HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

KORNÉL KONDÁS[1]

Roles of the Action Control Centre in case of cyber attack against the IT system controlling the electronic ankle monitors

A Tevékenység Irányítási Központ szerepe az elektronikus lábbilincsek működését felügyelő informatikai rendszer ellen történő támadás esetén

Abstract

In this article the author presents the tasks of the Action Control Centre in case of attack against the IT system which controls the electronic monitoring device of individuals whose personal liberty is restricted. Furthermore, the author sketches what kind of immediate and long term measures should be done by the Police if there is a mechanic or cyber attack against this IT system.

Keywords: Individual whose personal liberty is restricted, person in house detention, prohibition of leaving residence, electronic ankle monitor, IT system, cyber attack

Absztrakt

A szerző a cikkben bemutatja a Tevékenység Irányítási Központ feladatát az elektronikus lábbilincset viselő, személyi szabadságukban korlátozott személyek ellenőrzésére szolgáló technikai eszközt felügyelő informatikai rendszer ellen bekövetkezett támadás esetén. Vázolja, hogy ha a számítógépes rendszer ellen akár mechanikus, akár kiber támadást követnek el, abban az esetben a Rendőrségnek milyen azonnali és hosszú távú intézkedéseket kell foganatosítania.

Kulcsszavak: Személyi szabadságában korlátozott személy, házi őrizetes, lakhelyelhagyási tilalom, elektronikus lábbilincs, informatikai rendszer, kiber támadás

---

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz hallgató - National University of Public Service, Doctoral School of Military Sciences, PhD student, E-mail: kondaskornel@gmail.com, ORCID: 0000-0002-9666-7971

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

INTRODUCTION

As a result of the strict criminal policy of the Hungarian government and the unrelenting pre-trial detention practice of the criminal courts the capacity expansion program of the law enforcement (l.e.) is unable to keep the step. Presently prisons operate with 143 per cent average saturation, while in case of pre-trial detainees the situation is even worse, as since 2013, when as a result of the modification of the law on criminal procedures the upper time limit of the pre-trial detention was abolished.

Since 15 May 2013 the police can monitor the movements of the suspects placed under home detention with an electronic tracking device.

This solution is more cost efficient, ensures constant supervision, and minimizes the escape risks. It can be said it works, however it is still a question whether the legislatures and the IT professionals installing and operating the IT system which runs the electronic ankle monitor has considered how the IT system reacts in case of a cyber attack – how the supervision of the persons placed under the criminal procedure whose personal freedom is restricted shall be executed – in case of such attack? The purpose of the article is to highlight, what immediate actions are to be done by the employees of the Action Control Centre being in charge in case of such an attack.

APPEARANCE OF ELECTONIC ANKLE MONITORS IN HUNGARY

The court may impose various coercive measures to proceed successfully a prosecution against the suspects. Out of the coercive measures prohibition of leaving residence and the home detention are those which limit personal freedom, and where the court may order the application of electronic ankle monitor.

Prohibition against leaving residence: By the 1998 year Act XIX. 137. § (1) Law on Criminal Procedure *„The prohibition of leaving residence restricts the freedom of movement and the free selection of residence of the person under sentence; the person under the prohibition against leaving residence may not leave the designated territory, area without permission, may not change his place of residence and domicile.” [1]*

Home detention: *By the 1998 year Act XIX. 138.* §[407] (1)[408] *Law on Criminal Procedure „The home detention restricts the freedom of movement and the free selection of residence of the person under sentence. In case of home detention order the person under sentence may leave the domicile designated by the court only for the purposes specified in the court decision, in particular in order to ensure the normal needs of daily life or for the purposes of health treatment for the time and distance as prescribed in the resolution (travel purposes).*” [1]

In certain cases the court may designate movement zone or routes, eg. in case the suspect needs to take medical treatment regularly, or has appear at court, or if nobody can do the shopping for him. The court may also order the police to monitor the compliance with the home detention rules by using technical devices tracking the movements of the suspect.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

The electronic tracking device colloquially mentioned as ankle monitor is applied in Hungary since 15 May 2013. Before 1 January 2014 it could be applied only with the prior consent of the suspect, but since then its application can be ordered without such consent. The court may request the support of the police to the technical survey of the area. The public protection specialists and the IT professionals identify whether the basic conditions are provided for the operation of the device, eg. if there's connection to public electricity, eligible signal strength to ensure that the device sends signals to the observatory office.

In mid-November, this year, cca. 409 suspects in custody were recorded out of whom 283 person, i.e. 69 per cent of them were monitored by the police through electronic tracking device. By the application of the device the all-day supervision is ensured in a way that it does not require live force, therefore more police officers can be commanded to public domains increasing the population's subjective comfort of security. Based on data from 2 years ago the monitoring of home detention costs half million forint less when electronic ankle monitor is applied compared to the costs of the 24 hour constant police supervision. [2]

The attachable device (see picture) is able to supervise the suspect in two steps. In the first round there is an internal unit in the designated domicile, which sends a preliminary signal to a computer at the county headquarters' operations control centre in case the detainee leaves the designated area. In such case the attached device signals by vibration to the suspect as well. Then the tracking device switches to GPS signalling within a few seconds by which the police can precisely identify the actual position of the detainee and can follow his movements. Concurrently with the alarm a police officer can be commanded to the spot, so we immediately start to search the suspect violating the rules of home detention. The chain part of the device when fitted forms circuit. If somebody tries to break or damage it, the device immediately signals to the control centre even if the battery of the attached tracking device is running out.

By this supervising method the risk of escape is much lower than it used to be when the colleagues checked recurrently on case by case basis whether the suspects keep the rules of the coercive measures. Presently 22 home detainees are escaping, but there's none whose supervision was ordered by the court via using an electronic tracking device. [2]

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

Figure 1: Electronic tracking device [3]

RELATIONSHIP BETWEEN THE INFORMATION OPERATIONS AND THE NEW TYPES OF SECURITY CHALLENGES

Information operations *INFOOPS*[2]:Mean the activities coordinated within the physical ,information-based and cognitive dimension, which are able to influence the decision makers by affecting the opposite partner's information, information-based processes and info communication systems to achieve their political and military objectives simultaneously protecting and effectively utilizing the similar own processes and systems. The information operations are the integrating, synchronizing and coordinating operations between the applied information capabilities with a purpose to achieve and maintain information superiority on every level (political, military [strategic, operational and tactical], economic, cultural etc.) and at all time (peace, crisis, war). [4]

In order to reach its objectives the information operations realises its effects on physical, information and cognitive (human perception and consciousness) dimensions.

[2] Information Operations

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

As a result of the appearance of information era, information environment, information society and the digital, precision and network militaries, the operating areas and ranges of military operations expanded further. Besides the land-, sea-, air- and cosmic theatre of war another range of warfare appeared what is called information war scene. The information battlefield is actually the operating environment of information operations, which are interpreted in three dimensions (physical, information and cognitive dimension). [5]

The functioning of the information society fundamentally depends on that numerous information systems are using the internet. Therefore the security of internet is – being a critical structure itself – is essential from nation-security point of view, which should be taken into account in the course of organizing the protection of critical information infrastructures. Furthermore, in a country numerous systems organised into network operate which are not connected to the Internet. The vast majority of the management systems of law enforcement and military organisations operate in isolated, closed networks and are not connected directly to the Internet.

If the intention is to decrease the enemy's attacking capabilities, these networks has to be reached in the cyberspace via electronic routes within the entire frequency range. That is why such way of protection, the electronic ankle monitor - chosen as main subject of my article - and the related supervisory system connected into such network is of utmost importance.

As the cyber superiority is interpreted as part of the information superiority its achievement can be realized through the cyber warfare continued within the information operations.

The network warfare within the information dimension is nothing else than the whole of operations continued within the cyberspace, in other words cyber warfare. [5]

CATEGORISATION OF ATTACK METHODS

The cyberspace attack can be done in direct and indirect ways. In the course of a direct cyberspace attack the attacking party on one hand gets into the communication systems and computer-networks bypassing the different information security rules, accessing the different databases etc. and thereby getting useful information. On the other hand destroys, alters, deletes, etc. information important for the opposing party by confusing signs, misleading information, introducing malwares. In the course of an indirect attack, the attacking party makes available to the other party its own misleading information, or continues misleading network activity, and misleads as well as influences the situation-assessment, or overloads the system with false data, resulting that the network access shall be obstructed.

The purpose of the cyberspace protection is to keep up the access to the information, information-based processes within the own network based information systems, and to ensure the effective usage of these systems in times of peace, crisis or conflicts equally. The protection of the network based information systems ensures the maintaining of our management capabilities by exploiting the possibilities dwelling in our own systems, and

hinders enemies to intervene into our information systems. Minimizes the vulnerability of our own information systems and the mutual confusions between them.

Important element of the cyber warfare is the computer-network warfare, which also means attacking and defensive capabilities.

The *attacking of the computer networks* on one hand means the mapping, exploring of networks, on the other hand means actual attack. Possible purposes: disablement of computer systems, emerging unreliable operation (by generating data errors), data theft (for purpose of making money or selling), unauthorized use, or related data collection, impersonation both on the user side both in respect of the service provision, information collection for intelligence (via interception, by watching system operation), entering false data into the system, or threats, blackmail, or applying the above mentioned to these actions.

A computer network attack tools include a variety of malware, malicious programs, which are called Malware4. The Malware[3] is collective name for software of common features that get into the system without having been authorized so by the specific user. All software classified as malicious, which is not ensuring the proper functioning of a computer system or network.

Today, these types and variety software are constantly widened, so clear categorization is almost impossible. The best known of these programs: viruses, software worms, trojans, rootkits, browser-deteriorators, back door (backdoor) programs, keyloggers, spam proxies, spyware and adware programs, and the line goes on. The non-program types of malware are among others the spams, hoaxes, and the phishing, which pose a threat in the form of text information to the system and to its user. The malicious software can modify the programs, can occupy resources, manipulate data, can result hardware failure, while their removal require proper tools, time and energy, and in some cases require special expertise. [5]

The attacker rarely can access a remote computer and its data in a simple, one-step process. A wide variety of methods exist to a network attack, (eg. Sniffing, Spoofing, Session Hijacking, Spamming, Man-in-the-Middle Attack and the most commonly used Distributed Denial-of-Service / DDoS / Attack) so the attacker just needs to have the right expertise to combine the attacking tools with the appropriate methods. [5]

BASICS OF PROTECTING COMPUTER NETWORKS

Protection means the conservation of a private computer-network, that is implemented in order to prevent, making it difficult for an attacker to acquire the data and information stored in the databases, and to intentionally destroy or to make inoperable the information system.

[3] Malicious Software

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

The implementation of the protection of computer networks can be passive and active. Passive protection methods and devices can be: firewalls, virus scanners, access control, intrusion detection and adaptive responses.

Joint and complex application of listed methods and tools of computer network protection used in cyber warfare increases the security of the networks that is IT security. Confidentiality, privacy (protection against interception) integrity (protection against modification of data), and availability can be ensured in case of application of effective protection of data stored in the computer system.

One of the most widely accepted design principle of a secure network construction and implementation of protection also applied in practice is the so-called *PreDeCo methodology* that implements the development of a protection based on three interdependent and complementary controls. These are as follows:

- Preventive controls;
- Detective, ie. recognition and controls
- Corrective, ie. avoidance controls .[6]

The protection is not only physical and technical protection, but also the provision of appropriate logistical means and trained professional.

The *preventive controls* ensure the prevention of security incidents, the elimination of vulnerabilities forming basis to attacks and setting up barriers to their exploitation. One of the most effective preventive method is the vulnerability assessment, in the course of which experts specialized for this purpose carry out a comprehensive and in-depth investigation on the computer network.

The *detective controls* mean the collecting, authentic recording and displaying of the attack traces both before, during and after the incident occurred. Detecting breaking-in as quickly as possible is one of its most important elements, so as to limit the adverse effects (such as a virus) to spread and allows to begin the recovery activities s soon as possible.

The *corrective controls* are usually activated after that the attacks occurred, and attempt to eliminate the root cause of security incidents as well as minimize the damage that might occur. The ultimate goal is to restore the defect-free, normal state as soon as possible, which consequently also includes a number of preparatory activities - such as performing backups, creating a disaster recovery plan [6].

ROLES OF OPERATION MANAGEMENT CENTER (OMC)

The OMC staff member in charge, a professional police officer enters the program developed by 3M IT company using the user name and password generated to that specific user (see Figure 2), afterwards he will be able to control on a computer's monitor - designated specifically for this purpose in the centre - the movements of the persons wearing the electronic ankle monitor. The data and information on the persons wearing the electronic ankle monitor is available both in written and electronic forms.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

Figure 2: Front page of the electronic tracing system's IT program (The picture was prepared by the author)

The zone designated for the restricted persons is indicated with green circles and squares in the same colour on the monitor in normal, trouble-free status.

In case of a person restricted by home detention, the judge in its resolution decides about the place is that the person subject to the proceedings may not leave. Usually it is within the administrative borders of the restricted person's residence (Figure 3.)

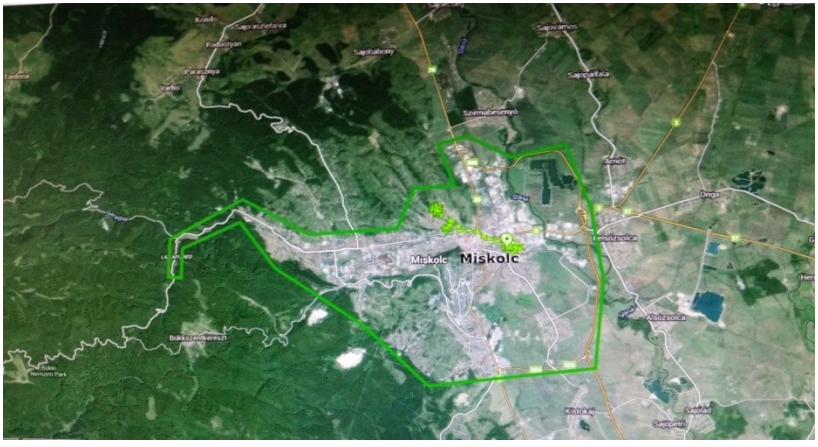

Figure 3. Designated zone for a person wearing an electronic ankle monitor being under prohibition on leaving residence [Picture prepared by the author]

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

In case of a person under prohibition on leaving residence the judge also designates in his resolution on the restriction of personal freedom exactly which is the hour interval on every day when the restricted person is allowed to leave the residence and the joint, fenced territory designated for home detention to ensure the normal everyday needs, or for medical examination or medical treatment, however is not allowed to leave the administrative borders of the municipality (see Figure 4.).

In this case before the arming of the ankle monitor on the restricted person, these data has to be recorded in the IT system.

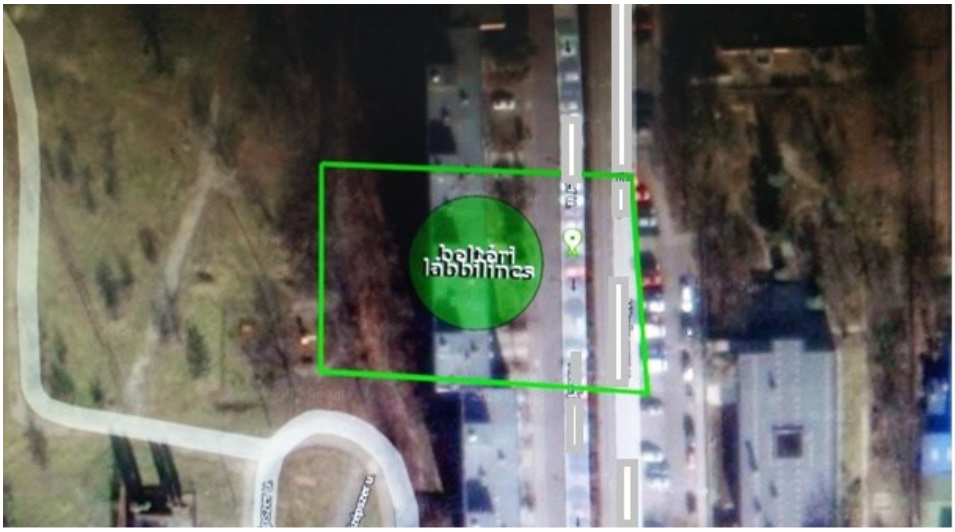

Figure 4: Designated zone for a person wearing the electronic ankle monitor in case of home detention (The picture was prepared by the author)

In case the IT system perceives altering status than the normal status, it indicated it with a signal to the staff working in the centre.

Following such signal alarm the OMC Duty orders the personal checking of the restricted person to be done by a police officer.

If despite that the establishment of protection has been done based on the three interdependent and complementary controls, i.e. the *PreDeCo methodology* and the attack (such as a virus or worm) against the IT system supervising the electronic ankle monitor occurs (against either level), it is immediate task of the Operation Management Centre staff to inform and instruct the police officers to take care of the guarding of the person(s) wearing the ankle monitor.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

In case of a cyber attack the OMC decides in respect of the persons wearing the ankle monitor, also considering the court resolution that two police officers guard the restricted person on the spot constantly or recurrently at specified intervals.

In case the judge announcing the relevant resolution does not prescribe the frequency of restricted person's manned guarding in case of such attack or malfunction of the ankle monitor for any other reasons, in such case the police chief of the public protection department as per the address of the restricted person decides whether the person wearing the ankle monitor is needed to be watched constantly until the system is functioning smoothly again, or it is enough to check recurrently by the public police officers.

Such decision of the department head on the intensity of watching is made by taking into consideration the criminal records, the weight of the ongoing criminal proceedings, and the conduct of the person under the criminal proceedings.

Following the detection of the cyber attack the OMC responsible on duty immediately notifies his superior, the information specialist on duty, as well as the deputy county police chief. Instructions are determined to them not to touch the computer system in question or the computer itself between noticing the attack until the arrival of the IT specialist in order to avoid further injury and for the preservation of data.

Notifies the Hungarian contact person of Geoview, who is responsible for operation of information systems supervising and managing the electronic ankle monitors.

Following the specified notification through the alarm chain a detailed report is to be prepared on the extraordinary case.

Following the collection of necessary information the deputy police chief informs the Main Duty of the ORFK (national police headquarters) about the events and constantly keeps contact with the IT specialist on duty ordered in, who immediately does the necessary IT security measures for the troubleshooting of the attack against the IT system within the frames of *detective control*. The Main Duty of the ORFK immediately has to order – via police officers sent to the spot – the watching of the target person until the troubleshooting of the IT error and the and the smooth restart of the system.

CONCLUSION

In connection with the electrical tracking device the authorities concerned (police, penal institutions, etc.) do not possess presently such a coordinated and unified procedure which would handle satisfactorily the incidentally occurring problems.

It is obvious that solving this issue is becoming more and more urgent as both financially and due to other reasons it is important to form the unified legal background as well as the executive protocol.

Therefore, in case of attacking the IT system that directs and controls the electrical tracking device the public protection forces are taken away from the public area for the to secure the necessary manned guarding.

HADTUDOMÁNYI SZEMLE

2016. IX. évfolyam 3. szám

Within the framework of public procurement tender a foreign company obtained the electrical tracking tender, so presently this company operates the related IT system.

The 3M produced the tracking devices and the related accessories.

In my opinion after finishing the test period the Home Ministry should strive that during production use the Police should be not just the user but the exclusive operator of this IT program.

The Ministry should strive that the user, in the present instance the Police should operate the IT system shown in my article, as they do it in the case of other IT systems.

I mention as an example the Robotzsaru (Robocop) integrated data processing and electric document managing system that is operated and developed by the Police.

I believe it does not give full security in case of a planned Cyber attack, either, but reaction can be quicker, more effective and efficient if all the units needed for the operation of the system are under the direction of one organisation.

In the article I highlighted that after obtaining the public procurement tender the 3M IT company operates the IT system controlling electronic ankle monitors, and the Hungarian Police is only the user.

This situation, in case of a cyber attack results in slower reaction and a huge chaos.

For the Home Ministry it would be more practical to reach that the whole IT system, that controls the electronic ankle monitors, should be integrated in the Robotzsaru Neo IT system, or as a separate unit it should be under the control, direction and operation of the Police.

LITERATURE USED

[1] 1998. évi XIX. törvény, a büntetőeljárásról, http://njt.hu/cgi_bin/njt_doc.cgi?docid=34361.312864, [letöltés ideje: 2015. 12. 06.],

[1] 1998. évi XIX. Act on Crimunal Law, http://njt.hu/cgi_bin/njt_doc.cgi?docid=34361.312864, [letöltés ideje: 2015. 12. 06.],

[2] Harle Szilvia: Biztosabb a házi őrizet lábbilincsel. http://police.hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/biztosabb-a-hazi-orizet-labbilinccsel, [letöltés ideje: 2015. 12. 06.],

[3] Munkácsy Márton: Minden vádlott erre vágyik. http://vs.hu/kozelet/osszes/minden-vadlott-erre-vagyik-0218#!s2 [letöltés ideje: 2015. 12. 06.],

[4] Haig, Zs.: Az információs hadviselés kialakulása, katonai értelmezése. In: Hadtudomány, XXI. évf. 1-2. sz. 2011. pp. 12-28. ISSN 1215-4121 (http://mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_4.pdf [letöltés ideje: 2016. 01. 15.],

[5] Haig, Zs.; Várhegyi, I.: A cybertér és a cyberhadviselés értelmezése. In: Hadtudomány, elektronikus szám pp. 1-12., 2008, ISSN 1215-4121 http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf, [letöltés ideje: 2016. 01. 15.],

[6] Haig, Zs.: Információ - Társadalom - Biztonság. Nemzeti Közszolgálati Egyetem, Budapest 2015. pp. 182-185. ISBN 978-615-5527-08-1