HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Inkovics Ferenc
ferenc.inkovics@gmail.com

THE CYBERSPACE AND ITS RISKS

Absztrakt/Abstract

Ma már egyre mindennaposabb dologgá válik, hogy egy több ezer kilométer távolságban levő barátainkkal video-telefonálunk, elektronikus levelet küldünk a világ legtávolabbi pontjára, és az is hogy pillanatok alatt érjük el az amerikai „New York Times" az orosz „Pravda", az ausztrál „Financial Review" vagy a japán „The Asahi Shimbun" legfrissebb híreit, videóit. A technika e remek vívmánya azonban csodálatos és szörnyű dolgokra is használható, lehet fegyver is. Az őserdőben is rengeteg veszély leselkedik az oda betévedőkre. Nekünk is számos veszéllyel kell szembe néznünk, amikor belépünk a kibertér dzsungelébe. E cikk ezekre a kockázatokra és veszélyekre hívja fel a figyelmet.

Today video-phoning with our friends who are 1000s km-s far away, sending an e-mail to a far corner of the world, and reading the news or watching the videos of the American "New York Times", the Russian "Pravda", the Australian "Financial Review" or the Japan "The Asahi Shimbun" in no time is becoming more common. However, this great novelty of the technique can be used for doing wonderful and horrible things. This can be a weapon, too. There is also a lot of danger in the rain forest for those who are getting into. We also have to face a lot of dangers when entering the jungle of cyberspace. This article calls the attention to these risks and dangers.

Kulcsszavak/Keywords: *kibertér, kibertámadás, kiberterrorizmus, kiberbűnözés, veszély, kockázat ~ cyberspace, cyber terrorism, cyber attack, cyber crime, danger, risk*

INTRODUCTION

During the past months and decades we could read articles, listen radio broadcasts and watch television programs that dealt with issues of information space, cyberspace and their concept, together with their positive effects on our society and economy. However, the continuous technical development has brought innovations on an other field, too. New technologies are used by "bad guys", as well. In the field of military technology there is a well known fact: once one of the opponents has new weapons or defending methods, later another one does. Of course, they can use it against each other. Similar parallelism can be found in the field of information and communication technology, too. The technical development sometimes helps the attackers of information systems, and later it helps the defenders. In consequence of this parallelism, the sentence that was said in 2008 by Bruce Schneier, one of the most known security experts in the world, is quite relevant: "Technology helps – both the attacker and defender, actually, although in different ways – but security is fundamentally about people [1]". Although this sentence is not expressly about information technology, but technical sciences. Perhaps it is more timely than several years ago. As it turns out from the quoted sentence, according to Mr. Schneier people stands in the center of security. This is justified because of the following. Although we can achieve security by using technical means and methods, these means and methods serve us, namely the people. This is valid, because even though we achieve security mostly with technical devices and methods, they serve the interest of us, i.e. they serve the interest of people, and they exist for us. We, humans, strive to maintain security around us.

Unfortunately the global security balance is not permanent. This article tries to demonstrate the risks and threats in the cyberspace and those who are responsible these risks and threats.

CYBER CRIME, CYBER TERRORISM, CYBER WAR

If somebody pronounce the expression cyberspace, at that moment most people knows he thinks of the on-line space that separated from physical world, and where computers communicate with each other. The word cyberspace originates from the Greek word kyber that means sail or navigate. And in fact, it means space where sailing is possible [2].

In the case of cyberspace, as most concepts in computer and information technology, unfortunately there is no unified, objective definition. According to Wikipedia, The Free Encyclopedia, cyberspace is a medium of computer networks, in which online communication takes place [3]. According to Merriam-Webster Online Dictionary cyberspace is the on-line world of computer networks and especially the Internet [4]. According to The Tech Terms Computer Dictionary the word cyberspace is used to describe the virtual world of computers [5]. First, William Gibson used the expression cyberspace in his novel Neuromancer written in 1984. According to Gibson, cyberspace is a matrix in which individuals, companies and businesses can have interactive contact with the information, and even they can also trade with it.

Analyzing any of the concepts, we always talk about an on-line space that is separated from the physical world and where computers can communicate with each other.

The usage and application of the means of information and communication technology have reached a level where these means are reckoned to be some kind of public utility. The reason of this reckoning is the nature of the service [6]. In certain ways parallelism can be drawn between water network, electricity network, phone network etc. and public utility of information technology. Just think, today it is natural that clear water comes from the tap, and

how uncomfortable if there is no water or tap water is dirty. But nobody says anything when clear water comes from the tap, because it is expected. However, when the service is not the expected service any more, then people can also say unwanted words. Similar parallelism is exist in the power supply, as it is also natural for people that there is power supply which is necessary for the operation of most of our technical devices. The situation is the same with the internet access, too. If internet service is not appropriate and/or the bandwidth is less than contracted, at the best, people or companies can have inconveniences, at the worst, serious problems can happen. It can be annoying when the bandwidth of broadband internet subscription that contracted for 20-50 MBPS[1] is reduced to one tenth of the original bandwidth, and only the minimal service is accessible. In such a case our favorite on-line HD video or news program can not be downloaded in no time. It can happen we have to wait for several minutes. But it is also possible poor quality of service prevent making video calls to our relatives living far away. A reduced bandwidth is a problem for companies, as well. Bad quality internet service or reduced bandwidth can inhibit a video conference meeting between managers working on different sites. This inhibition can cause a commercial disadvantage against competitors. Imagine situations, when banks cannot serve their clients, customers cannot use their debit or credit cards in shops, or visas for traveling cannot be issued to a country where people would like to travel for business or pleasure purposes because of malfunctioning or low-capacity communication lines. These were only examples and much worse situations can happen.

The importance of information systems is supported by the amount of damage that can be caused in the life of a country because of certain dysfunctional information systems. The malfunction of information systems can occur for many reasons: e.g. inadequate planning, disproportionately increased load or intentional tort. Crime has also appeared in cyberspace, and criminals are quite active. As our world is becoming more and more centralized more and more dangers and risks are lurking on us. In cyberspace fraud, identity theft, child porno and even cyber attacks are also becoming more common. Authorities try to oppose it, but the lack of law and the continuous technical development create serious barriers in managing the problems [7].

OECD (Organization for Economic Cooperation and Development) also recognized this risk and prepared a report about cyber security and cyber war. This report is a part of "Future Global Shocks" series of reports [8]. According to the authors using the correct terms are essential. Spying or espionage, hacker activities and cyber war should not be considered to the same concept. Unfortunately the media and even some governmental officials often tend to wash up the boundaries between different concepts and definitions. The attackers and defenders of the cyberspace use the same information and communication technology, probably this fact also play a part in the confusion of definitions. As a result of the fact that the same technology are used for both the attackers and defenders, a strong tension has now been developed between cyber attack and cyber defense. Thanks to this tension and the accelerated technical development, new attack and defense methods come to light day by day.

Using the correct terms helps us in understanding and keeping up the pace with the results of this technical progress in an easier way. Therefore it is important to clarify such definitions as cyber war, cyber terrorism, cyber crime and cyber vandalism. Bruce Schneier defined these 4 concepts in his book "Schneier on Security" [1]:

1. Cyber war—Warfare in cyberspace. This includes warfare attacks against a nation's military — forcing critical communications channels to fail, for example — and attacks against the civilian population.

[1] MBPS: MegBitPerSecond, one unit for measuring the bandwidth and data transfer rate, 1 MBPS = 1024 KBPS (KiloBitPerSecond) = 1048576 BPS (BitPerSecond)

2. Cyber terrorism — The use of cyberspace to commit terrorist acts. An example might be hacking into a computer system to cause a nuclear power plant to melt down, a dam to open, or two airplanes to collide. In one of his Crypto-Gram essays, he also discussed how realistic the cyber terrorism threat is.
3. Cyber crime — Crime in cyberspace. This includes much of what we've already experienced: theft of intellectual property, extortion based on the threat of DDOS attacks, fraud based on identity theft, and so on.
4. Cyber vandalism — The script kiddies who deface websites for fun are technically criminals, but he thinks of them more as vandals or hooligans. They're like the kids who spray-paint buses: in it more for the thrill than anything else.

As some other concept of information technology, these 4 concepts have no exact definitions as well. The definitions of Bruce Schneier need to be extended, these definitions are now too general.

In connection with cyber war we have to note: war always means an armed struggle or conflict between 2 or more parties. But we must not forget the following important factors of war:

1. the opponents are known
2. wars begin with a declaration of war or a clear hostility
3. wars end with peace treaty or cease fire agreement

The cyber war definition of Bruce Schneier has to be extended with these amendments.

Comparing Schneier's definition of cyber terrorism to other definitions, the definition of Dorothy E. Denning defines the main point of cyber terrorism more specifically. Here is her definition:

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

For defining the word cyber crime, the concept of company TechTarget is more appropriate: cyber crime is a term for any illegal activity that uses a computer as its primary means of commission. The U.S. Department of Justice expands this definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence.[9]

Practically Mr Schneier doesn't define the word cyber vandalism, just refers to its implementers. Therefore use this definition: cyber vandalism is a vandalism which is carried out by the means of information technology. This definition now has returned its essence.

The above mentioned definitions correspond to their traditionally/originally defined pairs but all these are given in the cyberspace.

In cyberspace there is only a little example for cyber war. But in the 2008 Russian-Gregorian war besides the armed conflict, the opposing countries fought an intensive information battle despite the low coverage or limited facilities of their internet network infrastructure [10].

During the past decades there are 3 events that are said to be cyber wars [11], but since the other party is not known or the perpetrator can only be assumed, therefore these should be pigeonholed into the category of cyber terrorism or cyber crime. Here they are:

1. 1999 – Moonlight Maze: several computer systems of the USA (including The Pentagon, NASA, etc.) have been attacked. The suspected attacker was Russia but Russia denied any involvement.
2. 2003 – Titan Rain: The USA was again the attacked country, but at this time China was supposed to be in the background.
3. 2007 – Estonia: Estonia was attacked and Russia was supposed to be responsible for this attack.

The essence of cyber terrorism is the same as the essence of terrorism: creating terror. However, at this time the tool is not a bomb, nor an aircraft but a combination of means and methods of information technology. The place where they are used isn't an airport or a railway station but the cyberspace. An attack may significantly affect airports or railway stations, and so can cause large damages to the traffic and public transport. In the beginning most of the pirates of the cyberspace originate from the USA or Russia. However, today Chinese hackers have significant knowledge, as well [12].

Fortunately, there was only a little example for cyber war and cyber terrorism. However, we have heard news about several cases or incidents where cyber vandalism or cyber crime was reported. The reason of cyber vandalism can be envy, political activism or simply desire to abuse, however, primarily there are power or financial reasons in the background of cyber crime. If we reserve a small amount of time to read about cyber attacks and cyber crimes, we can easily find published studies and analyzes in the subject. Such studies and analyzes reveal that only a few of us realized the importance of cyber crime, and most people doesn't proceed with enough care on its own digital security. For cyber criminals it is not a problem to track or monitor the on-line or off-line activities of people. We are exposed to several risks during on-line shopping, using social media, and even during on-line banking. Computers, or phones (especially smart phones) can be infected by an on-line virus, identities or bank accounts of people can be stolen, or people can be victims of credit or debit card fraud. On our planet 65 out of 100 internet users have become a victim of some kind of cyber crime. This high figure shows the popularity of the cyber crime. Don't forget: opportunity makes the thief, and most of the internet users haven't done all necessary steps for their protection. One fifth of the internet users don't have properly protected computers. However, level of security can be increased significantly by continuous installation of updates and applying anti-virus and firewall appliances and/or programs [13].

There are problems with the protection of WIFI network or our home, as well. Unfortunately even today there are some people who do not protect their WIFI networks. Some people have WEP[2] protection instead of the WPA[3], the strongest known encryption for WIFI networks. But WEP is easily breakable, even up to a minute [14]. The minimized protection or the lack of it makes it easier for unauthorized intruders to get the information they need, such as eBay accounts and passwords, hotel booking information and/or other electronic identifications of people.

This way it can be figured out easily when we aren't at home. Furthermore, having the necessary information criminals can buy valuable articles and goods on-line on behalf of other people. Moreover criminals can do worse actions than aforementioned ones. They can use internet access of other people for launching cyber attacks, and when police officers will looking for the origin of the attack, they will find the owner of the internet subscription. Of course there is no perfect protection, but it is time to focus a little bit more on our own security. It is also a step to a better protection, if the name of the WIFI network doesn't clearly show that who owns it.

---

[2] WEP: Wired Equivalent Privacy, this is an algorithm for encrypting wireless computer networks

[3] WPA: Wi-Fi Protected Access, this is also an algorithm for encrypting wireless computer networks, but this one is more secure to WEP

The massive expansion of social networking sites is a great benefit to those who deal with phishing. It is proved, as most of the phishing attacks target the users of social networking sites. In January 2010 a little bit more than 8% of the phishing attacks occurred on social networking sites. By December 2010 this figure has been multiplied nearly tenfold [15].

Cyber war, cyber terrorism, cyber crime and cyber vandalism are carried out by the methods of cyber attack. Only the targets of the different attacks and the rate of destruction differ. In order to minimize the damages in the cyberspace, it is necessary to place more and more emphasis on cyber protection. It is the interest of all of us that the balance of power is not shifted in favor of the attackers. According to Peter Sommer and Ian Brown, the authors of the above mentioned OECD report, the nature of cyber war and cyber attacks was not global but local so far, and the chance for developing a global cyber war is very little. They also point out that governments should be prepared for intentional and unintentional interferences. They also highlight the fact that economic and financial stability, epidemics, diseases cause orders of magnitude higher problem to the world. But the authors emphasize that as the development of cyber protection primarily is the task of infrastructure operators and the government therefore governments have to make proper preparations, as well [8]. Clear and well-formulated strategies are necessary for a successful preparation. But why don't we talk about a huge Action Plan? The answer is simple: because even though information systems are based on information and communication technology, they use different techniques. Different ways of protection have to be developed against DDoS (Distributed Denial of Service) attacks, phishing or a DEMP weapon (Direct Electro- Magnetic Pulse weapon). As different data, information and preparation is necessary for fighting against each kind of attacks, various threats should not be treated as a single risk or danger.

As an answer for cyber incidents that occur all over the world, more and more countries create a cyber center or take steps forward in the field of cyber protection and cyber attack:

1. United Kingdom: In March 2010 UK launched its cyber center that has to deal with not only tasks connecting to the cyber protection of the island country but is capable to implement counter-attacks, as well. This center has adequate human and financial resources and will be able to fight with cyber attackers regardless of whether they are internal or external attackers [16].
2. Austria: weaknesses, areas of a possible attack, consequences of a possible attack for both the population and the army are assessed in the Austrian cyberspace [17]
3. Germany: The goal of the Bundeswehr is similar. The country should not be unprotected and unprepared in a cyber war. The attacks against the chancery office and ministries justify the need of the Department of Information and Computer Network Operations ("Abteilung Informations- und Computernetzwerkoperationen") which primarily serves defense purposes [18].
4. Russia: According to the events happened in Russian-Georgian war, it can be assumed that Russia created cyber unit for not only protection purposes but attack purposes, as well.
5. The USA: The more developed a country's internet network is the more vulnerable the country is in the cyberspace. The United States recognized its own vulnerability in the cyberspace, therefore a Cyber Command has been created [19].
6. EU (European Union): EU aims for a closer cooperation with the USA in the field of cyber protection. For the sake of the cause, common cyber protection mechanism will be developed and joint field-exercises will be held in cyberspace [20]. Cyber Europe 2010 was the 1st field-exercises in the cyberspace for European Union, and thanks to the agreement on cyber protection, there will be more in the pipeline.

Unfortunately the task of the units dealing with cyber protection is more complicated because of the fact that in a cyber attack it is difficult to prove the identity of the perpetrator,

because the attackers are able to hide behind IP addresses of a country or even several countries. Attackers have the advantage that a cyber war can be initiated from "home", and dropping cyber attackers off behind the enemy lines is not necessary. And cyber terrorism, cyber crime and cyber vandalism are also not tied to a location. The cyber attackers don't have to jump a fence, and cyber criminals don't have to wear ski mask or possess a real gun when breaking into a bank.

INFORMATION TERRORISM AND CYBER TERRORISM

Terrorist threats and actions performed through information infrastructures are called information terrorism. Information terrorism can use information infrastructures, but it can also be directed against them. In the course of information terrorism, attackers can apply low-tech[4] and high-tech[5] means and methods. But in the course of cyber terrorism, that usually starts from cyberspace and exerts negative impact on computer networks, mainly high-tech means and techniques are applied [21].

Low-tech means and techniques should not be underrated, because using them at the right place and at the right time they can cause not only terror but also extensive damage for both information societies and institutions. Attacking a bank, a power-company or a mobile network operator with high-tech means and methods is not as frightening as a low-tech terror attack can be where dozens of people die. However, the consequences of a high-tech attack can be very significant damages and sometimes can claim more casualties than a conventional attack. Just think how the technical means are integrated into our life, and do not forget these means cannot work without power. Today more and more people use bank and credit cards. But what happens when a bank is the target of a cyber terrorism. People might face some problems: e.g. paying with credit and debit cards is not possible; no cash withdrawal from ATM-s, no money transactions, etc. The governments which apply the techniques of modern information and communication technology have to face the threats of cyber terrorism, too. Even our country, Hungary, also belongs to these countries. "Digital Mohács", a scenario for a cyber attack against Hungary, created in 2009 reviews such information systems in Hungary that are mostly exposed the risk of such attacks. This scenario tries to call the attention to the cyber terrorism by reviewing the different systems that can be attacked [10].

THE ATTACKERS

Technology is continuously developing, and occasionally it brings radical and sudden changes in the methods of communicating between people and information management (e.g. social networking sites). Because of these changes it is not enough only getting a knowledge or degree in Information Technology. It is necessary to keep pace with development continuously, because the determining technologies of future are not known. Innovations appear almost daily in information and communication technology (including means and solutions), and so do the attack and defense methods, as well.

We are all aware of that cyber attacks are performed by no normal users. Nine out of ten cases attackers are armed with significant physical and intellectual skills. Review those people who possess the skills and knowledge for performing a cyber attack [23]:

---

[4] High-tech: this term refers to the most advanced technology that is currently available. This advanced technology is at the cutting edge [22].

[5] Low-tech: refers to the simple unsophisticated technology, also used for more modern techniques and design that are no longer at cutting edge [22].

1. Hackers: IT professionals who are well versed in the operation of certain information systems, and with the help of internet they can access such data and rights that is inaccessible for average users. Based in their knowledge, hackers can be differentiated as white-hat or black-hat hackers. White-hat hackers use their knowledge to call the attention for security problems. Ethical hackers and penetration testers are typical white-hat hackers. However, black-hat hackers look for not only the weak points of IT systems, but they take the advantage of the known weak points for various reasons (e.g.: to make money, to possess given data, etc.). Industrial spies, people who brake into systems for stealing data of people, companies and/or governments, are typical black-hat hackers.
2. Hacktivists: a group of people generally with political motivation, who are activists and hackers at the same time. In order to support their goals they are able to crack web sites, steal data or even launch cyber attacks, too.
3. Cyber criminals: IT professionals with high level IT knowledge, who use their skills for implementing crimes. For this activity they use malwares (malicious software) and known security vulnerabilities that are unknown for the defenders.
4. Industrial spies: these people are not the products of the information society, industrial espionage has existed since the beginning of the industrialization. Industrial spies acquire and sell the innovations of competitors and data of new developments stored on computers.
5. Internal experts and external contractors: nowadays many organizations and companies use internal experts and external contractors. These professionals often possess rights for accessing such information that can be used for committing serious abuses. They can do unethical and unlawful activities but it is not inevitable.
6. Terrorists: Those people who use the novelties of technology for creating terror during terror attacks. These attacks often result in serious human casualties. Terrorists can use the technical novelties for their soft[6] or hard[7] activities.
7. Jerks: such people who cause damage in the cyberspace without any reason and meaning, alike vandals in streets. They are capable to modify websites, erase data, etc.
8.

A question may arise: Why aren't crackers, phreaks, phishers on the list? For this question here is the answer below. Hackers are often mistaken with crackers. However, crackers deal with no on-line security vulnerabilities, but cracking copy protection and removing other restrictions (e.g brake shareware programs for having no time limitations in usage or enabling more or even full functionality). After cracking, crackers often have income from selling multiplied pirate copies of this manipulated software. Phreaks obtained financial benefits by hacking phone lines. They had the technical skills for manipulating the computers in telephone exchanges, so they could control phone lines, get data of calls, tap somebody's phone conversation, start/finish phone calls, etc. Nowadays there are only a few phreaks, and because of financial gain phreaks belong to the group of cyber criminals. Phishers draw profit from the credulity of people. Their motivation is also financial gain; therefore they are cyber criminals, too.

Previously, attackers of cyberspace were reviewed. In order to compete attackers successfully, people has to think in a way as if they were one of them. For acquiring the skills

[6] Soft activities of Terrorists: activities that are used for building terrorist cell, communicating between terrorist cells, or preparing and planning terrorist attacks (e.g.: propaganda, recruitment, gathering information, etc.).

[7] Hard activities of Terrorists: violent and/or disruptive activities that are carried out with means of information technology

and knowledge what attackers have, people has to train themselves. Several organizations, companies can be found on internet that offer education packs, trainings for defending or even implementing attacks in cyberspace. Some of these trainings:

1. CEH (Certified Ethical Hacker)
2. LPT (Licensed Penetration Tester)
3. CCISO (Certified Chief Information Security Officer)
4. ENSA (EC Council Network Security Administrator)
5. CHFI (Computer Hacking Forensic Investigator)

Reading the above list of trainings that are accessible to almost everybody, a question may arise, whether the hackers of the future are trained in these trainings. Unfortunately the risk, that the trained person will misuse its skills, is given. The fact that somebody can hack into a computer system and can modify it or influence its operation significantly does not mean that he will do it illegally.

METHODS OF ATTACK

It cannot be declared that an applied technical solution can only be used for offensive or defensive operations in cyberspace. It also cannot be declared that a given technique of information and communication technology can only be used for civilian or military purposes. This is due to that we all use the novelties of cyberspace. The same operating systems, network protocols, encryption algorithms, security software, etc. are used by attackers, defenders, civilians and soldiers. Thanks to the same facts, the above discussed expressions (cyber war, cyber crime, cyber terrorism and cyber vandalism) are difficult to distinguish.

In general it can can be stated on used methods that they attack sensitive areas of given information systems and take advantage of the weaknesses of these information systems. However, the previously mentioned parallelism (multipurpose use) creates significant tension between techniques and methods of defense and attacks. This tension is rooted in the following question: what an organization (army, cyber center etc,) that was created to ensure protection should do when a vulnerability of a system is revealed. Bruce Schneier has mentioned 2 choices in his book 'Schneier on Security' [1]. If they do not take any further steps (no not let the developers and operators of information systems and computers know about this vulnerability), they can reap benefits from this vulnerability during the defense. However, if this vulnerability was known by the attackers then all the other systems would be endangered. If this organization responsible for protection indicates the manufacturer to arrange the correction, then not only the information systems of good guys will be more protected but information systems of bad guys, as well. If an organization designed to protect doesn't do anything, it will leave the bad guys and also the goods guys insecure. Enforcing the public interest it is suggested to call the attention of the developers and manufacturers of it in order to take the necessary steps to correct it. The correction will give an adversary a less opening even if this protection can also protect the attackers.

Every week tens of new attack methods appear. Due to this, cyber attacks are diverse and it would take a lot of time to list all various forms of cyber attacks. Therefore it doesn't make sense to list of them, but grouping does. Cyber attacks can be grouped as follows [23]:

1. Cyber attacks carried out with MalWare (Malicious softWare): malware is a program that carries out changes in the computers without the permission and authorization of the user. It can damage computers, or the threat of damage exists. Malware are created for various purposes: e.g. spying, sinning, vandalism or just for pranks. Malware can be grouped into 2 main subgroups: program-type malware and text-type malware. Viruses, worms, virus development kits, trojan and back door programs, virus droppers, spy programs, key-loggers and other malicious software

are program-type malware. Spams, hoaxes, fake winning letters, phishing and other text type malicious contents are text-type malware. The possible damages caused by malware are:

- resources are reserved
- data loss, data modification, hardware error can occur
- removing them needs time, energy, or even further resources.

2. Attack methods mostly using Malware: this includes any attack that does not use malware, or attacks that uses malware alongside additional complements. Denial of service (DoS), distributed denial of service (DDoS – CodeRed, nimda), spamming, viral spamming (e.g love-letter or 'you are tagged on a video' letter) flooding (TCP SYNpacket), a man in the middle attack, SMTP backdoor command attack, IP address spoofing attack, IP fragmentation attack, TCP Session High jacking, information leakage attack, JavaScript applet attack, cross sire scripting (XSS) and much more are such attacks.
3. Social engineering: When an attacker use social engineering he doesn't attack a computer or computer network directly, but users with sufficient rights for given computers and/or computer networks. In order to achieve the objectives attackers steal, cheat, blackmail, or simply mislead people. They obtain the necessary access codes, passwords, user names or probably even the desired data with such methods. Unfortunately, the user is the weakest chain in the security of information systems, and attackers take the advantage of this vulnerability.

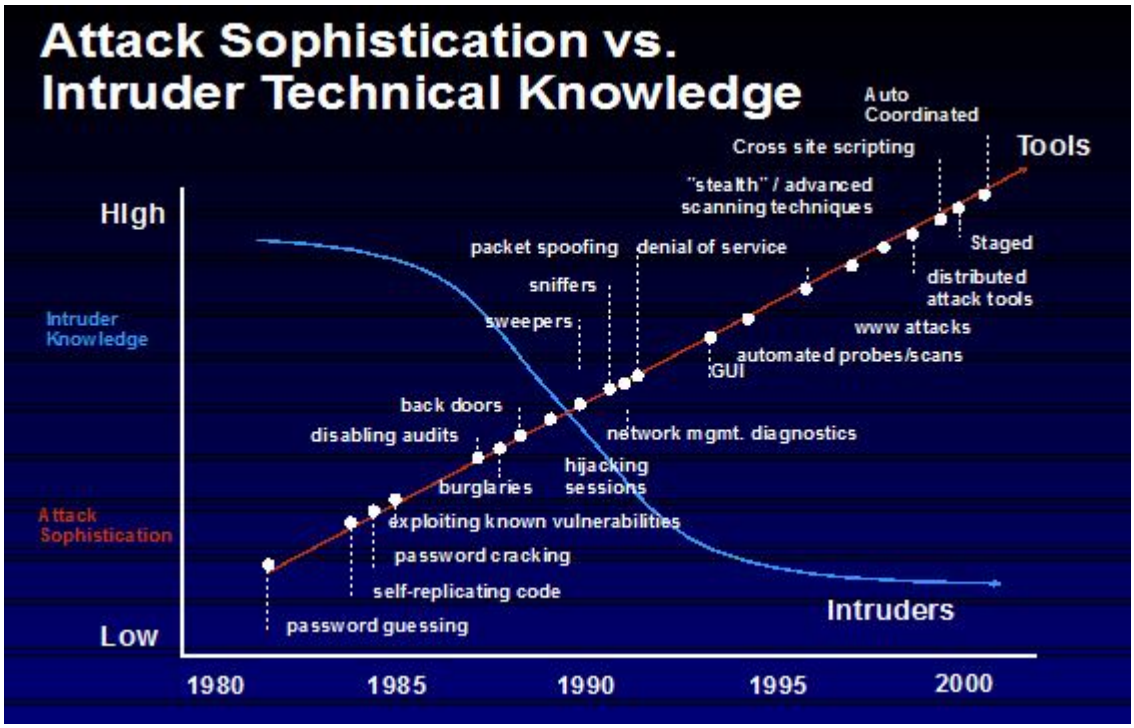
From the 1st group of the cyber attacks (cyber attacks carried out with malware) the following program-type malware should be mentioned in more detail [23]:

1. Viruses and worms: these are the most known malicious software. The relationship between then is that each multiplies and so they can spread. The difference between them is in the way of multiplying. Viruses add their own program code to an existing program. Worms do not need host program, they are able to reproduce themselves. Copies of worms are partly stored on data storage devices and partly are sent through the network to which the infected computer is connected.
2. Virus development kits: these alone are not contagious and not malicious, but even people with minimal technical skills and knowledge can also produce viruses.
3. Trojan and backdoor programs: For trojan programs it is generally true that besides fake or real functions, they are able to perform unwanted operations without the knowledge, will and/or authorization of the user. These operations can cause data modification, data deletion, but even creating new data, as well. Backdoor programs operate without the knowledge, will and/or authorization of the user, but their task to try opening back-doors in information systems without authorization. Opening back-doors can provide administrator rights to the attackers.
4. Virus droppers and injectors: these can be compared to living virus hosts that are immune to the virus, they infect others but themselves are not ill. Droppers and injectors create copies of viruses and send them to the network. They themselves are not malicious and not able to do self-reproduction.
5. Spy programs (spyware): these can also get into the computer systems without the knowledge, will and/or authorization of the user. There they hide and monitor the events of the information system. Spy programs prepare and send reports about these events and even stored data.
6. Key-loggers: essentially these are a special type of spyware that monitor the keystrokes on the keyboard. Passwords, identifiers, user names, bank card data can be collected and sent with using key-logger.

From the 1st group of the cyber attacks (cyber attacks carried out with malware) the following text-type malware should be mentioned in more detail [23]:

1. Spam: spam is an unsolicited letter that arrives in our postbox. Spams have a direct effect including the consumption of computer and network resources and the cost of human time that is needed for sorting them. They arrive in an amount that requires significant resources to handle them (e.g. sending and receiving them needs a significant part of the bandwidth, storing them needs large storage capacity, and separating expected letters from spams is time-consuming and may need extra resources).
2. Hoax: hoax is a special type of spam. In general it contains deceptions, fake alarms (e.g. awareness of a new virus, spam or attached file). It encourages the reader to send it to its friends. A series of chain letters can be launched with this method. Handling a big amount of hoaxes can cause similar effect to spams (e.g. a big part of the available resources would be used).
3. Fake winning letters (especially news with Holland or Spanish lottery), Nigerian fraud letters: these are spams that exploit the credulity of people and encourage people to transfer small amount of money. These letters ask for money for helping children with cancer, but they can offer access to bigger fortunes against sending a small amount of money to a given bank account. Blocked bank accounts of African businessmen, lottery winnings, etc can be mentioned as larger amount in these letters. The requested amount can be only a couple US dollars up to hundreds of US dollars.
4. Phishing: these are spams that also exploit the credulity of people. Usually they cheat people out of data and information. But at this time people give the data and information by courtesy, because they are abused. The method is very simple. Apparently people get a letter from their bank. For some reason they ask people to check data with them. For this check there is a link to a webpage that takes people to a fake webpage of their bank. When people enter their data (login name, password, other identifiers) this website saves them into a database. Later, on behalf of people the saved data can be used for electronic purchases (e-shopping), electronic transfers, etc. Banks try to combat against similar frauds by informing their clients about these frauds. Unfortunately a lot of people fell for the trick, therefore phishing still cause billions of EURO damages. The URL of the fake bank is very similar to the real URL (e.g. real URL: www.raiffeisen.hu, rake URL: www.raifeissen.hu). These kinds of fraud can be avoided with more care of reading and thinking.
5. Phraming: this is a kind of development of phishing. The IP address of the fake webpage is written in the host files of computers. Thus the name resolution is carried out with the help of the host file instead of the primarily set DNS server, therefore the user believes in opening the real URL.

Information systems should be prepared for attacks. Of course, there is no 100% protection, but it is necessary to do our best. Increasing the preparedness of an information system against attacks should be the task of both the installers and operators of the information system. Unfortunately developers, installers, and operators often do not modify default settings: e.g. default settings are used for installing then for operating IT systems, functions that are not used are left on, and important updates and patches are often not installed in time [24]. For the interest of the security of information systems it is important that, from time to time at least the basic or medium level security checks should be done, thus information systems can be protected against most of the attack methods.



1. figure. Attack Sophistication vs. Intruder Technical Knowledge [25]

Most of the organizations and individuals are not fully aware of the dangers that are lurking on them. Furthermore, they don't have sufficient resources and competent technical skills for fencing off the different attacks, reducing the possible caused damage, or restoring information systems. It is a satisfaction to know that Hungarian government realized the necessity of increasing the consciousness on information and network security, therefore increasing of the national consciousness on information security is set as one the tasks of National Network Security Center (former CERT Hungary) in an edict [26]. It is a gratifying news that Hewlett Packard (HP) and several multinational companies will join to raise this awareness, by promoting the knowledge on security of information technology [27].

The information technology is continuously developing and at the same time he methods used for attacking are developing, too. As a result of this trend (development), intruders are able to carry out more and more complex and sophisticated attacks with less and less technical skills (see Figure 1). DoS[8] attacks are at the top of the list of the threats that are lurking on people in cyberspace. Because of the above mentioned technical deficiencies and lack of resources, the defense against them is limited. As a result of this limitation probably this leadership will remain in the near future, too [28].

SUMMARY

IT Professionals see little chance of an independent cyber war, but there is example for applying cyber attacks in the past, and it is reasonable that cyber attacks will be used in order to prepare or complement a war that is fought with conventional weapons. An infrastructure of a state can be impaired with cyber attacks and attacks against information infrastructures at a much smaller investment of financial and other assets. Successful cyber attacks can perform the task that can be carried out conventionally with applying airplanes and bombs together with orders of magnitudes higher financial resources.

[8] DoS: Denial of Service, a form of an attack in cyberspace that makes computers and computer networks unavailable for their users.

The appreciation of cyber crime has become very high, therefore importance of cyber attacks should be underrated. There is no on-line system that can be fully protected, and people cannot achieve the desired technical benefits with closed offline systems.

Recruiting staff in the black market for performing cyber attacks is quiet inexpensive: e.g. in Russia where students, who are rather poor but well-educated and skilled in information technology, are selling their knowledge. These students offer access to servers dominated by them for 20-30 US dollars, and now you can purchase a 1-day long DDoS attack for 80 US dollars [29].

The first hacker attack was back in 1960. As a result of this attack, a telephone exchange operated abnormally. Today the technical development makes it possible that a nuclear power station can be attacked by cyber attacks. It is possible to fight a war or launch political or other types of attacks without bombers, tanks, guns and bullets. Actually perpetrators can be hired to cause devastating effects without spatial constraints. Because of the globalization of information and communication systems, the vulnerability of these systems is greatly increased. Moreover, operations, attacks, malfunctions of an information system can effect the operation of other information systems. Therefore in the future priority attention should also be used on maintaining the power balance between attack and defense including applied means, methods and techniques of information and communication technology.

References

[1] Bruce Schneier: Schneier on Security, Wiley Publishing, Inc., Indianapolis, 2008, ISBN: 978-0-470-39535-6

[2] Mészáros Rezső: A kibertér társadalom-földrajzi megközelítése, Magyar Tudomány folyóirat, 2001 júliusi szám. http://epa.oszk.hu/00700/00775/00032/769-779.html (downloaded: 2011.06.16)

[3] Cyberspace http://en.wikipedia.org/wiki/Cyberspace (downloaded: 2011.06.16)

[4] Cyberspace http://mw4.merriam-webster.com/dictionary/cyberspace (downloaded: 2011.06.16)

[5] Cyberspace http://www.techterms.com/definition/cyberspace (downloaded: 2011.06.16)

[6] Informatika mint közmű http://computerworld.hu/informatika-mint-kozmu.html (downloaded: 2011.06.19)

[7] What are cyberspace crimes http://www.ehow.com/about_4596810_what-cyberspace-crimes.html (downloaded: 2012.05.23)

[8] Reducing Systemic Cybersecurity Risk http://www.oecd.org/dataoecd/3/42/46894657.pdf (downloaded: 2011.06.19)

[9] Cybercrime http://searchsecurity.techtarget.com/definition/cybercrime (downloaded: 2012.06.02)

[10] Dr. Kovács László, Krasznay Csaba: „Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen” NEMZET ÉS BIZTONSÁG III:(1) pp. 44-56. (2010)

[11] Kiberháború az orosz észt viszony kapcsán
http://hacktivity.hu/portal/archivum/folia/2007/Hacktivity_Muha_Lajos_2007.pdf
(downloaded: 2010.05.17)

[12] Hekkertámadások a Távol-Keletről
www.hadmernok.hu/2010_4_serege.pdf (downloaded: 2011.06.13)

[13] Kiberbűnözés
http://www.lfmagazin.hu/tudomany-es-technika/kiberbunozes (downloaded:
2011.06.20)

[14] WEP: Cracked in 60 seconds
http://www.wi-fiplanet.com/news/article.php/3670601 (downloaded: 2012.05.23)

[15] Kettészakadt a kiberbűnözés
http://computerworld.hu/ketteszakadt-a-kiberbunozes-20110516.html
(downloaded: 2011.06.20)

[16] Márciusban indul a brit kibervédelmi központ
http://www.sg.hu/cikkek/70984/marciusban_indul_a_brit_kibervedelmi_kozpont
(downloaded: 2011.05.29)

[17] Kibervédelem osztrák módra
http://www.sg.hu/cikkek/70425/kibervedelem_osztrak_modra (downloaded:
2011.05.29)

[18] Kiberháborús egységet hoz létre a Bundeswehr
http://www.sg.hu/cikkek/65536/kiberhaborus_egyseget_hoz_letre_a_bundeswehr
(downloaded: 2011.05.29)

[19] Kiberparancsnokságot állít fel a Pentagon
http://www.sg.hu/cikkek/68205/kiberparancsnoksagot_allit_fel_a_pentagon
(downloaded: 2011.05.29)

[20] Közös kibervédelmi gyakorlatot tervez az EU és az USA
http://www.sg.hu/cikkek/81411/kozos_kibervedelmi_gyakorlatot_tervez_az_eu_es_az_
usa (downloaded: 2011.06.03)

[21] Muha Lajos (szerk.): Az informatikai biztonság kézikönyve.: Informatikai biztonsági tanácsadó A-tól Z-ig., Budapest: Verlag Dashöfer Szakkiadó, 2005. 3210 p., ISBN:963 9313 12 2

[22] Cyber terrorizmus
www.zmne.hu/dokisk/hadtud/terror/lekt_Kovacs_Laszlo.pdf (downloaded: 2011.06.12)

[23] Dr. Kovács László: Kritikus Információs Infrastruktúrák – egyetemi jegyzet, Budapest: ZMNE kiadó, 2007

[24] Akadálymentesítse weboldalát
http://www.itbusiness.hu/Fooldal/main_flash_banner/liferay_symposium.html
(downloaded: 2012.05.30)

[25] Shimeall, Tim: Cyberterrorism
http://www.cert.org/archive/ppt/cyberterror.ppt (downloaded: 2012.05.30)

[26] 223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatás biztonságáról

[27] A kibertámadások korai észlelése
http://computerworld.hu/kibertamadasok-korai-eszlelese-20120118.html
(downloaded: 2012.06.02)

[28] Védekezés a DoS támadásokkal szemben
http://tech.cert-hungary.hu/sites/default/files/uploads/nhbk_vedekezes_a_dos_tamadasokkal_szemben.pdf (downloaded: 2012.05.02)

[29] Inside the Russian Cyber-Underground
http://www.eweek.com/c/a/Security/Inside-the-Russian-CyberUnderground-517933/
(downloaded: 2011.06.21)