract— At the present time it's hard to black out our secret informations because of the developing technology. Nowadays getting access to secret information is so easier than the past by the way of cyber attacks. People can damage the systems with little energy and effort. As a result of these causes, conception of cyber security has occurred in the world. Cyber security can be made personal or corporate. Especially after the cyber attacks started to target to critical platforms, governments started to take care about cyber security more than before. So cyber security and it's technics started to grow faster. In this article, we are going to mention about what is cyber security, which technics and methods are used in cyber attacks and what should be made for cyber security.

Keywords— Cyber security, cyber space, information systems, Stuxnet, cyber army.

I. INTRODUCTION

The world order has changed with means of portable computer technology and proliferation of internet. Distances between people have decreased and new communication habits has appeared. At the present time, when an event happened in the world, it can be known from all over the world at the same time. However, advancing technology has caused some problems, either. The best example of that is the internet. Internet is spreading rapidly with the way of development in the computer technology.

After the Cold War, the internet had started to spread and therefore; a wide cyberspace has appeared. Cyberspace is the environment which is composed of information systems that spread all over the world and space and nets that are link these systems ("UlusalSiberGüvenlikStratejisive 2013-2014 EylemPlanı", 2013). Access to information communication speed has increased rapidly with the spread of the internet. The cyberspace spread to wide environments like personnel lives and business lives in a short span of time. In addition to people, countries are taking advantages of information technologies and effects of cyber environments about infrastructure services, communications, diplomacy, provide intelligence and defence technologies. In addition, communications between governments and people increased and the governments could control their people easier than before with the help of cyberspace.

Because of all these causes, the technology has to be stable, secure and resilient. However, advancing technology and spread of cyberspace are making it harder to be stable, secure and resilient. As a matter of fact, spread of cyberspace and advancing of technology caused increasing of cyber attacks. Therefore, the cyber security increase in value.

Cyber security means protection of information systems, guarantee of privacy, integrity and accessibility of information, detecting of cyber attacks, reacting against detected cyber attacks and after cyber attacks reverting the systems to their condition before cyberattack ("UlusalSiberGüvenlikStratejisive 2013-2014 EylemPlanı", 2013). This concept which is be constituted for answering the attacks in the cyberspace excited attention of governments in a short span of time. The most important case of cyber security is providing privacy, integrity and accessibility of data.

Cyber security is important to people for privacy of critical information as private life, id numbers, passwords, credit card informations etc. To governments it has very important position for keeping private information secret, preventing spread of intelligences, providing services, protecting of economy and especially protecting critical infrastructures like nuclear power stations.

At the present time, cyber attacks can be made by hackers, interior attackers, cyber activists and intelligence agencies. Governments have to take their precautions to react these attacks. After cyber attacks to Estonia and discovery of Stuxnet Worm, cyber securityperceptions have changed in the world and the governments started to pay more money to provide their cyber security.

II. SOME CYBER ATTACK TOOLS AND METHODS

There are so many types of attacks in the cyberspace. Therefore, computer scientists should be able to protect computers from them. Attackers use these attacks and spoil computers and networks by the ways of changing, destroying, cutting the services

and leaking information. These attacks can harm people, organisations and public bodies. They can cause financial damages and loss of reputations.

In the cyberspace, most of these threats appears with more than one variable. Because of multidimensionality of threats, cyber defence has to be multidimensionality, as well. In cyberspace, every move should be in secret. But solving of advanced security programs require associations. In this part of article, cyber attack tools and methods will be explained.

2.1. Viruses

Viruses are computer softwares which change themselves as system files or programs. Viruses are special malicious softwares that set-off to other files and spread. The first virus according to records is a boot sector virus named "Brain" and it has appeared in 1986 (Graham & Howard, 2010). Basic principle of loading viruses is that the viruses need to be activated by users. Else they can't load themselves. Viruses generally set-off to systems with the ways of opening e-mails and running USBs automatically.

2.2. Worms

Worms are malicious softwares that copy themselves from one device to another as viruses. Their basic difference from the viruses is that worms don't need to be activated by users. Worms especially capture functions thattransport files and data. After they set-off the system, they keep spreading themselves. The most dangerous characteristic of worms is their substantially reproduction abilities. They use methods of transportation data and files in setted-off systems and they send themselves to every e-mail in all systems that are in contact with setted-off systems. Because of that network traffic can be too slower. Especially in early on they are created, security softwares can't know them so they spread so fast and they influence network traffic negatively. Because of that, these influential worms are used in cyber attacks intensely. Because worms doesn't need a program or file to spread, worms can drive tunnels in systems and they provide opportunity of capturing remote access (*Virüs, SolucanveTruvaAtıNedir?*, 2012).

2.3. Trojan Horses

Trojan horses are the computer programs which presents themselves as they have beneficial functions but at the same time they enclose malicious functions to bypass the security mechanisms and sometimes they exploit authorisations of legitimate system units (Kissel (Ed.), 2011). Generally Trojan horses are presented as free softwares and they set-off the systems by downloading and loading by users.

Generally Trojan horses provide opportunity of capturing remote access. Therefore, they provide opportunity of using computers as zombie computers, either. Best way of being protected from Trojan horses is not loading of programs that have unknown sources.

2.4. Rootkits

Rootkits are the computer programs which are set-off the system, hide themselves among running processes, provide opportunity of capturing remote access and hard to find (UlusalSiberOlaylaraMüdahaleMerkezi, 2014). Objectives of rootkits are not making systems slower or spreading. Their objectives are to establish complete dominance on computers and hide themselves.

Rootkits set-off the systems with the way of running senior authority. In addition, they set-off in multiuser systems with the way of gaining root privileges by root aperture.

2.5. Spywares

Spywares are computer softwares that created for spying on computers. Spywares collect important information of users and process of users without user's knowledge and they provide opportunity of these informations sending to ill-wishers (UlusalSiberOlaylaraMüdahaleMerkezi, 2014).

Spywares don't need to spread like viruses and worms. Their objectives are ensuring confidentiality of themselves and collecting information. They generally install in free versions of programs and the computer warn when they are installed. But generally users don't care about warnings and install spywares unconsciously.

2.6. Denial of Service(DOS)

Denial of Service is inhibition of users access and making that the system can not provide service. In some conditions, service may not stop but it slowdowns and system doesn't mean anything for providing service. In denial of service attacks, network sources of host computer are exhausted and it is expected to become unable to respond requests from the system. If denial of service attacks are carried out from more than one resources, it is named as distributed denial of service(DDOS). Denial of service attacks can be made as method of occupy the network or making the system unavailable by physical damage.

III. A BRIEF HISTORY OF CYBERCRIME WITH EXAMPLES FROM THE WORLD

In this part of article, we will give information about some cyber attacks because of showing cyber security's importance and dimension of cyber attacks. Beginning of the internet which is commonly used at the present time is ARPANET. USA felt itself in danger of nuclear threat in Cold War and planned a network topology against nuclear threat. In time with joining of UK and France, first intercontinental

network was established. Thus, network topologies began to grow.

Growth of network topologies increased curiosity of new technology. In 1971, an employee of BBN Technologies Bob Thomas who is part owner of ARPA in advanced Technologies wrote the first self-replicating program. He named the program as "Creeper" and installed the program DEC PDP-10 computers which run on TENEX operating systems. Creeper started to spread on ARPANET in a short time. The program was writing on the screen "I'm the creeper, catch me if you can!" in computers it setted-of. When the problem was noticed Reaper was written for deleting Creeper. Thus, the first worm in Arpanet had been the first pointer of future threats about cyber security (Bıçakcı, 2014).

After the Cold War, ARPANET started to spread. First, it started to spread in universities then it started to spread in personal computers. Providing cyber security became more complex with spread of internet. Because of that, a new attack made against ARPANET and in October 27, 1980 ARPANET stopped service for 72 hours because of a virus that setted-off status messages (Rosen, 1981).

Another example of cyber attack in the world is the Morris Worm. Robert Morris programmed a self-replicating and self-propagating worm that can be installed in the internet as a master project when he was just 23 years old and he named the program as "Morris Worm". Morris decided to test his program on internet system of Harvard University. After the loading of program, he noticed speeds of copy and spread of worm is more than he estimated. Worm exploited so many deficits in target system. One of them is Unix Sendmail. Morris' attacks caused so serious material damages. Morris Worm is first target-specific worm in history (Güner, 2015).

One of the most interesting examples in the world is the cyber attacks carried out against Estonia in 2007. Estonia draws attention as one of the countries with the highest internet usage. Every citizen of this country has digital identity to access government agencies and banks over the internet. In the country, many government agencies serve on the internet. In 2001, data exchange layer X-Road connected government agencies and citizens. This is the most common application example of e-government applications. Also in 2005, country allowed local election voting over computer networks. Thus, they blaze a trail. According to 2010 data 75% of the country's population are internet users (Seybert, 2011).

At the evening of December 27, 2007 cyber attacks started against the country as ping intensity and in a short time, attacks transformed as denial of service (DOS) attacks (Bıçakcı, 2012). Ping intensity was so high and it targeted so many institutions therefore, experts claimed that attacks were made by wide audience.

Big banks in the country were prepared therefore they weren't affected from attacks. But, government websites was affected so much and they couldn't provide services. The lack of systems that control and watch IPs in the country had made the threat more palpable (Bıçakcı, 2014).

In this attacks data packets that designed special to crash X-Road system were sending to routers and IPs were recording from several countries by DOS attacks (Bıçakcı, 2014). Estonia government tried to prevent attacks by increasing bandwidth but it didn't suffice and government called for help from NATO and other countries.

Cyber security perception has changed with these attacks. The world understood what cyber attacks can achieve and started to discuss in which conditions cyber attacks can be cause of war. Security organizations, especially NATO started to take precaution to prevent cyber attacks and they started to promote their members to do that. One of them is CCD COE (Cooperative Cyber Defence Centre of Excellence)NATO established in Tallinn(capital of Estonia) in 2008.

In 2008 before an military operation to another country cyber attacks were made. These attacks were almost same with cyber attacks against Estonia but this country wasn't depended on as much as Estonia therefore effects of these cyberattacks were less than attacks against Estonia. In these operations the most remarkable point was using of hybrid war technique. In operations cyber attacks and conventional warfare techniques were used in the same time.

The most notably and best known example of cyber attacks is Stuxnet. Stuxnet is a worm which was targeting nuclear facilities of Iran. It is detected by a software corporation named VirusBlokAda in Belarus in June, 2010. It affected nuclear facilities of Iran in Buşehr and Natanz (Avcı, 2014).

Stuxnet showed industrial systems and self-enclosed systems can be targets of cyber attacks, too and it moved cyber security to a new dimension. In this project, worm can be set-off by electric lines, too but according to experts base of set-off method is loading of worm to an engineer of Natanz Nuclear Facility's laptop by an USB (Avcı, 2014).

There is so many claims about who produced Stuxnet. The common thought made as a result of research on Stuxnet is this worm has avery complex form. Also another common thought is this worm

wrote by an expert crew, not a person and for this project so much money were spend. Owing to these, the experts are thinking the worm wasn't written by a simple crew, it was written by government sponsored enterprise.

Stuxnet especially targets to mainboard (PLC). This is the most important feature of Stuxnet. This worm was especially spread by Microsoft Windows and it was targeting Siemens' S7 300 modules (Bıçakcı, 2014). Stuxnet was setting-off to computers by external hard drives, copying itself to computer drive directory and searching for Siemens' SCADA(Supervisory Control and Data Acquisition) programs named WinCC and PCS 7. After it found these programs, it integrates itself to program by using Siemens' passwords and it changes control logics as malicious software programmer's claims by attaching modules to program. In this way it can affect control mechanism of whole facility. It introduced itself as a System32 file named "lsass.exe" and it is distributed by this way.

Another noteworthy aspect of the Stuxnet is it's use of four Zero Day Exploit. Zero day exploit is the system exploit that isn't noticed yet by software developers. In closed source softwares noticing of zero day exploits harder than open source softwares and this condition threats the system's secure. In fact, using of zero day attacks isn't new, attackers used them before, too and they had broad authorities in systems by this way but generally, these attacks use just one zero day exploit. Stuxnet use four zero day exploits. With this feature Stuxnet is an unique program and it has an unique place in cyber security. Other noteworthy aspects of the Stuxnet are it's signing it's drivers with the root certificates stolen from Realtek company to load it's kernel drivers easily to hide itself and it's trying to change physical processes hidely in energy facilities.

Creating this worm is about databases, root informations, PLC algorithms, stolen electronical signs of Realtek and Siemens' hardware. Experts claim the worm can't be written by just a person, they think it was written by a crew that is comprised of experts in different areas. This condition supplies discourse of this worm created with support of government.

After short time from Stuxnet, Budapest University of Technology and Economics declared to the public a Trojan named "Duqu". Several features of Duqu are very similar with Stuxnet's features therefore, experts claimed Duqu was produced by programmers that can reach Stuxnet's kernel. But Duqu's main object was gathering intelligence about industrial control systems. To do that Duqu was copying passwords, capturing screen shots to understand how some special processes are being made and stealing many documents (Laboratory of Cryptography and System Security, 2011).

While discussions about using Duqu in cyber espionage Iran's Computer Emergency Response Team (CERT) declared in May 28, 2012 "Flame Malware" was founded (Selvan, 2012). Object of software was gathering intelligence. The software was recording every sound, screen shot, keyboard key and Skype talk and monitoring network traffic in setted-off computers (Selvan, 2012). Also the software was making Bluetooth enabled and making list of Bluetooth-enabled devices. It was spreading by this way. It is claimed the software was collecting AutoCAD drawings, PDFs and text documents, also it was analyzing Arabic and Hebrew texts if these documents have geotagging it was collecting them, too (Antiy Labs, 2012).

IV. DIMENSION OF CYBER THREATS AT THE PRESENT TIME AND CYBER ARMIES

At the present time, cyber threats have reached very large dimensions. With the end of the Cold War, contents of cyber threats advanced with spread of internet and it started to affect more systems in a short time. Of course, cyber attacks which are made with physical access are undesirable and critic as cyber attacks which use internet. Stuxnet which is mentioned before in this article is one of best examples of that.

At the present time, everybody can reach cyber attack tools easily even people who don't know anything about cyber attacks. This is a very undesirable condition in terms of cyber security. Effects of this condition had seen in Estonia in 2007. We also mentioned about that. At the present time, cyber activists are attacking when a condition happened they don't like. Therefore cyber attacks may be encountered every time and people and institutions should be ready as they can answer cyber attacks.

At the present time, cyber power is accepted as the fifth power after army, navy, air and space powers. Cyber power needs less cost and it affects more than other elements of power. Therefore, cyber power appeared as a power which every country has desired to have. In the same time, with using of conventional warfare techniques and cyber power together, the hybrid warfare techniques has occurred.

Increase of cyber war is the possible consequence of ever-increasing cyber threats. Cyber war threats can come by hackers, interior attackers, cyber activists and intelligence agencies. Therefore, states have to take precautions to protect their agencies from every cyber warfare. One of these precautions is building cyber armies as these armies can answer cyber attacks instantly. Objects of cyber armies protect their

government's agencies against every cyber warfare threats and attack every systems of other countries when it is necessary. Cyber armies have to be competent as they can size cyber supremacy.

Another reason of necessitating the existence of cyber armies is cyber terrorism. At the present time, terrorism cause trouble to many countries, now it threats nations in cyberspace, too. Cyber terrorists can attack military, financial and service infrastructures of target countries by using of hackers' programs. Therefore, many countries are concerned about this condition.

At the present time, many countries started to build their cyber armies. Experienced cyber attack incidents showed how cyber threats reached high dimensions. Therefore, cyber armies have to be competent as they can react every attacks instantly. Cyber armies are competent as they can protect military, financial and service infrastructures.

CONCLUSIONS

At the present time, cyber security has ever-increasing importance because of ever-increasing cyber threats. Variety of cyber threats and dimensions that has reached made changing of cyber security perception and providing an active and dynamic cyber security infrastructure necessary.

Precautions that individuals should take are using licensed antivirus softwares, using an active firewall, not entering websites that are untrusted, notdownloading any files from untrusting websites and not sharing every information in everywhere. Individuals should use websites that's URL addresses start with "https" and they should scan their files before downloading on web-based antivirus softwares.

Providing cyber security is harder for governments. Cyberspace's size cause inadequacy of the cyber security precautions. Because of that, governments are trying to take precautions by creating their own cyberspaces.

Because of uncertainty of actors and propagation speed of cyberspace, governments can't react attacks with conventional methods. Therefore, governments need asymmetric cyber armies that can answer rapidly. Cyber armies should be able to immobilize during attacks, they should take precautions and they should have possibility of intervention.

The most important factor in cyber security is human. Human is the weakest link of cyber security. Therefore, providing training about cyber security to users of computer technologies is very important. Every cyber threats that individuals can face and their answers should be taught to individuals. Institutions should build their own cyber security infrastructure and they should train their employees as governments.

In cyber security, awareness should be created firstly and expert managers should be found. In a possible attack, what will protect and how will it protect should be identified, continuous watching and control should be provided on system. Hardware and software precautions should be taken and hardwares and softwares should be configured as they will have a strong protection against cyber security breaches when softwares produce. Source codes of softwares should be protected. A national strategy should be created and nations should act according to this strategy. R&D activities about cyber security should be supported and international cooperations should be increased. Teams that can answer attacks instantly should be created. Backups of critical informations should be taken periodically for protecting them from possible attacks. Also system should be tested periodically to find system vulnerabilities and precautions should be taken to close them.

In critical infrastructures like nuclear facilities, providing cyber security is more important. In infrastructures like this, open source operating system should be used. This operating system should have unique packets and architecture and it should write as unique on kernel. Because, attacks that target waisted system architecture are clear. Softwares that will use hardwares and operating systems should be unique and national, too. In infrastructures like that, a closed network structure should be created and controlling of this network should be provided continuously. Wireless networks shouldn't be used in network structure. Any computer or external memory shouldn't enter the system from outside and control of system's users should be provided.

REFERENCES

[1] Antiy Labs. (2012, July). *Analysis Report on Flame Worm Samples Version 1.3.0*. Retrieved Jan 2, 2016, from http://www.antiy.net/downloads/Analysis-Report-on-Flame-Worm-Samples.pdf

[2] Avcı, Burak. (2014, June 21). *Stuxnet VirüsüNedir,NasılÇalışıyorveKaynakKodları.* Retrieved January 08, 2016, from http://www.burakavci.com.tr/2014/06/stuxnet.html

[3] Bıçakcı, Salih. (2012). YeniSavaşveSiberGüvenlikArasındaNATO'nunYenidenDoğuşu,*UluslararasıİlişkiIer, Vol 9 (34).* Summer 2012, pp. 205-226.

[4] Bıçakcı, Salih. (2014). .NATO'nunGelişenTehditAlgısı: 21. YüzyıldaSiberGüvenlik.*UluslararasıİlişkiIer*, Vol 10, Number 40 (Winter 2014), pp. 101-130.

[5] Bilgiportal İnternet Sitesi. (2012, October 22). *Virüs, SolucanveTruvaAtıNedir?*Retrieved November 16, 2015, http://www.bilgiportal.com/v1/idx/19/2480/Gvenlik/makale/Virs-solucan-ve-Truva-at-nedir.html

[6] Graham, James & Howard, Richard. (2010). *Cyber Security Essentials.* Boca Raton, Florida, ABD: Auerbach Publications. pp.198, 199.

[7] Güner, Reyhan. (2015, March 28). İlk BilgisayarSolucanınınMucidi: Robert Morris. *SiberBülten*. Retrieved January 14, 2016,https://siberbulten.com/efsane-hackerlar/ilk-bilgisayar-solucaninin-mucidi-robert-morris/

[8] Kissel, Richard (Ed.). (2011). Glossary of Key Information Security Terms,*National Institute of Standards and Technology[2011]*. Retrieved October 23, 2015, http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

[9] Laboratory of Cryptography and System Security (CrySyS). (2011, November 14). *Duqu: A Stuxnet-like malware found in the wild*. Retrieved January 09, 2016, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

[10] Rosen, Eric S. (1981, January). Vulnerabilities of network control protocols: an example, *Software Engineering Notes, Vol 6(1)*, pp. 6-8. Retrieved January 14, 2016, https://tools.ietf.org/html/rfc789

[11] Selvan, Sabari. (2012, May 28). *Flame worm - Iran uncovers Stuxnet-style malware*. Retrieved January 09, 2016, http://www.ehackingnews.com/2012/05/flame-worm-iran-uncovers-stuxnet-style.html

[12] Seybert, Heidi. (2011). "Internet use in households and by individuals in 2011", *European Commission Eurostat Industry, trade and services Statistics in focus, 66/2011*. Retrieved January 14, 2016, http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/publication?p_product_code=KS-SF-11-066

[13] UlusalSiberGüvenlikStratejisive 2013-2014 EylemPlanı. (20Haziran 2013). *ResmiGazete*, Sayı 2013/4890. Retrieved October 23, 2015, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

[14] UlusalSiberOlaylaraMüdahaleMerkezi (USOM). (2014, July) *SiberGüvenliğeGirişveTemelKavramlar*. p.11. Retrieved October 23, 2015, https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf

★★★