Zsolt Dr. HAIG

CLASSIFICATION OF INFORMATION BASED ATTACKS[1]

A cikk osztályozza az információalapú támadásokat, amelyeket a támadók egy komplex információs támadás során alkalmazhatnak az infokommunikációs rendszerek ellen. A szerző bemutatja a számítógép-hálózatok elleni támadások, az elektronikai alapú felderítés és az elektronikai támadás fontosabb jellegzetességeit.

In this article the information based attacks will be classified that could be used during a complex information attack by the attackers against the info communications systems. The author presents the main features of the computer network attacks, electronic based intelligence and electronic attack.

INTRODUCTION

The information society highly depends on the advanced, but strongly vulnerable integrated information infrastructures, such as telecommunications networks and computer networks, which are operated in the information environment. One of the essential points of the information society's vulnerability follows from the feature of information infrastructures - particularly the critical information infrastructures – which are able to ensure the operation of the society. The global-scale interconnected networks - which are a result of rapid spread of info communications technology - are exposed to a greater threat than ever before. Sources, tools and methods of these threats can be extremely variable and may occur at various levels.

Considering the tendencies of information attacks, we can declare that regarding the targets the attacks can be divided into two groups, namely:

- threats against the computer networks and
- threats against other info communications systems.

It would be practical to group the threats according to this; however, this categorization is not exact enough. In most cases, the targets are complex, overlap each other, that is, a system could contain multiple components (such as computers, telecommunication devices, navigation equipment, etc.). This overlapping essentially comes from the convergence of information technology.

According to another principle of classification we can categorize the information attacks based on the methods of threats. Accordingly we may talk about the following methods of attack:

- computer network attack;
- electronic-based intelligence;
- electronic attack.

In the following we are going to introduce the methods of attack according to the above mentioned classification.

COMPUTER NETWORK ATTACK

The computer network attack essentially has a dual purpose. On one hand the detection of computer networks exploitation and access to data, on the other hand, the influence and destruction of data and information, and the obstruction and restriction of the networks' function.

The computer network exploitation means an intrusion into the computer systems, which allows access to the data stored in databases, and using them for own aims. The detection of the network ensures:

- mapping the structure of computer networks;
- exploration of its hierarchical and operational specialties based on their traffic features;
- registration of the content of the data flow used on the network, and

[1] The paper has been supported by the Bolyai János Research Scholarship of the Hungarian Academy of Science

- gathering of data stored in the database, and using them for their own aims.

In the course of this activity the system is not compromised, and the data stored in it is not modified or deleted. However, should the data get into wrong hands that could cause a significant loss to the one enduring the attack. So in the course of this attack the confidentiality of data stored in the system gets injured. In addition, considering that in possession of the obtained data, the system becomes easier to be attacked, so this activity is as serious of a threat, as the attack itself that causes real damage.

The attack causing real and clearly detectable damage is an intrusion to the other party's computer systems or networks. As a result the data stored in databases could be damaged, modified, manipulated or made inaccessible; or rather the system or network itself is compromised by the attack. This means a deceptive, confusing activity in the computer networks and the exchange, destruction of programs and data contents. As a result of this, the vulnerability of data stored in the system increases, and the access to services is reduced.

The computer network attack tools include various malicious softwares (Malware). Malware is the collective noun for softwares, which have a common feature that they access the system without the user's permission. All software is classified as malicious, which doesn't ensure proper operation of a computer system or network.

Nowadays these types of software are constantly growing, so their clear categorization is almost impossible. The most well-known of these programs are: viruses, worms, Trojan programs, root kits, backdoor programs, keyloggers, spam proxies, spywares and adwares, etc. Non-program types of Malwares include spams, hoaxes and phishing. These, in the form of text information mean danger to the system and its users.

Each Malware has its own special function. These include e.g. disrupting of the system operation, data stealing or taking control over the computer, etc. The Malwares can modify the programs and data, reserve resources, cause hardware errors. Their removal may need suitable devices, time and energy, and special skills in some cases.

The different methods of attack, combined with the tools, mentioned above allow the intrusion to the network, the obstruction and degradation of its operation, and accessing data. An attacker with a simple attack hardly ever has access to a remote computer and its data. Usually, the attackers have to combine several methods and tools of attacks, to avoid all the security procedures that are applied to ensure the security of networks. There are a lot of methods to attack the networks (such as Sniffing, Spoofing, Session Hijacking, Spamming, Man-in-the-Middle Attack, Denial-of-Service (DoS), Attack, Distributed DoS, etc.). Thus, the attackers only need the proficiency to combine the tools of attack with the appropriate methods.

The protection of the information systems is often high-level. Therefore it can't be penetrate to these systems with technical tools in all cases. This problem was resolved by a very effective form of intelligence, which is called Social Engineering. The data regarding the network's weak points, the most important passwords, etc. are gathered by misleading, extortion, fraud, or threatening from the person who manages those or who has access to them. This activity has a significant role in helping the attacker to avoid the various security solutions, such as firewalls or intrusion detection systems.

ELECTRONIC BASED INTELLIGENCE

Electronic based intelligence usually has a dual purpose. On the one hand, *access to data* stored and transmitted in info communication systems and *using them*. On the other hand, *obtaining the target information* that is necessary for the execution of an effective attack. The efficiency of attack against the critical information infrastructure depends on whether the attacker knows the target's physical location, its structural composition, hardware and software elements, data traffic and weak points, as well as the operators and users of the given information system or network. [1] Nowadays, various methods and technical devices can be used for this purpose, which are significantly increase and multiply the limits of human perception. The intelligence devices are capable to collect data in the full frequency spectrum, send them to a data fusion intelligence centre, where valuable information can be obtained from them. [2]

The modern *signal intelligence (SIGINT) devices* provide detection, interception, location of various active electronic emitters (radios, radars, etc.) and evaluation of their technical characteristics in the full radiofrequency spectrum. Now days SIGINT systems can also detect the modern low probability of intercept (LPI) electronic devices (e.g. frequency hopping and spread spectrum systems). The new generation receivers are able to detect radiation and determine the emitter's location that is necessary for the execution of a potential physical or electronic attack.

Most of the electronic based intelligence devices are available and can be purchased on the market. These equipments could obtain the most important data from all information system which use**s** electromagnetic emitter.

The detection of the passive (non-radiating) electronic devices can be solved in other way. One method, for example, can be the detection of different wired communication traffic by technical devices. These devices, which obtain information by induction method using the generated magnetic field in the cables, can also be purchased on the trade market. [1]

The usage of most of the modern electronic based intelligence devices doesn't endanger the soldiers' life. These devices can be installed on various platforms (e.g. unmanned aerial vehicles – UAV) or *unattended ground sensors* (UGS).

Unattended ground sensors contain several sensor technologies, deployed at the area of operation, detecting, classifying and reporting target information via wireless links to a remote control centre. UGS systems use small, low cost and robust sensors expected to last in the field for weeks or even months. Other systems are providing communications, processing, as well as target verification and identification services.

UGS systems utilize a combination of detectors, including seismic detectors, used to identify ground vibration caused by vehicles. Magnetic detectors monitor movement of metal objects such as weapons or vehicles. Acoustic sensors are used to detect targets by specific acoustic signatures (e.g. noise of engine) while passive infrared sensors detect movements of objects in a narrow field of view. [3] Generally the detected sensor data is transmitted to a data-fusion intelligence centre.

ELECTRONIC ATTACK

The electronic devices operating in the electromagnetic environment combined with certain natural phenomena (e.g. propagation of electromagnetic wave) are often sources of harmful (deliberate and unintended) electromagnetic emissions. These are called the *electromagnetic environmental effects.*

The electromagnetic environmental effects include the following:

- electrostatic discharges;
- high-energy electromagnetic pulses which are resulted by nuclear explosions above the ground
- high powered pulses of directed energy devices;
- deliberate and unintended electronic interferences;
- hazards of electromagnetic radiation to personnel and
- natural phenomena effects of lightning and precipitation static.

As it is seen from the list many types of electromagnetic environmental effects can be generated by electronic attack. By using electromagnetic and other directed energies the electronic attack can:

- reduce the adversaries' effectiveness of info communication systems;
- reduce opportunities of command and control,
- make its important electronic devices out of order;
- mislead its information systems.

In all cases, some kind of radiating, reradiating or reflecting device is used for the electronic attack for obstruction, restriction or destruction of the function of targets.

According to the military: „electronic attack is the subdivision of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability.” [4] Electronic attack is actions taken to prevent or reduce an adversary’s effective use of the electromagnetic spectrum.

The components of the electronic attack are the following:

- electronic jamming;
- electronic deception and
- electronic neutralisation.

„*Electronic jamming* is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy’s effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy’s combat capability.” [4]

Electronic jamming can be carried out from a number of platforms using a wide variety of techniques and devices. The electronic jamming can be accomplished with active (radiating or reradiating jamming signal) and passive (reflecting electromagnetic waves) devices.

Electronic interferences are such electromagnetic radiations, which

- distort the signals, and information in the receivers;
- make the radio communications, data transfer and target acquisition difficult and impossible;
- reduce the range of the intelligence devices and preciseness of the automated command and control systems;
- deceive the operators.

Special emitters, so called electronic jammers (radar jammers, radio jammers, navigation system jammers, etc.) or reflecting devices are used for electronic jamming. These devices can generally be found at the electronic warfare troops. However, simpler designed devices with limited capabilities can be used by non-regular forces, paramilitary organizations or terrorists. [1]

Electronic Jamming is detectable and hence can be classified and located by an adversary. In addition, it can cause unintentional interference in friendly electronic systems.

„Electronic deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy’s combat capability.” [4]

The primary use of electronic deception is for platform or area defence against non-communications systems by using a variety of techniques including:

- flares, repeaters and false target generators to produce deceptive transmissions;
- imitative techniques to replace the emission of radars, navigational aids or communication devices;
- chaff and other reflectors to create false targets;
- radar-absorbent material, protective paints and coatings to reduce radar cross-sections;
- other energy-absorbing or dissipating material, protective paints and coatings to reduce Infra-Red (IR) signatures. [5]

The conditions of the effective electronic deception are on the one hand, that the other party has to sense the misleading signals; on the other hand, these activities have to look real so the deception couldn’t be discovered. In the interest of this, the electronic deception requires detailed and thorough planning, coordination and implementation.

Electronic neutralisation is the deliberate use of electromagnetic and other directed energy to either temporarily or permanently damage adversary devices.

Electromagnetic pulse (EMP) weapons can generate sufficient electromagnetic energy on a target to render it, its electronics (microprocessors, microelectronic circuit), or both are useless. These devices can be used as bombs (E-bomb), that if detonated in a certain altitude, they could destroy all electronic equipment operating in a nearly circle shaped area. An alternative manner of application is when a high energy radiofrequency weapon (HERF) is directed to a given target, damage the equipment with high energy impulsions. The benefit of the latter application is that whereas the E-bomb is applicable only one time, the HERF device can be deployed many times.

EMP technology is potentially non-lethal, but is still highly destructive. An E-bomb attack would leave buildings standing and spare lives, but it could damage and destroy different electronic devices, particularly the elements of information infrastructures.

Today, the increasing danger is that these high-energy devices may be produced at home from components, which can be purchased at a shop only for $ 1000. Of course, these have smaller power, but if they are deployed in a well-placed location, their power is sufficient to partially or totally degrade critical information systems. [1] States - which have modern information systems – know this well. Perhaps therefore, shortly after the attacks on the Twin Towers former U.S. President Bush has ordered the development of a strategy for the critical infrastructures protection.

It should be mentioned that one of the most threatening information risk is the *cyber terrorism*, or in a broader sense the *information terrorism*. Of course this is not a new tool or method, rather than an organised form of information attacks, which more dangerous than some hackers' or separated groups' computer network attack. Its importance is that these attacks are carried out in political aims, and in order to achieve their goals exploit the information technology development of developed countries.

Examined the current situation of information terrorism, could be stated that the terrorist organisations use the information technology – including first of all the Internet – for almost exclusively propaganda aims, but for the moment they can't apply it for attacking info communications systems. The last years the terrorist groups and other radical organisations more and more forcefully, openly and well trained use the internet for publishing their ideas, training, keeping in touch, recruiting, and last but not least psychological warfare.

Nowadays the terrorist organisations have more and more computer experts. But in many cases they have not enough technical background and motivation to conduct a comprehensive information attack against a country. However, we must not forget about that there is continuous possibility of an attack. As soon as the potential political benefits of this attack will be recognised, and for example an intrusion to the information system of a bank or an information attack against an electric power supply system will be evaluated equivalent with a bomb assassination, the terrorists will expectedly make a big effort to carry out these types of attacks.

The damage caused by the terrorism in the information dimension can be measured accurately, and it becomes more and more equivalent with conventional attacks that are more difficult to execute and require deep organisation. According to the international organizations the numbers of targets which are threatened by information terror attacks are increasing, since the Internet has become worldwide. Therefore, in the near future we have to face that terrorists in the interest of their goals, will exploit the methods and devices of information attack, and they will start complex information attacks using all repertoire of information warfare.

CONCLUSIONS

Based on the introduced classification it can be concluded that the critical information infrastructures of the information society could be attacked by many ways. The targets of these attacks are not only the computer networks, but all types of info communications systems and devices of the information infrastructures. If these attacks are carried out against a country's information infrastructure in a planned, coordinated and synchronized way and according to the principles of information warfare, it could cause serious damages to the function of the systems, and could affect the society's operational processes.

Derived from the complexity of attacks, the protection must be complex too. It is not enough to prepare the info communications systems for **a** single type of attack, but the system of complex information security must be developed. Both the government and defence sphere are responsible for this process.

Keywords: Computer network attack; electronic based intelligence; electronic attack, electronic jamming; malware; cyber terrorism

Kulcsszavak: Számítógép-hálózati támadás; elektronikai alapú felderítés; elektronikai támadás, elektronikai zavarás; rosszindulatú programok; cyber terrorizmus

REFERENCES

[1] Haig, Zsolt, Kovács László, Makkay Imre, Seebauer Imre, Vass, Sándor, Ványa László: *Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban.* Tanulmány. MEH Informatikai Kormánybiztosság, 2002.

[2] Ványa László: *Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre.* PhD-értekezés. ZMNE, Budapest. 2002.

[3] Unattended Ground Sensors. http://defense-update.com/features/du-1-06/feature-ugs.htm (downloaded: 01. august 2009.)

[4] Joint Publication 3-13.1 US Joint Electronic Warfare Doctrine, 25. January 2007.

[5] AJP-01(B) Allied Joint Doctrine September, 2000.