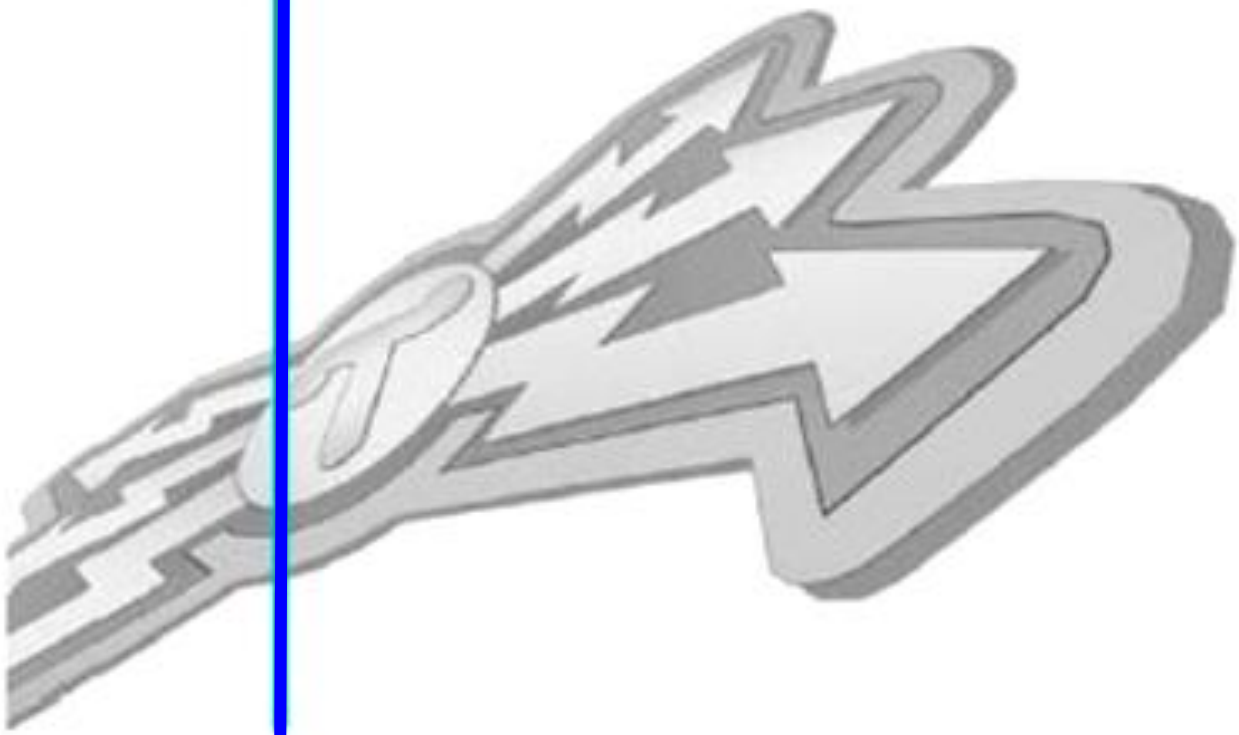
# HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos
kiadványa

# SIGNAL Badge

Professional journal of Signal Departement
at the National University of Public Service

4. évfolyam 1. szám
2013





***2013. június 30.***

# *HÍRVILLÁM*

***a Nemzeti Közszolgálati Egyetem Híradó Tanszék tudományos időszaki kiadványa***

# *SIGNAL BADGE*

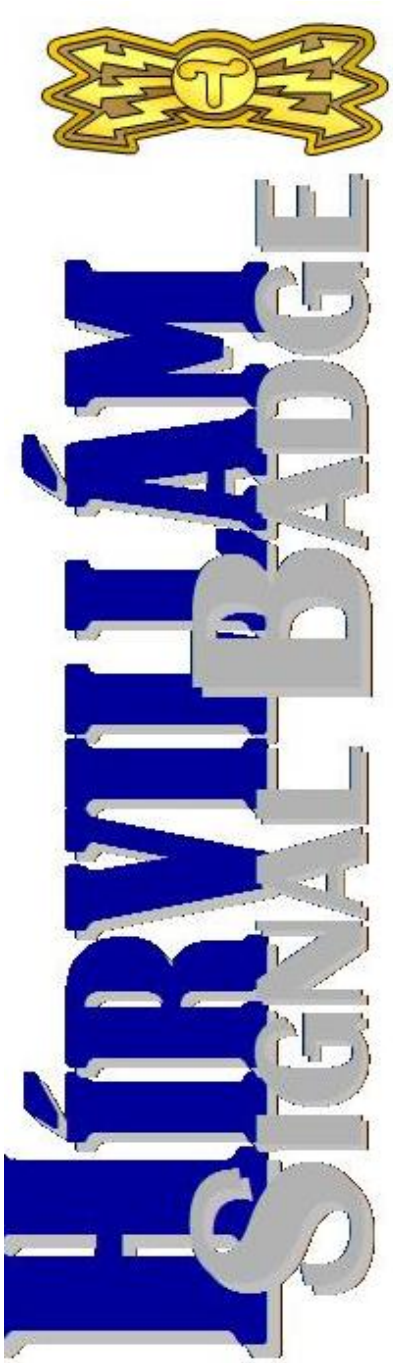
***Professional Journal of the Signal Departement at the National University of Public Service***

***Megjelenik évente két alkalommal***

***Published twice a year***

*4. évfolyam 1. szám*

*Budapest, 2013*




*Felelős kiadó/Editor in Chief*
Dr. Fekete Károly alezredes

*Szerkesztőbizottság/Editorial Board*

*Elnök/Chairman of the Board*
Dr. Pándi Erik r. ezredes

*Tagok/Members*
Dr. Farkas Tibor főhadnagy
Dr. Horváth Zoltán alezredes
Jobbágy Szabolcs százados
Dr. Kerti András alezredes
Prof. Dr. Rajnai Zoltán ezredes
Dr. Szöllősi Sándor ny. őrnagy
Tóth András főhadnagy

*Szerkesztette/Co-ordinating Editor*
Prof. Dr. Rajnai Zoltán ezredes

*HU ISSN 2061-9499*

*NKE Híradó Tanszék*
*1101 Budapest, Hungária krt. 9-11.*
*1581 Budapest, Pf.: 15*
*+36 1 432 9000 (29-110 mellék)*

*hhk_hirado_szakcsoport@uni-nke.hu*

# Tartalomjegyzék

**Köszöntő**

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

Az újesztendő több változást hozott tanszékünk életébe. A tanszékvezetés élén váltás történt, január 1-jei hatállyal Dr. Fekete Károly alezredes úr kapott megbízást oktatási egységünk irányítására.

Birtokba vehettük és kipróbálhattuk az ócsai bázison a három új híradó konténerünket, amelyek sokkal nagyobb mozgásteret biztosítottak a gyakorlatok eredményes és színvonalas végrehajtásához.

Szokásainkhoz híven ismételten megszerveztük Balatonkenesén a Nemzetközi Katonai Információbiztonsági Konferenciát, amelyet eredményesnek értékelték a résztvevők.

Az ERASMUS mobilitási program keretében lehetőségünk volt a harmadéves hallgatói állományunkból részképzés céljából a francia tiszteket képző főiskolán (Ecole Spéciale Militaire de Saint-Cyr) küldenünk egy fő honvéd tisztjelöltet, aki a francia idegenlégió dél-amerikai (Gayana) támaszpontján végrehajtott kiképzésen is eredményesen és tapasztalatokkal gazdagon tért vissza.

Végzős hallgatóink sikeres záróvizsgát tettek, így szeptembertől elfoglalhatják új beosztásukat.

Remélem, hogy egy kellemes nyári kikapcsolódást követően, ősszel, közösségünk ismét folytatja oktatási, kutatási és tudományos munkáját szakmai kultúránk elmélyítése és hírnevünk bővítése érdekében.

Ezen gondolatok jegyében kívánunk kellemes időtöltést az idei év első számának áttekintéséhez!

**Budapest, 2013. június 30.**

**Pándi Erik**
a Szerkesztőbizottság elnöke

***Puskás Béla[1]: The risks of networks complexity***

*"We have built our future upon a capability that we have not learned how to protect! "[2]*

**Abstract**

*"We live in an accelerated world" sounds one of the most common truisms of our age. Comparing to the previous decades this feeling is mainly caused by the dynamic flow of information, fast traffic and transportation means and the globalization, which have been resulted by the booming technical development. Nowadays a journey from Hungary to the United States does not resemble the risky and long-run adventure as it was at the wake of the last century. We also can keep connection with our relatives living on another continent easily. Consequently the people have got closer to each other but at the same time they loosened their connections as well. We live in the virtual space and rarely contact our friends physically. This gap between the individuals and their physical reality is getting so wide, that they don't realize the devastation of environment or the natural disasters.*

## 1. How has the revolutionary electronic development changed our common life?

On the 4th of September in 1837 the inventor, Samuel Morze introduced his electromagnetic telegraph. In order to use it two things were essential. One of them was the Morze alphabet, while the other was the telegraph network itself. At that time the bit rate was "only" at around 5 bit/sec.

In 1876 Alexander Graham Bell had the telephone patented. He also had to establish and operate a network thus he founded the Bell Telephone Company in 1877. Presently it is the well-known American Telephone and Telegraph Co. (AT&T).

Between 1895 and 1901[3], based on James Clerk Maxwell's theory regarding the radio waves, Nikola Tesla, Guglielmo Marconi and Alexander Popov "independently" from each other invented the radiotelegraph.

In 1957 the Soviet Union launched "Sputnik", the first satellite of mankind. As a response, the President of the USA and the Department of Defense founded ARPA[4]

[1] Óbudai Egyetem Ph.D hallgató
[2] George Tenet Former CIA director
[3] In 1901 Marconi introduced his invention for what the Nobel Prize in Physics was awarded to him in 1909-ben. Tesla had already introduced his patent in 1896, while Popov had done so in 1895.
[4] Advanced Research Projects Agency

in 1958. In 1969 an experimental network was established and some others joined in later. Five years earlier Paul Baran had already pointed out: in order to create a minimum risk level communication channel, a partitioned network had to be established instead of the decentralized ones. According to his theory the separated packets used on the Internet had to be sent through individual nodes toward their destinations. Nevertheless his idea was rejected.

**In the Seventies the Internet started its own life.**

More and more institutions joined the network, but not on the way as Baran thought. Instead of the partitioned network a scale-free model was evolved. Due to its extension and rapid development the network couldn't be controlled exclusively. The dominant original goal of an operational network, which is protected against attacks, was not taken into account any more. On the contrary THE INTERNET, which is highly resistant against random errors, was born. It is quite similar to the other networks of our life, such as social networks, networks of the human bodies (nerve system, connections between cells etc.) but it resembles the networks of spreading epidemics and many other else.

*Do we really know what has come to life by the Internet?*

The main problem is that not only the simple common user doesn't understand it, but the IT professionals are not able to clear up the matter as well. We don't have proper knowledge about the network structure and we can't obtain it by our way of thinking. We have to apply the theory of networks. For example documents are being prepared faster on Internet than the search engines can locate and index them. Nowadays they don't even try it and only the 30-40 % of the whole document is mapped even by the most effective search engines. In case of cell phones, especially the smart phones, the situation is quite the same. Their development is so fast that their effect to the hardwares, softwares and the other system can't be measured. Recently 10 % of the Internet data flow is going through mobile networks.

*Then how the USA, NATO or Hungary can prepare themselves for the future IT warfare and how can we protect our critical IT systems against the hackers and terrorists?*

Today the real task is not to understand the occurrences going on the Internet or the Internet itself as an entity. Today when it became a part of our life we have to insert it into our complex world.

The terrorist organizations and other criminal groups sometimes hide secret messages in the chaos of the Internet. They can communicate on the network or exploiting its and the users' weaknesses in order to gain money.

## 2. Against whom do we have to protect our systems?

In most of the cases the attackers are completely unknown. They hide their sources and even their homeland can't be identified properly. Usually not the owners of the concept execute the attack, but they get "innocent" prying men to do the messy job. They provide only the method and pattern of the attack. The communication channels and the logistics background are also given by someone else. They rarely have particular political or economical interests, the attack is simply considered as a challenge or a funny joke. I think that in the future it will be very important to get familiar with the nodes of networks and their connections. We have to realize that the network is not just one-dimensional. The connections and effects of seemingly different social and electronic networks have to be researched. Not only the threatened system has to be examined but all the other linked networks as well. Besides the structures of networks we have to know the structures and the very details of the points (e.g. cells). From this point of view the node cannot be described as a mathematical concept because if today something is considered to be indivisible, tomorrow that can be a set. According to Albert-László Barabási the XXI century is going to be the age of complexity.

## 3. What has to be studied?

The matter is not so simple. Moreover it becomes more complex if we consider another dimension as well: the movements of nodes. The nodes can change continuously and dynamically. If the nodes are the critical infrastructures we have to count on their permanent movements. What has not been a node before that can become so and vice versa. This fact regards the Internet nodes especially.

In order to determine the items of networks we have to deal with complexity as well. Traditional telecommunication, television, informatics etc. networks and their nodes can be mentioned only within the category of electronic networks. All the network items such as routers, switches, modems, hubs, repeaters, transfer medias, servers, data storages, firewalls, adapters and their features influencing the functions of the "system" have to be studied. We also can test the linking "devices", for example printers, monitor-keyboard switches, different input devices, adapter interfaces (smart phones, TV, PDA, GPS etc.), medical equipment, control systems of critical infrastructures such as traffic lamps or airplanes. The device-free surveys concerning the physical and logical network topology, softwares, hardware and software settings, regulators, physical protection, the human factor, environmental

effects are also very interesting of course. The parameters of these factors are quite sophisticated as well but their mutual effects and the quality of their linkage create a complex and immense system.

The Internet has become a complex network. Since it is continuously expanding it can be called scale-free network as well. While studying the network, Barabási and his team noted two facts: the expansion and the popularity.
The scale-free systems are highly resistant to random errors but a targeted attack against the centres can disintegrate them easily. Many vertices, which have only a few edges, can be eliminated but it doesn't have significant effect on the whole network. The destruction of the 80% of Internet nodes leaves the remaining 20% operational nodes working as an intact network.

*There can be another practical question in connection with the networks: Do the malfunctions of devices, eruptions of social conflicts, devastations of biological or chemical disasters happen accidentally?*
The segments of the network can be paralysed by a series of chance events or a well-organized, targeted attack. It is easy to see, that as the drawing of the lottery, the malfunction of a random device is also not able to interfere the operation of the whole scale-free network. What is the probability that I can select that particular node, which has many links or especially important for the connection? In case of the Internet and other similar networks the degree exponent is less than three. Because of this fact there is no threshold, which prevents the network disintegration, when the nodes are removed continuously. However a targeted attack is different. If the nodes with many links are destroyed firstly and it is carried on with the other nodes with less and less links, the network falls apart at a certain threshold. Usually this threshold can be reached quite soon and the attacker doesn't have to destroy too many nodes with many links. Although our system resistant to errors, but the removal of the nodes with many links (e.g. central routers) impose an almost unbearable burden onto the other important nodes and transfer medias. The other items can work for a while, but later packets are going to be lost and congestions are going to emerge, which is very similar to a DoS attack. I am of the opinion that the nodes providing important links can cause similar problems. Although redundant connections are always installed within the systems these connections have smaller capacity. Perhaps if the Internet would have not started to live its own "life" and in 1964 Baran would have succeeded in fulfilling his basic theory concerning the primacy of distributed models, we should not fear of the targeted attacks as much. But there is no point dealing with "what

if...” questions because these processes are irreversible. We could consider the particular “systems” of evolution having similar networks instead. We may owe our life to it.

Consequently the items of the system, their mutual effects and links and the map of the network have to be known properly. I haven’t mentioned the types of graphs, which make the structure of networks more difficult. For instance whether a graph is directed or not does make difference and the network structure modification effect of the relocation of the edge between two vertices can not be neglected either. The complex system can not be protected without this knowledge.

Based on data bases, data storages, documents and images some modern softwares are able to graphically depict the complicated networks and map the complex structures. By the assistance of these softwares false information and connections can be identified, forecasts and algorithms can be prepared. The different aspects (timeline, too many or few but highlighted connections) could reveal hidden, important information.
One of the most important part of the cognition is the obtainment and sorting of information. The concerning data can be obtained from unclassified and classified sources, for instance from the data bases of telecommunication ventures, social sites, Internet providers, manufacturers and many other sources.

**Summary**

If we know our system and lead a safety-conscious life we can avoid such unpleasant events[5], which occurred to the director of MI6, Sir John Sawer. It is obvious, that the problem of mapping the complexity is not only a matter of IT professionals. We have to realize that everything is linked with each other and the physical and logistical networks have mutual effects on each other as well. We can’t be sure that the erased digital information really vanishes.

[5] In 2009 Sir John Sawers’s wife uploaded some family images onto a social site. By these pictures hostile organizations or individuals could obtain sensitive information, which could endanger Sawers and indirectly the MI6.

**References**

Barabási, A.-L. (2003). *Behálózva.* Budapest: Magyar könyvklub.

University of Debrecen. (without date). *Az Internet története.* Download date: 30/09/2012, source: www.inf.unideb.hu: http://www.inf.unideb.hu/~bodai/internet/internet_tortenete.html

Defense Technical Information Center. (2002). *Information Technology Industry Study Final Paper.* Download date: 30/09/2012, source: www.dtic.mil: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA425460

Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., 2010

ELTE. (2006). *Az elektronikus sajtó története*. Download date: 27/09/2012, source: http://mmi.elte.hu: http://mmi.elte.hu/szabadbolcseszet/index.php?option=com_tanelem&id_tanelem=548&tip=0

National Geographic Magyarország. (without date). *Samuel Morse, a távíró feltalálója*. Download date: 28/09/2012, source: www.ng.hu: http://www.ng.hu/Civilizacio/2005/04/Samuel_Morse_a_taviro_feltalaloja

Péter, B. (19/09/2012). A globális IT-rendszerek erdejében. *Computerworld*, page: 4.

***Tamás Horváth[6] - Tibor Kovács[7]: Possibile application of thermal cameras with regard to security engineering***

**Abstract**

*Even professionals of security technology do not meet thermal cameras frequently during their work experience because their usage, not least their cost restrict them for industrial and military use. The human eye is capable of seeing only a very small part of the electro-magnetic spectrum. We are able to pick up neither UV nor IR ranges. High-tech equipment is required for that purpose. Security professionals discover more and more areas for the use of thermal images. It is worth focusing on thermal cameras and their potentials in more detail and settling for the fact that lenses are now possible to be made of metal.*

## 1. Applications of thermal cameras in the field of security technology

Scientifically speaking, thermal convection has been used for thousands of years. In the beginning, as our ancestors did, we, modern people are also getting to accustomed it. Sitting around the open fire or next to the fireplace intending to catch the warm streams looking for the hottest spots indicates we are looking for the thermal convections. Therefore it is worth learning the practical background of what we are doing. Our palms may be used as thermal sensors to find the most comfortable place for us. Today this physical phenomenon is increasingly applied by scientists with absolutely stunning results that security protection systems installed at high-security-risks facilities may benefit from.

## 2. General rewiew

The reason for the first steps of development can easily be given: there were clear-cut military motives: ensuring visibility in darkness without any kind of light and capability of visual observation under low visibility conditions and on battlefields.
The theory of bolometer has been known for years: the measurement of electromagnetic radiations sent by objects and living beings with the help of temperature-dependent resistance. This theory was elaborated by Samuel Pierpont

[6] (Security Engineer, MSc, senior expert) Hungarian Electric Power Company plc tamhorvath@mvm.hu
[7] Docent of Unversity, PhD/CSc Óbuda University kovacs.tibor@bgk.uni-obuda.hu

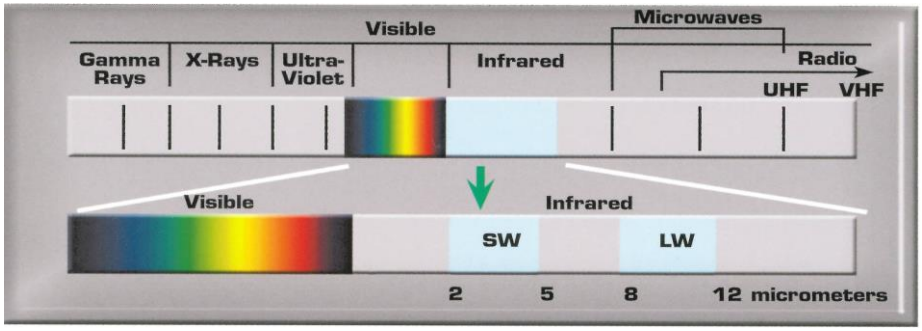
Langley in 1878, which then was followed by a pause of hundred years in development. Although the theory had been invented, the level of the electronic industry was behind. The engineers had to wait for fast electronic devices which were able to process the signals of the sensor in time.

**Milestone of development**

1960s - First sensor invented and published by Texas Instruments, Hughes Aircraft, Honeywell
1980s - USA Government's program for uncooled detectors
1991 - Production increased due to the Gulf War, prices decreased
1994 - Invention of micro bolometer by Honeywell, new developments started by Boeing, Lockheed Martin, British Aerospace
1998 - First detector introduced by Bullard for fire department

**The basics**

Before indulging in the details of the operation of thermal cameras, their physical basics are worth clarifying. The technology makes use of the range from 1 µm to 1 mm wavelength. The most common wavelength used for security applications are from 8 to 12 µm which is a range of LWIR[8]. There is a wide variety of military applications in which the devices operate at the longest infrared range at times (Fig, 1).




*1. figure: Electric magnetic radiation ranges*

The range of thermal radiation ranked in bands:

- Short Wave Infrared (SWIR), from 1µm to 3 µm
- Mid Wave Infrared (MWIR), from 3 µm to 5 µm

[8] LWIR – Long Wave Infrared

- **Long Wave Infrared (LWIR), from 8 µm to 12 µm**
- Very Long Wave Infrared (VLWIR), from 12 µm to 25 µm
- Far Wave Infrared (FWIR), from 25 µm to 1 mm

**The sensor**

A thermal sensor called microbolometer is used in thermal cameras applied in the field of security which is a bolometer made specifically for thermal cameras. The most frequent starting material is the grid of vanadium oxide (VO) or amorphous silicon. Vanadium oxide is a correct choice for sophisticated security applications as VO changes its resistance in almost all ranges used for thermal cameras. Electronically, the resistance of VO is approx. 100 kΩ making it applicable for various circuits.

**Basic parameters**

The comparison of thermal cameras is a sophisticated task. For professionals dealing with CCTV[9] systems it is essential to set up a standard control method to be able to compare all technical parameters correctly in the case of comparing cameras operating at visible light. We must follow correct determination but in this case we have a special built-in component called microbolometer. Its main physical parameter is the NETD [10] showing the required camera 'sensitivity' which determines the temperature difference the camera is able to detect. Obviously, this technical parameter should be checked with a fixed F Stop parameter[11].

e.g. 50 mK[12]=0,05 $^{O}$C at F1.2

The resolution of the best selling microbolometer is the following:

→ 640 x 480
→ 320 x 240
→ 160 x 120

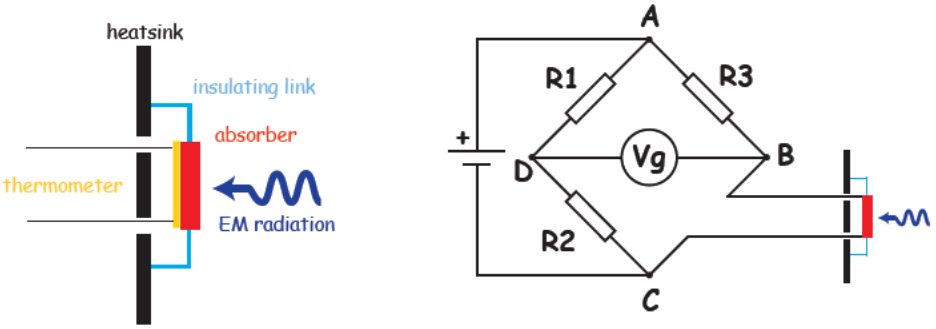
Since 2008 the megapixel category of microbolometer (1024 x 768) has been in the market, with the 1 MP or higher resolution bolometers made for the Army.
The most common approach today is applying the highest resolution cameras for all purposes. However, in case of thermal cameras a high resolution video analysis

[9] CCTV – Circuit Closed Television system
[10] NETD - Noise Equivalent Temperature Difference
[11] F STOP - Controls the size of the aperture of the camera "lens"
[12] mK – Kelvin/$10^3$ – temperature measuring unit called Kelvin

is generally not necessary. Therefore, it is sufficient to apply a camera with a lower pixel number.

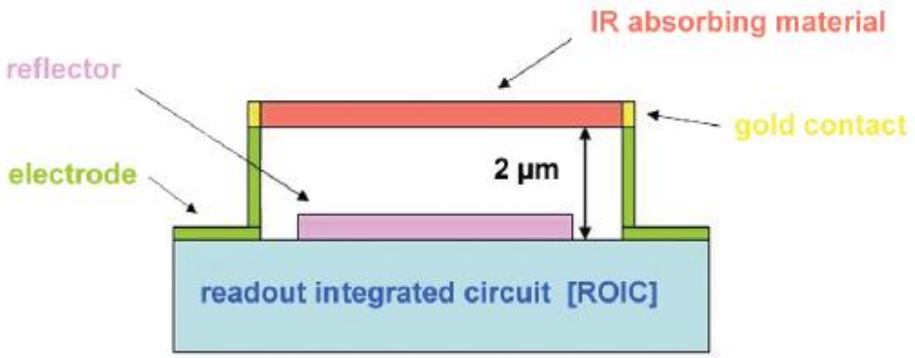
## 3. Physical processes

After having revised different camera parameters let us focus on the operation of the bolometer sensor itself.




*2. figure: Microbolometer (resistive)*[13]

Fig. 2 demonstrates the physical operation of the bolometer. The type depicted is a resistive one, which adjusts its resistance to thermal radiation, making it applicable in a simple measuring circuit.




*3. figure: Microbolometer structure*

Fig. 3 demonstrates the bolometer structure. The main goal is to set NETD as low as possible for engineers to maintain a gap between the readout circuit and the bolometer itself so that the thermal noise rate can remain at a low level.

[13] J-D Ganiere – Experimental Methods in Physics (2011-2012) – course

## 4. The differencial quation of heat convection

The heat convection can be expressed by a mathematical equation. A simple equation of the heat convection can describe the heat difference which can be distinguished by the thermal detector at determined wavelengths. The most significant equations are as follows:

Differential equation of heat convection:

$$C\frac{\mathrm{d}(\Delta T)}{\mathrm{d}t} + G(\Delta T) = \eta P = \eta P_0 e^{j\omega t}$$

The value of the heat change:

$$\Delta T = \frac{\eta P_0 e^{j\omega t}}{G + j\omega C} = \frac{\eta P_0}{G\sqrt{1+\omega^2\tau^2}}$$

Time constant:

$$\tau = \frac{C}{G}$$

where

C: heat capacity of the bolometer membrane
G: heat draining of the bolometer and its surrounding
$P_0$: power of the thermal radiation touched by the bolometer
η: proportionality factor
ω: circular frequency of radiation
ΔT: temperature change of membrane

## 5. Resitive bolometer

The definition of a resistive bolometer is when the resistance of the detector changes significantly depending on the temperature of the device. Equations to be applied:

Resistant change on sensor:

$$\Delta R = \alpha R \Delta T$$

Temperature coefficient of the bolometer:

$$\alpha = \frac{1}{R}\frac{\mathrm{d}R}{\mathrm{d}T}$$

Temperature coefficient of metals:

$$\alpha = 0{,}002\ \frac{1}{^{o}C}$$

Having used the equations we can determine the terminal voltage depending on the current at the working point.

Terminal voltage on the bolometer:

$$V_s = \frac{i_b \alpha R \eta P_0}{G\sqrt{1+\omega^2\tau^2}}$$

Finally, terminal voltage can be determined:

$$V_s = i_b \Delta R = i_b \alpha R \Delta T$$

The electronic characteristics determined in equations above can be suitable for generating video images after the necessary adjustments.
There are other bolometers which work according to different physical parameters (ferroelectric, pyro electric, thermoelectric). In security technology resistive bolometers provide numerous advantages due to their accuracy of resistance being an electronic parameter.

## 6. Types of tetectors

The required goals can specify the types of bolometers in which the micro bolometer would be built. In the case of military applications, the cooled micro bolometer utilisation is widely accepted. The coolant is to be used for receiving higher sensitivity, which means NETD values could be reduced to $10^{-1}$ compared to types used in security industry.

## 7. Cooled detectors

**Advantages**

- Suitable for multispectral applications
- Applicable for high speed movements detection
- Outstanding sensitivity

**Disadvantages**

- Expensive technology
- Considerably sizeable than the uncooled version
- Long period of MTBF
- High energy consumption

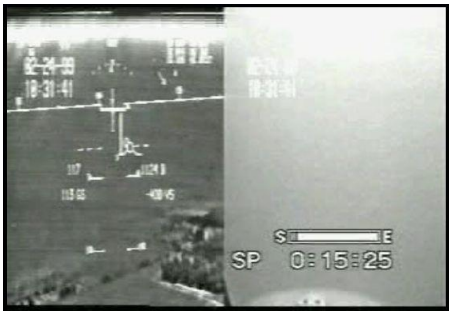
**Known applications**

- IR-headed missiles (air-to-air missiles sensitivity could be extremely high, e.g. they can be applicable from 10-20 km, e.g. AIM-9M Sidewinder and FIM-92 Stinger)
- Boarder guard applications
- Maritime application

*4. figure : IRIS - T air2air missile on beam*

## 8. Non-coled detectors

The spread of non-cooled micro bolometers has been supported by the development of circuits. At first mass production was only present in military development but later economic reasons enforced the increase of production capacity. Civil applications include the fire department, the civil aviation, flying in foggy weather, etc.




*5. figure Thermal camera in aircraft (a)*


*6. figure Thermal camera in aircraft (b)*

As it can be seen, the security risk of aviation could be reduced by an EVS[14] built-in thermal camera system.

[14] EVS – Enhanced Vision System – Extending visibility of pilots in foggy weather.

**Advantages**

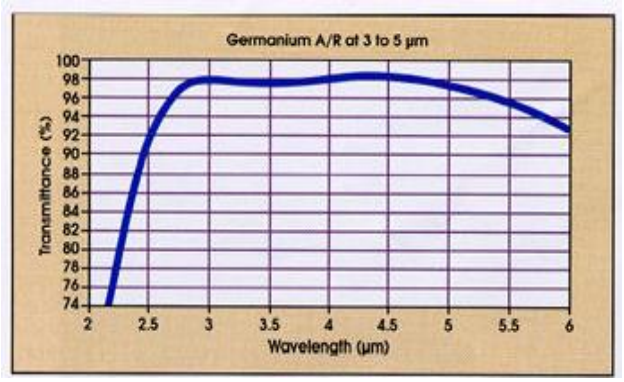
- the small size of non-cooled micro bolometers is suitable for standard size box cameras
- Real time signal
- Low energy consumption
- Very long period of MTBF
- affordable for civil industrial production

**Disadvantages**

- Low sensibility compared to cooled ones
- Unsuitable for high speed movements and multispectral applications
- Thermal radiation can be shaded by glass so the lenses must be made of a special material

## 9. Applicable lenses

No cameras may be manufactured without lenses so we should also use objectives for thermal cameras. The thermal radiation must be transferred to the micro bolometer grid which can be done by lenses made of a special material. It is evident that thermo convection cannot pass through glass so developers should turn to other materials. Although there are other possibilities, one of the best kinds of material proves to be germanium for cameras of security technology purposes.




*7. figure: bility of thermo convection transfer by Germanium (Ge)*

**Base material for lenses**

- germanium (Ge)
- zinc selenide (ZnSe)
- zinc sulphide (ZnS)ZnS
- zinc sulphide multispectral (ZnS MS)

- silicon (Si)
- calcium fluoride ($CaF_2$)
- amorphous material transmitting infrared radiation (AMTIR[15])

In accordance with the goals of applications professionals may select the best type of material for lenses. The transmitting ability of infrared radiation always depends on the wavelength in the IR band. If the requirements of resolution are relatively low (e.g. 320x160 pixels), amorphous plastic may also be used.
There is an important parameter of germanium: the metal (Ge) itself is so soft that even nails can scrape and damage its surface. Scratched germanium lenses go wrong instantly, therefore the surface of lenses must be protected. Many thermal cameras have non-removable objectives and can only be disposed of as one piece, which raises the costs in the case of a single damaged lense.

**Surface coating**

- BBAR (broad band anti-reflective)
- Creep BBAR
- DLC (diamond-like carbon)

Besides surface coating, mechanical protection is quite common in the military industry, where the lense covers can be removed by a remote control.

**Manufactures**

There are a few dominant manufacturers for thermal cameras in the market, some of the most important firms are listed below:

- FLIR Systems (USA)
- OPGAL Optronics Industries (Israel)
- E.D. Bullard Corporation (USA)
- Axis Communications (Sweden)
- Tainjin SEC-EGO Electronics ltd (China)
- IRCAM (Germany)

**Thermal camera sin practice**

Unfortunately professionals do not frequently encounter cases in their job where thermal cameras are applied or installed in practice. The obvious reason for this is they are too expensive to be widespread. However, sophisticated solutions for

[15] AMTIR – amorphous material transmitting infrared radiation

clients working in special industry area (e.g. electric power plants)do require the application of these devices. As mentioned before, the video streams provided by thermal cameras are not made for constant security guard or operator surveillance, their main function facilitates video analysis. Only in a few rare solutions should the operators control the camera pictures as a normal video stream. Instead, the video analyser software of the device induces controls switching on other subsystems or alerts security guards for operative activities following the macro regulation set previously. It is the best if the analyser program made for thermal cameras directly support the required activities.

**Basic video-analysing rules**[16]

| **Detection Rules / Behaviors** | |
|---|---|
| **Person** | Person moving in an area |
| | Person crossing a line |
| | Crowding |
| | Person tailgating |
| | Loitering |
| | Grouping |
| **Vehicle** | Vehicle moving in an area |
| | Vehicle crossing a line |
| | Stopped vehicle |
| | Tailgating vehicle |
| **Static Object** | Suspicious object |
| | Traffic obstacle |
| | Asset protection |
| **Counting** | Count people |
| | Count vehicles |
| | Measure stickiness (dwell time) |
| **PTZ** | Preset – Person moving in an area |
| | Preset – Person crossing a line |
| | Preset – Vehicle moving in an area |
| | Preset – Vehicle crossing a line |
| | Autonomous Target Tracking |

[16] Downloaded: http://www.agentvi.com/61-products-62-vi_system

**10. Detection – rcognition - identification**

A few quite important parameters of thermal cameras must be prioritised when selecting a device. Their data sheets may indicate excessive distances for camera reach. Technical details must be dealt with care, bearing in mind that the phrase 'up to'in front of numbers refers a maximumal, rather than a general range. As mentioned before, the one essential technical parameter is NETD. There is another one which shows what kind of pictures can be obtained from the camera in question from a certain distance. It is the DRI[17], an abbreviation explained below.

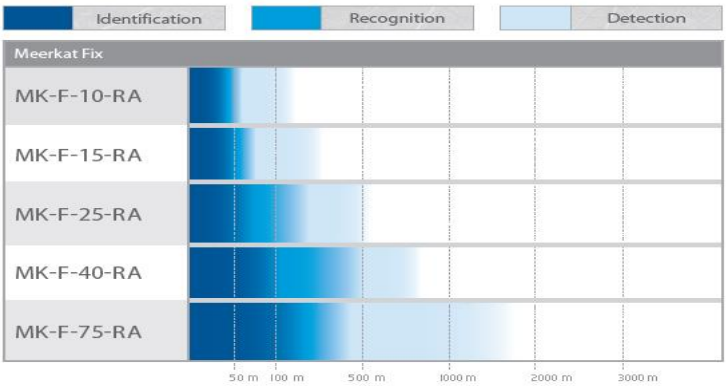
**Detection**
Detection is a capacity of the thermal camera which means the camera in question is able to make temperature difference between two points in its view angle. In practice this means 2 pixels / meter only. This can indicate the presence of a moving person if the camera had been installed to detect motion.

**Recognition**
Recognition is a capacity of the thermal camera where well-trained operators are able to determine from the provided video stream the presence of cars or people or animals in the picture. In practice this means 8-10 pixels / meter. This enables the differentiation of people in the camera image.

**Iidentification**
Identification is a capacity of the thermal camera where well-trained operators are able to conclude from the provided video stream that in the picture there are solders with guns. In practice this means 16-20 pixels / meter! This makes the users capable of recognizing people with weapons.

CCTV usually uses a specific set of guidelines for Detection, Identification & Recognition (DRI) of an object or person. This typical equates to D=10%, R=50%, I=120% of screen height.[18]

[17] DRI – Detection – Recognition - Identification
[18] https://www.dedicatedmicros.com/europe/products_details.php?product_id=263




*8. figure: DRI parameters of a few thermal cameras*

As an example, the following DRI parameters can be deduced with regard to MK-F-75-RA thermal camera produced by Xenics.

- Detection:1.800 m;
- Recognition: 450 m;
- Identification: 120 m.

**An example in practise:**

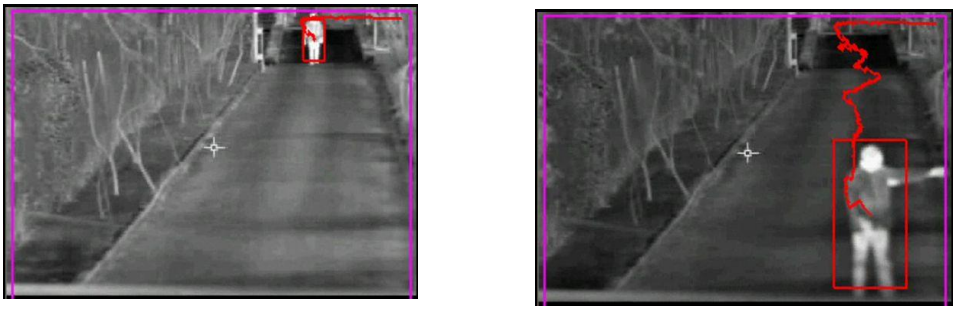

*9. figure: Meaning of DRI*

**Summary**

In conclusion we can say that the application of thermal cameras should considerably decrease the security risks if these applications are selected very carefully. The focus of our clients must be directed to their advantages. Shortly, the prices of these cameras will become low enough to be accessible and affordable for even domestic users.

**A few pictures of thermal cameras**

*10. figure: Detecting and tracking down a car*



*11. figure: Detecting and tracking a moving persons*


*12. figure: Thermal camera test*

1.: Camera resolution: 640x480 pixel 2.: Camera resolution: 320x240 pixel
3.: Camera resolution:D1 quality D&N 4.: (Meerkat: XENICS (Belgium) hőkamera)

**References**

http://www.xenics.com/documents/20090714_LR_Meerkat_security_A4.pdf
http://www.marchnetworks.com
W. Radford; R. Wyles; J. Varesi; M. Ray; D. Murphy: Sensitivity Improvements in Uncooled Microbolometer FPAS
Peter Kornic: Selecting lenses…Janos Technlogy Inc.: http://www.janostech.com/thermal_image_lenses/index.html
Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., 2010
ICU (Infrared Imaging Components for Use in Automotive Safety Applications): www.icu-eu.com
http://www.lumitron-ir.com/application_security.php
http://www.opgal.com/
http://www2.l-3com.com/irp/products/security.htm
www.flir.com
Matyi Gábor: Nanoantenna-mom dióda szenzorok elektrodinamikája 2007 (PhD thesis)
J-D Ganiere: Experimental methods in Physics (2011-2012)

***Zsolt Roman[19]: Properties of svbied attacks and related building damages based on middle east conflicts***

**Abstract**
*In recent years, violent purpose bombings mainly consisted of suicide attackers using car bombs in the Middle East. These large scale bombings are usually carried out against buildings in urban environment. Video footages of the preparations and the attacks are very valuable from a military point of view. The aim of this paper is to draw conclusions on the properties of these attacks: the general charge weight of VBIED is approximated, and we point out some important issues regarding structural response and protection methods against these blast effects.*

## 1. Assembling the VBIED

In all regions which the footages cover, the soviet armoury was in service, so when the conflicts began, these weapons became available for the insurgents and terrorists. Apart from mortars and artillery shells, homemade explosives are used too. Homemade explosive is rather used only to convert conventional war equipments into IEDs. They remove the initiator from mortars and artillery shells by drilling a hole into the main charge. Then they place a piece of detonating cord in the hole together with homemade explosive (Fig 1.). One can create a charge as large as he wants, consisting of these modified mortars. A charge like this contains significant amount of fragments itself, because of the many steel casings involved.


*1 figure: Mortars being converted into IEDs*

[19] M.Sc. Structural Engineer, Ph.D. student, Doctoral School of Safety and Security Science, University of Óbuda zsolt.roman@ymail.com

Dozens of converted mortars and shells can be hidden in a car, or a few pieces might as well be mounted on a motorcycle (Fig. 2). It is more complicated to hide the content of a lorry, which is in some cases only covered by plastic sheets.

*2: figure: Mortars and shells on a motorcycle and in a car*

ANFO can also be found in VBIEDs, it is either filled in barrels, or large steel pipes, or maybe in bags. Since the aim of the terrorists is to cause as much damage as possible, they usually put plenty of gas cylinders into the charge (Fig. 3). Detonating of the charge is carried out using an electrical switch connected to the detonating cord system, which will set off the whole charge almost simultaneously.


*3. figure: Gas cylinders, ANFO bags and cans loaded in lorry VBIEDs*

One can determine the amount of explosive used in different attacks based on the footages which show the preparations and the assembling of the SVBIEDs. These amounts differ from what is given in the table issued by ATF (Table 1). To determine explosive mass based on video footages, Table 2 and Table 3 were used, where the details of the most common Soviet-type mortars and artillery shells are listed.

| ATF | Vehicle Description | Maximum Explosives Capacity | Lethal Air Blast Range | Minimum Evacuation Distance | Falling Glass Hazard |
|---|---|---|---|---|---|
|  | Compact Sedan | 500 pounds 227 Kilos (In Trunk) | 100 Feet 30 Meters | 1,500 Feet 457 Meters | 1,250 Feet 381 Meters |
|  | Full Size Sedan | 1,000 Pounds 455 Kilos (In Trunk) | 125 Feet 38 Meters | 1,750 Feet 534 Meters | 1,750 Feet 534 Meters |
|  | Passenger Van or Cargo Van | 4,000 Pounds 1,818 Kilos | 200 Feet 61 Meters | 2,750 Feet 838 Meters | 2,750 Feet 838 Meters |
|  | Small Box Van (14 Ft. box) | 10,000 Pounds 4,545 Kilos | 300 Feet 91 Meters | 3,750 Feet 1,143 Meters | 3,750 Feet 1,143 Meters |
|  | Box Van or Water/Fuel Truck | 30,000 Pounds 13,636 Kilos | 450 Feet 137 Meters | 6,500 Feet 1,982 Meters | 6,500 Feet 1,982 Meters |

*Table 1: Recommended assumption for VBIED charge size by ATF [1]*

| Size | Type | Charge [kg] | Explosive | | Length [mm] |
|---|---|---|---|---|---|
| 122mm | OF462 | 3.68 | TNT | Amatol 40/60 | 560 |
| | OF471H | 3.8 | TNT | | |
| | OF471 | 3.6 | TNT | | |
| 152mm | OF530 | 6.86 | TNT | | 650 |
| | OF550 | 7.00 | TNT | | |
| | OF551 | 6.53 | TNT | | |
| | F533 (old) | 8.00 | TNT | | |
| | OF540 | 6.25 | TNT | | |
| | F542(old) | 5.86 | TNT | | |

*Table 2: Details of Soviet-type artillery shells [2]*

| Size | Type | Charge [kg] | Explosive | | Length [mm] |
|---|---|---|---|---|---|
| 82mm | O832 | 0.4 | TNT | Schneiderite | 313 |
| | O832DU | 0.435 | TNT | Dinitronaftalin | 330 |
| 120mm | OF843 | 2.67(TNT)/1.58(Amatol) | TNT | Amatol 40/60 | 656 |
| | OF843B | 1.4 | TNT | Dinitronaftalin | 668 |
| | F843 | 3.9 | TNT | | 750 |

*Table 3: Details of Soviet-type mortar shells [2]*

| | Mortar | Artillery shell | ANFO, misc. | Gas cylinder | Sum (kg) |
|---|---|---|---|---|---|
| Motorcycle | 4 | | | | 1.6 |
| Car | 120 | | | | 468 |
| | 80 | | | | 32 |
| | | | 2 bags | | 40 |
| | | 30 | | | 114 |
| | | | | 3 | - |
| | 120 | | | | 110 |
| Microbus | | 8 | 6 barrels | | 1076 |
| | | | pipes | | 500 |
| | | | 4 barrels | | 510 |
| | | | pipes | | 750 |
| Lorry | | 20 | 4 | 15 | 820 |
| | | | 40 cans | | 600 |
| | | | 50 bags | | 750 |

*Table 4: Estimated VBIED charges based on different video footages*

It can be stated that the real charges which occur in case of SVBIED bombings are far smaller than the ATF recommendation. Only in one video was it possible to count as much explosive as there is in the ATF table: an attack in Afghanistan was carried out with a pickup truck (which can be taken passenger car), it contained appr. 468 kg of explosive. Some reports made by explosive experts after major attacks also estimates a charge size which corresponds to what the footages show. This does not mean that values mentioned by Table 1 are not possible at all, but the probability of such a large charge to occur is quite small.

## 2. Characteristic signs of the attacks

The SVBIED attack starts from a distant place, where the VBIED is constructed. One person – the suicide bomber – is driving the vehicle. Many footages show these men carrying weapons, so care has to be taken in case of stopping the vehicle, because the driver might attack if he feels the success of the attack endangered. A common way of attack is when the suicide bomber is parked and waiting for a convoy, or other target to pass by (Fig. 4). This attack style is different from the one when the attacker drives his vehicle near the target and blows it up, because that being the case, the target is moving towards the bomb and not vica versa. This

requires other defence techniques, which is out of the scope of this paper, moreover, in this case the targets are vehicles, and not buildings.

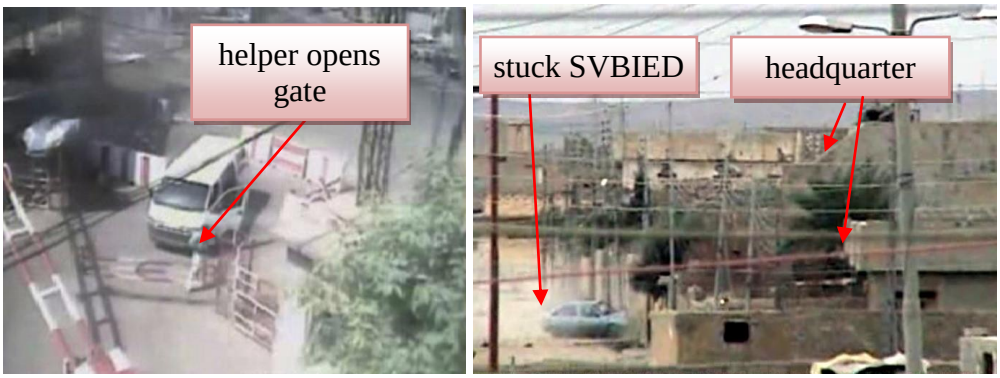

*4. figure: SVBIED attack against a moving target*

In other cases, the most common property of the attacks is that the suicide bomber drives his car as close to the target as possible, and detonate there. This might happen surprisingly, concealed, either slowly or fast. It becomes clear from the videos, that the proper protection of the target's perimeter is essential. This is clearly visible in cases when the suicide bomber drives at a high speed and blows the vehicle up very close to the checkpoints as a sudden attack (Fig. 5). Though no exact reports are available about these attacks, it can be assumed that the extremely close explosion caused severe damages and casualties.


*Fig. 5: SVBIED attack against an unprotected checkpoint*

It's not unusual that terrorists launch twin suicide bombings. If the first bomber is stopped or detonates at the protected perimeter, the second bomber is likely to have a free way to the building. If both explosions take place near the building, all the effects get magnified.

There are cases when the protection system of the target building successfully stops the attacker (Fig. 6 right). This way, the protection of the building is provided by the safety distance. Sometimes the attacker has helpers, who help him get closer to the building. This is done either by a "battering ram", when another SVBIED attacks first, or by handwork, when the helpers remove obstacles in front of the SVBIED (Fig. 6 left). If the targeted building has an insufficiently designed protection wall, the vehicle itself can get through the wall, as seen in a footage from Iraq.




*6. figure: Helpers opening a gate for SVBIED (left) and stuck SVBIED at the gate (right)*

Other helpers of the attacker provide covering fire on the target building (Fig. 7). A few gunmen start firing on the building from separate locations, so the attention of the guards is distracted. This firefight alone can cause damages to the structure and injuries to those inside, especially if we take it into consideration that sometimes the attackers use 14.5 heavy machine guns besides regular 7.62 rounds. It also happens, that this firing takes place not only before the explosion, but continues after it. Though the flying rounds are not likely to hit the people lying still in the inside, but they pose a threat because they can light the flammable materials by generating sparks.

A mixed-style attack happened in 2009 against a headquarter of the Iraq National Guard. The attacker parked his VBIED just in front of the building, then he left. The others then started to fire on the building, forcing those inside to flee, and they blew the truck up when it caused most casualties.


*7. figure: The attacker's helpers provide covering fire on the target building*

It is worth to highlight the case of Salerno military base, which was attacked 1 June, 2012 at the boarder of Afghanistan and Pakistan and this is a good example of how sophisticated the terrorist groups are nowadays (Fig. 8). The Taliban group was specially trained for this attack, where they entered the base with a dozen gunmen after the SVBIED explosion. The soldiers at the base managed the situation, and they killed all the attackers, but this attack warns us to keep an eye on this kind of complex attacks. The first military reports said the attack was successfully repelled and the base was secured, but later this got modified and at least two dead and several wounded were reported [5].


*8. figure: The Salerno base attack: entering gunmen on the right*

## 3. Blast effects

**Explosion types**

Due to the irregular shape of the charge and the way it is connected by the detcord, the charge doesn't behave like a concentrically detonated spherical charge. It could be a topic of a separate research to check the distance at which the shock wave will have the same properties as what a regular spherical charge would cause. Based on the footages, it is not possible to determine how asymmetric the shock wave propagation is.

Different explosive types cause different blasts. Fire effects and flames have to considered when dealing with charges which contain flammable materials. Though the compressed gas cylinders contain quite much highly flammable gas at high pressure, their effect is far from being equivalent to the same mass of TNT. Though fuel-air explosives might have a TNT equivalence of far more than 1, the explosion of a homemade gas cylinder will not produce ideal mixture of oxygen and gas [4].

Effect of the shock wave is less significant in these explosions, most damage is done by the flames, both for structures and people. A visible property of these attacks is the weak shock wave with a big, spectacular fireball (Fig. 9).

Though flames form during the chemical reaction of the explosive material too, this cannot be mistaken for an explosion containing added flammable materials. It can be noted, that all the vehicles contain gasoline, which is likely to catch fire in the blast, but this is negligible compared to the big amounts of gas or gasoline used in such VBIEDs. So it is necessary to consider fireproof design when reinforcing our military bases or highly protected residential buildings.

*9. figure: Blasts of SVBIEDs containing flammable materials*

It is also possible to slightly identify the explosive type based on visual sight. Explosives with negative oxygen balance (like TNT) produce black, dark smoke, while homemade explosives (like ANFO, HMX, TATP) generally produce light, grey or white smoke (Fig. 10).

*Fig. 10: Explosions with different smoke colours of TNT, ANFO and homemade charges*

Some explosions produce a hemi-spherical cloud-like visual effect as the shock wave is propagating outwards from ground zero (Fig. 11). This sudden appearance of a vapour cloud, and then its disappearance is not explosive dependant, rather is it depending on the atmospheric conditions. In case of huge humidity or cold weather, as the shock wave passes by, pressure drops suddenly, temperature of air also drops, and it can't contain as much water as before, so water is condensed into a vapour cloud.

*11. figure: Suddenly appearing vapour cloud showing hemispherical shock-wave propagation*

## 4. Damages of buildings and their neighbourhood

Damages of buildings are without doubt mostly dependant on the distance of blast to the building. The closer the SVBIED gets to the target, the severe damages and injuries will it cause to the buildings and to the people.
On 8 September, 2007, terrorists attacked the coast guard headquarter of Dellys, Northern Algeria. It is visible in the footage, that the headquarter is only protected by a weak gate, which the attacker easily breaks through, and the blast took place inside the base (Fig. 12). The explosion torn the lightweight structures apart, leaving 30 dead and 47 wounded. The SVBIED consisted of homemade explosives and a large gas cylinder. Though this VBIED cannot be considered as big, the huge number of casualties show how important the distance of the blast is.

*12. figure: The SVBIED bombing of Dellys coast guard and the aftermath of the attack*

On 17 August 2009, the police station of Nazran, Ingusthetia was attacked by a suicide bomber (Fig. 13). Protection of the police department was inadequate from the at least two viewpoints. The attacker could break through the poorly protected gate, and the explosion took place inside the base. Second problem was that the

explosives stored in the base - due to insufficient containment protection - were also detonated by the huge blast, which magnified the effects. Pre-attack footages show barrels at the back of the vehicle, so probably ANFO was used for the attack. Experts later reported they assume that 400 kg of TNT equivalent charge was used for the attack [6]. This charge is not considered big either, but in this case again, the closeness of the blast caused many casualties.

*13. figure: The aftermath of SVBIED bombing of Nazran police station*

The building's roof structure was completely ruined, and all windows, including those of the neighbouring buildings, were shattered, which is responsible for the huge number of injured. Nevertheless, the structure of the building remained intact, no spectacular damage can be identified. 25 people died and 164 injured in the attack. It is important to point out, that the masonry wall at the perimeter of the building got completely destroyed, so it provided no effective protection against the blast. It is proved by several footages, that the global failing mode of the buildings is progressive collapse. Progressive collapse is a relatively rare event in average daily life, as it requires both an abnormal loading to initiate the local damage and a structure that lacks adequate continuity, ductility, and redundancy to resist the spread of damage [3]. This means that it is not the building's lateral bracing system which the shock wave will overstress - and thus cause collapse -, rather it is overstressing a structural element locally, and when it fails, the superior elements resting on the failed element won't be able to withstand gravity loads and they will collapse one after another. In case studies of Middle East SVBIED attacks it can be found, that masonry structural elements are usually responsible for progressive collapses, as they are weak enough to fail, and they usually work as supporting walls, so their damage triggers the collapse mechanism. This is verified by a couple of aftermath footages, where masonry units can be seen below and around the ruins, so the original building material can be assumed (Fig 14.).


*14. figure: Buildings after progressive collapse*

Big explosions has significant cratering effects, which, in urban environment, can reach the depth of public works pipes. The damages of water pipes can be identified in craters filled with water. One example is the 2009 twin suicide attack against the Iraq Ministry of Justice. Bridges are vulnerable to SVBIED attacks too, especially those with large spans. Usual failing mode is that the girders disconnect from the supports and they collapse as rigid bodies. This might happen in case of a blast taking place on the bridge, below the bridge, or at a checkpoint located near the abutment. On Fig. 15 it can be seen how big plastic deformation was caused in the support beam by the enormous downward pressure on the bridge.

The effect of the explosion on the armoured vehicles also has to be considered. The effects of a close blast is different from running on a mine or IED, because the shock wave approaches from a different direction, and fire effect is a significant danger too. Fig. 16 shows images where vehicles burnt out, while the buildings suffered only minor damages.


*15. figure: SVBIED attack of a bridge above Tiger river, Al-Ruhaiya, Mosul, Iraq*



*16. figure: Armoured vehicles burned out due to VBIED attacks*

Fig. 17 shows an attack on a military base in Iraq. NATO standard T-Walls are set up around the perimeter of the base. This wall is not especially designed against blast effects, and as it is shown on the figure, it is destroyed by the explosion. The wall not only failed to protect the base from the shock wave, but as it crushed, it turned into dangerous fragments inside the base.


*17. figure: Failure of T-Wall protection wall due to SVBIED attack*

Another widespread protection system is HESCO bastions, which give much better protection compared to rigid concrete walls. But sometimes the HESCO bastion fails too, like in an attack seen on Fig. 18 (left). On Fig. 18 (right), the HESCO bastions are located in a radialized direction to ground zero, so they remained intact, but surprisingly, the double-row HESCO bastion at Salerno base also remained intact, though it was a reflecting surface. Based on all the cases where HESCO bastions are present, we can claim, that it is among the best currently available solutions for base protection, though its capacity needs further investigation. We also have to point out, that the building behind the wall collapsed in the Salerno attack (Fig. 8). HESCO wall is not to blame for this, the distance of the building from the wall was not great enough, safety distances required by the standards were probably not kept. The video footage of Salerno attack shows a preparation phase, where the attackers are planning the bombing with the miniature model of the Salerno base, and they clearly see how close the dining building is to the wall. This has to attract the attention of those who deal with site planning of military bases, and we have to try to avoid these kind of unfortunate casualties.

*18. figure: Failed HESCO bastion (left) and standing RC structure after SVBIED attack (right)*

If a building does not collapse, it doesn't mean that the attack claimed no casualties. Since casualties, injuries are mostly caused by fragments or other non-direct effects of the shock wave, the intact structure of the building tells us little about the seriousness of attack. Fig. 18 (right) shows the aftermath of a giant SVBIED attack in Iraq, where the reinforced concrete structure remained globally intact, only concrete cover was removed and local damages were done. But the inside of the building is ruined completely, several casualties were claimed by the attack, but these were not due to progressive collapse. In some cases, the explosion is so weak, that the attack could even be called negligable. Even though, some minor effects of the blast wave are still present, and can be identified on video footages: attic walls collapse, lightweight roof sheeting is torn up, electrical flash-overs happen. Masonry walls, which are not supported on all 4 edges, are likely to crash down due to dynamic or ground seismic effects. A spectacular example of this is seen on Fig. 19, where the security camera of the base show a little wall in front of a base building before and after the attack.


*19. figure: Crash-down of a little wall due to blast effects*

**Summary**

Based on the analyzing of video footages showing suicide car bombings in the Middle East, we can remark that the charges used in the attacks are generally smaller than what is recommended by the ATF table, and this is proven by aftermath report estimations too. Charges contain converted mortars, artillery shells, ANFO and gas cylinders. We differentiate between massive VBIED bombings, and smaller explosions, which have more fire effects. Terrorists provide covering fire on the target for the attacker, so the one and only effective protection is the sufficiently tough wall and gate system far from the buildings, located at the perimeter of the base. Safety distance is especially required, because buildings can be damaged even if a blast protection wall is present (Salerno). From structural point of view, most damage is due to progressive collapse, and this is mostly

caused by weak masonry load bearing walls. Besides structural viewpoints, we have to take it into consideration that protecting human life is not only endangered by collapsing structures, but it is endangered by the fire and fragmentation effects of the blast.

*„TÁMOP-4.2.1.B-11/2/KMR-2011-0001 The project was realised through the assistance of the European Union, with the co-financing of the European Social Fund."*

**References**

[1] Bureau of Alcohol, Tobacco, Firearms and Explosives - URL: www.atf.gov
[2] A. B. SHIROKORAD, Широкорад А. Б. Энциклопедия отечественной артиллерии, Mn. Harvest, 2000, ISBN 985-433-703-0
[3] US Department of Defense: UFC 4-023-03 - Design of buildings to resist progressive collapse
[4] US Department of Homeland Security - Information Bulletin - Compressed Gas Cylinders as Components of IEDs, 2004
[5] http://www.washingtonpost.com/world/national-security/attack-on-us-outpost-in-afghanistan-worse-than-originally-reported/2012/06/16/gJQAlyaihV_story.html
[6] Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., 2010
[7] http://en.rian.ru/russia/20090818/155848718.html

***Anna Barbara Szabó[20]: The European Union and the United States of America from the Perspective of Data Privacy***

**Abstract**
*While the data protection policies of the United States of America (USA) tend to differ state-by-state, the European Union is aiming to create and apply a unified legal system in all of its 28 member states, which during their accession process, all EU candidate states must integrate into their legal system. In the USA, there is often a greater emphasis on the liberty of speech and the freedom of press, than the right to informational self-determination. This complicates those legal proceedings, which are commenced by a European state against contents, which are hosted on websites by an American hosting company. Furthermore, the USA, in the name of fight against terrorism, – often unwarrantedly and improperly by EU legal standards – is collecting data during international trading and personal transportation, which violates the human rights accepted by the European Union. Due to the actuality of the topic, I shall compare the data privacy regulations of the EU and the USA.*

## 1. Historical overview

There is a perceptible difference between the evolution of the legal systems of the two powers: in Europe, the typical predominance of the continental legal system prevails, with its codification, and the preponderance of the written law against jurisprudence. Meanwhile in the USA the common law, known as the Anglo-Saxon law is dominant, which prefers jurisprudence making precedents, which allow different interpretation of the law in different legal cases even in the same state [1]. The professional literature classifies the European data privacy protection as a third generation system, which initial purpose was to lessen the dependency of the citizens towards the state in regards of obtaining public information. Second generational data privacy regulations have brought the emergence of the right of informational self-determination, while the third generational legislation was shaped by developments of the business world and the advancements in technology. As civilization progressed, the demand for a transparent state, the right to have access to and disseminate public information and for the freedom of information came to prominence, besides the protection of personal information. This has also brought about the need for transparency in the use of public funds at

[20] Ph.D. student, Doctoral School of Safety and Security Science, University Óbudai

state- and other public bodies. The aforementioned factors have considerably supported the democratic operation of the state. [2]

The protection of information in the European Union is determined by a data protection directive of the OECD (*Organisation for Economic Co-operation and Development*), based on international consensus, which came into force in 1980. An essential purpose of this directive is to enable the smooth operation of economic relations whilst protecting private information. The principles laid down by the OECD have influenced the creation of the Council of Europe's agreement, titled "*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*", which was approved in 1981. [3]

In 2001, the office of the European Data Protection Supervisor's was created, in order to ensure that all the institutions and bodies of the European Union have the appropriate respect to the citizen's private life during the processing of personal data. [4]

In contrast, the citizens' right for the protection of their private information is significantly weaker than in Europe, despite Samuel Warren's and Louis Brandeis' study, published in 1890, which found that the advancement of technology can be intrusive to one's privacy. This necessitated the creation of a new system for the protection of one's right to informational self-determination. This system has matured by the 1970s, when it was decided – citing fundamental rights –, that the citizens should be protected against large state records. Hereafter I shall present the most significant milestones of this process, based on a study, by András Molnár. [6] [7]

In 1928 in the case of Olmstead vs. the United States, with a majority decision the Supreme Court held that telephone intercepts without a court order do not violate basic constitutional rights, because physically, the constitution regards the protection of privacy only within the house. It was because of this decision, that Louis Brandeis had formulated the "*right to be let alone*". The "*right of privacy*", only as an umbrella term was relatively lately introduced to the basic constitutional legal concepts in the 1960s, but still, it is not explicitly mentioned in the Constitution of the United States. William Prosser, as a professor of law classifies the right to privacy into the legal system of compensation, where he views the public disclosure of private facts as a violation of the right to privacy, which results to a disadvantage for those affected, regardless of veracity. He defines the action of libel as a separate category, as well as the possession of image, name and other identifiers. Later, Gary Bostwick established the principle, that third parties should have access only to a certain protected zones to information about the individual.

In 1977, a judgment, made by the Supreme Court in regards to the Whalen vs. Roe case has established, that the interests, which are affected by issues related to the private sector are made up by several separate interests, which include information on the individual and its right to remain a secret. [8]
In a study by David Solove in 2006, he views the unauthorized collection of information, the abuse of information, which have been legally obtained and the publication of such information to the general public unconstitutional.
In summary, the U.S. does not apply a standard law for data privacy, because it is possible to interpret it differently from one Member State to another. In despite of some courts having declared the protection of data privacy as a basic right, there is no single official supervision. Another vulnerability presents itself as only American residents, and those with valid residence permit are subject to the Privacy Act (the federal data protection law).

## 2. Relationship between the European Union and the United States of America

As the development of the information society continues, privacy and the right to informational self-determination can succeed less and less. In regards to data, lesser-developed countries are becoming increasingly vulnerable against more developed countries, which by the exploitation of the technological rift are carrying out unreported data mining. One way to reduce such dependency is to legitimize data collection between countries by mutual agreements and the establishment of proper safeguards. The legal harmonization of the OECD and EU satisfies this principle.
The “Safe Harbor” was created to facilitate the transmission of data to the United States. The assurance of the protection of private data during its processing is the most cardinal requirement of transmitting data to a third country. According to the Committee of the European Union, data transfer to the U.S. is considered to have an accepted level of safety, when the recipient U.S. Company is on the Safe Harbor list. The Safe Harbor list contains those Companies, which have agreed to meet the Safe Harbor data protection directives, set forth by the government of the United States.
The legal basis for all these are the 2000/520/EK (July 26$^{th}$ 2000) resolution of the European Committee based on the 95/46/EK directive of the European Parliament and the Safe Harbor act for providing adequate data protection, issued by the U.S. Department of Commerce, which contains all the data protection directives, that a U.S. based Company should meet. [9]

In the context of the Stockholm-program, the European Parliament has asked the European Commission to make a proposal for negotiations with the USA regarding data protection aimed at law enforcement and data exchange. The task force, based on the 29th article chaired by Jacob Kohnstamm has found that the passenger name records (PNR) of the U.S. collects such vast amounts of personal data of citizens travelling from the EU, which clearly is beyond the principles of necessity and proportionality. It states, that the fight against crime and terrorism does not justify the mass surveillance and tracking of passengers. Such police-like methods in EU member states are only feasible in special cases and within constitutional boundaries. The task force has also stated that it has not been presented with any statistics, which compares the number of criminals caught with the assistance of the PNR system with the number of surveyed passengers, which would justify the need for such surveillance. Thus, the task force recommends narrowing the range of personal data managed by the PNR system. In agreement with the European Data Protection Supervisor, the task force considers the recording of special data by the U.S. Department of Homeland Security unacceptable. Furthermore, it considers the 15-year long preservation of such data disproportionate, considering that according to the EU Charter of Fundamental Rights such data needs to be anonymized or deleted six month after use.

The European Data Protection Supervisor supports the logging and documentation of each access to PNR data, so proper use by the U.S. Department of Homeland Security can be verified. [10] [11]
The trans-Atlantic partnership plays a significant role in the foreign politics of the EU, which aims to develop a trans-Atlantic market by 2015. In the framework of a trans-Atlantic partnership the European Union expects its partners to accept the values which it represents. Such values are democracy, human rights and the rule of law, sustainable economy and sustainable growth. The protection of these values must be assured even during the defense from global threats, such as terrorism. Despite the USA and EU being the world's largest bilateral trading partners, which causes economic dependence, nevertheless some acts of the U.S. – of which the European Parliament has on several occasion called on the U.S. Government to cease – often contradict the values represented by the European Union. Such acts are the penalties by death still accepted by a number of U.S. States, the maintenance of the Guantanamo Bay detention center and the unilateral visa requirement against some EU member states. The records of persons, suspected to be involved in terrorism and proven innocent are not being deleted from the database, furthermore the U.S. keeps records of their namesakes

and last, but certainly not least – the controversial data mining done by the U.S. National Security Agency. [12]

**Summary**

The difference between the two powers goes beyond its historical roots. Despite that the United States itself is composed of numerous member states as well, its foreign policy does not view the European Union as a singular entity, and continues to show differences in treatment while dealing with EU member states.

The interpretation of data privacy and informational right to self-determination in the U.S. differs significantly from that of the EU. On the long term, the problems mentioned earlier can endanger the trans-Atlantic relationship, or if the partnership is formed based on the current conditions, the European Union is destined to play a subordinate role in the economical relationship.

## References

1. Katalin Gönczi Katalin - Pál Dr. Horváth Pál - István Stipta - János Zlinszky: Egyetemes jogtörténet (Nemzedékek Tudása Tankönyvkiadó, 2002.,ISBN: 9789631945720)
2. András Jóri: Adatvédelmi kézikönyv, OSIRIS KIADÓ KFT., 2005.
3. Gazdasági Együttműködési és Fejlesztési Szervezet (OECD), általános tájékoztató (Downloads:http://oecd.kormany.hu/az-oecd-rol, 11.09. 2013.)
4. Az Európai és a Tanács 95/46/EK irányelve http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu 11.09. 2013
5. Dr Rajnai Zoltán: Új kommunikációs technológiák a védelmi szektorban, BÁNKI KÖZLEMÉNYEK 2013: (1) pp. 1-11.
6. Az Európai Adatvédelmi Biztos, általános tájékoztató(Downloads: http://europa.eu/about-eu/institutions-bodies/edps/index_hu.htm,11.09. 2013.)
7. Adatvédelmi Biztos honlapja, általános tájékoztató (Downloads: http://abi.atlatszo.hu/index201.php?menu=usa, 11.26. 2013.)
8. András Molnár: A magánszférához való jog az Amerikai Legfelsőbb Bíróság joggyakorlatában (Downloads: http://dieip.hu/wp-content/uploads/2011-2-11.pdf, 11. 25. 2013.)
9. Tamás Győrfi: Az amerikai alkotmányjog szabadság-fogalma (Downloads: http://jesz.ajk.elte.hu/gyorfi4.html,.11.25. 2013)

10. Adatvédelmi Biztos honlapja, általános tájékoztató (Downloads: http://abi.atlatszo.hu/index201.php?menu=safeharbour, 11.26. 2013.)
11. A stockholmi program – A polgárokat szolgáló és védő, nyitott és biztonságos Európa 2010/C 115/01 (Downloads http://eur-lex.europa.eu/Notice.do?mode=dbl&ihmlang=en&lng1=en,hu&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=513011:cs, 12.01. 2013.)
12. 29. cikk szerinti adatvédelmi munkacsoport, 00664/11/HU WP 181, 10/2011 sz. vélemény „az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntető eljárás alá vonása érdekében" című, európai parlamenti és tanácsi irányelvre irányuló javaslatról, 2011. április 5. (Downloads: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_hu.pdf, 12.01. 2013.)
13. Az Európai Unió Hivatalos lapja: P6_TA(2006)0238 EU–USA transzatlanti partnerségi megállapodás, C298 E/226, 2006. 12.18.(Downloads: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:298E:0235:0235:HU:PDF, 11.26. 2013.)

***Gabor Vanderer*** [21] ***: Applicability of risk-evaluation theories in crtitical infrastructures***

**Abstract**
*Business (and governmental, municipal, non-profit etc.) organizations have long been paying attention to safeguarding their information assets and information infrastructure. On one hand, it is getting more and more important with the development of an information society, and on the other hand, it is a response to the growing external threats jeopardizing the operation of enterprises. By now, there are many regulations, procedures and industry standards that has been developed for organizations to handle these threats, but these methods mostly use a traditional, business-based approach.*

## 1. Information wealth

Information has always had a great value. Owners have been interested in defending their treasure since the beginning of times. Many kings and generals relied on a network of intelligence and communication and all of them were aware of the consequences if this information falls into unauthorized hands. That was a call for the development of the art of cyphering (and decoding) while also increased the value of storing and transmitting the information in a secure way. Safequarding the Information has never been the monopoly of the state: civilian traders, or even the church wanted to safeguard their information as well, even if they did not had the same resources. Our world has changed a lot since those times, but it is still very true that information is the key success factor in today's knowlenge-based society. It has a value that can easily decide between success or failure in the life of a company. It is self-evident that information needs to be safegaurded. As more and more companies entered into the information security market, the general concepts for an effective approach have crystallized. This helped to establish the standards for information security (ISO/IEC 27001) which includes:

- Confidentiality (information should be accessed by authorized people only)
- Integrity (information should be full and accurate)
- Availability (information should always be accessibe for authorized people)

[21] Ph.D. student, Doctoral School of Safety and Security Science, University Óbudai

## 2. Information security and IT security

Information security is a much more complex problem than IT security (Michelberger – Lábodi, 2012). Firewalls, virus protection, 0-day prevention (and all the things usually categorized as IT security) are forming only the technical background. Obiviously it is not enough. These systems are being used by people. The confidentality, integrity and availability of this information is jeopardized by the slothful attitude of the inside users and the people outside the company authorized to use this data (suppliers, partners, etc.)
As Pál Michelberger said (Michelberger – Lábodi, 2012, p 243), the weak link is always the human part. In his opinion (and I can only agree with this), infromation security is more of a journey than a destination. If we investigate IT security it becomes clear that not even a well-secured system can persist forever. New vulnerabilities unravel every time, new software bugs emerge which should be addressed. Safeguarding the information vault depends not on the (currently) state-of-the-art technical implementation but on the permanent inspection and development of the existing systems. And feedback, obiviously.
Organizations usually regulate the usage of information-barriers and the information itself to safeguard their information-wealth (ISO 27001). Safeguarding can be successful if they define:
- information elements to be secured
- inside and outside threats
- probabilities of each threat
- regulations and instruments required for protection (ISO 27002)

The aim of information security is to maintain business continuity in a regulated way and to moderate the damage caused by security accidents. The parts of this regulations are regulations describing the processes of the organization and the rules for the use of IT devices and systems. Organizations have to concentrate on the information management system instead of buying equipments in order to ansure long-term secure operation.
We can define different levels of protection within information securty (Ji-Yeu Park et.al. 2008):

- Information technology infrastructure (hardware, software and network protection)
- Information handling (data entry, modification, deletion and access)
- Procuration (process regulation, workflow)

- Organization (information security strategy, risk management)

A good example for this is a „holistic" approach (Michelberger – Lábodi, 2012, p 244) where authorization have to be implemented on all 4 levels:

- IT level – user authentication
- information handling – guarantee that only the required data will be accessed
- process level – sharing of critical processes, personal and workplace-based access control
- organization level – risk avoidance, group-based authentication, regulating the permanent supervision of the authetnication system.

It is commonly accepted today that the first stage of security is a written security policy. It is impossible to set goals without the definition of tasks and responsibilities (and the human and financial resources required). Information security – as a process – can only be ensured after having this done.

## 3. Risk management

The aim of risk-management is to identify threats that could jeopardize the operation of the organization. They may exist inside or outside of the organization (a typical external example is the market of a company). In a traditional risk-management we usually assign amounts of money to each detected risk (calculated damage caused be the event), associated with a probability of occurrence. The cost of defence against each threat is compared with this, and a cost-benefit analysis is made to decide on security investments.

There are situations where factors for the calculations above can only be assessed with an extremely low precision. In these situations professionals talk about vulnerability and describe only the threats to the operation (and do not use numbers).

Organizations operating critical infrastructure elements have to use the second approach. These organizations also use cost/benefit-based analysis for decisions (obivously); but when critical infrastructures enter the picture it is not reasonable to define damage in monetary value. Organizations simply have to be prepared against the threats.

## 4. Standards and recommendations

People say that an engineer can find a standardized solution for almost everything. The only problem is to find the relevant standard. This applies to the area of information security as well. There are several de facto and de jure standards

related to information security. The latest standards commonly use a process-based approach but each one concentrates on different areas. However most of them covers the area of security.

A commonly used information security management system is the British-originated ISO/IEC27k standard-group. (www.iso27001security.com). Organizations working with it define security requirements and the corresponding actions based on organizational strategies. This standard places a special emphasis on information security (integrity, confidentiality, availability). It has no part dedicated especially to critical infrastructure systems (however „ISO 27799 - ISO27k for healthcare industry" covers one critical infrastructure). It has a framework tipicaly suitable for defining information security for critical infrastructures.

It is an interesting thing that being process-based, the standard is not dependable on any kind of technical solution. However, it contains some parts on network security (ISO/IEC 27033)

It was a common procedure to prohibit internet connection for critical infrastructure elements, but nowadays it not always sustainable. A typical example is the banking system. All organizations use the Internet for bank transfer (and they have to use bank transfer by govermental regulations), but only a fraction of them is able to implement some kind of workaround (transfer money by phone, for example). Not even the banks are prepared for this in the required volume. Using the Internet is sometimes mandatory so some calculated risks have to be taken. The ISO/IEC 27032:2012 standard addresses Internet Security specifically.

Another interesting regulation is addressing cloud services. The ISO/IEC 27017 is currently esisting in draft version only (final version is scheduled for 2015). There are no plans for auditing the cloude providers at all.

As I already mentioned in the previous chapter the weak link is always the human part. It is reasonable to create rules for employees on how to act in different situations. One of the most important standards is the British-originated MSZ ISO/IEC 20000-1, -2, targeting operational issues based on the recommentations of ITIL (Information Technology Infrastructure Library, www.itsmfi.org). It contains a formal system of requirements about the acceptable level of information services, a guideline about service controls and one more for auditing.

Service management activities are connected to the currently popular PDCA model, which is applied in several standards.In addition to the management system, the issues of planning and implementation of information technology systems, and the planning and creation of new services, there are five basic areas of complete service management:

1. Service security (service level, service reporting, capacity, service continuity, availability, information security, budgeting and accounting for IT services)
2. Management processes (configuration and change management)
3. Release (documents, operational description distribution management, the documentation of approved modifications)
4. Solution processes (incident and problem management)
5. Relationship (customer service, business and supplier relationship management)

ITIL is widely used by informatic outsourcing companies for SLA definitions, however, the specialities of critical infrastructures can be fitted into MSZ ISO/IEC 20000-1 –based specifications. See later in the chapters about BCP and DRP plans. ITIL takes a process-based approach. It defines activities which are segmented into processes. All processes have 3 levels:

- Strategic level: Organizational objectives are defined, together with the outline of methods to achieve these objectives.
- Tactical level: Strategy is translated into organizational structure and plans which describe the processes to be executed, assets to be deployed and outcome(s) of the processes.
- Operational level: The execution of tactical plans to achieve strategic objectives within a specified time frame.

ITIL does not have a separate topic for information security. It targets the subject as a part of all the processes. For example Data and information management (ITIL v3 Service Design Chapter 5.2) or Roles and responsibilities (ITIL v3 Service Design Chapter 6.4) have details on information security control, and there is a separate process on Information security management and service operation (ITIL v3 Service Operation Chapter 5.13). ISACF (Information Systems Audit and Control Foundation) also developed a recommendation, the widely used COBIT (Control Objectives for Information and related Technology) (www.itgi.org/cobit). It is an internationally developed and accepted framework (mainly for business organizations) which helps to understand and handle the risks around the areas of information and information security. COBIT is aimed at harmonising information technology services and the operational processes of the organisation as well as facilitating the measurability of the security and management features of information technology services.

COBIT starts from business targets. Achiving these targets requires information to be available and resources to be allocated to the information systems. All of these processes should be handled under coherent processes. ITIL helps to fill the gap between business risks, verification needs and technical problems. COBIT concentrates specifically on creating a cost-effective security.
A COBIT is az üzleti célokból indul ki. Az üzleti célok eléréséhez információt kell biztosítani, az információk biztosítása érdekében pedig az informatikai erőforrásokat összetartozó eljárások keretében kell kezelni. Segítségével áthidalható az üzleti kockázatok, az ellenőrzési igények és a technikai jellegű kérdések közötti távolság. A COBIT kimondottan a költséghatékony biztonságmegteremtésére koncentrál.

ISO/IEC 38500 is a high level, principles-based, advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of IT. The objective of the standard is to provide a framework of principles for Directors to use when evaluating, directing and monitoring the use of IT in their organizations. It also targets human behaviour.

Based upon the standard, a GRC model can be developed:

- Governance – Corporate goals and processes, the organizations running the processes with special weight on the supporting information technology systems
- Risk management – Identifing the probabilities of expected events and defining an acceptable level of secutiry for the processes and their supporting information systems
- Compliance – Organizations have to meet internal regulations and external (govermental) regulations and standards.

The outcome of the model is a list of requirements continiuosly following the changing conditions. Thus the management of the company is aware of the risks and risk-based decision-making. The ISO/IEC 38500 builds on consciously undertaken risks so its use is contraindicated for the operation of a critical infrastructure. In this scenario, core operation allows negligable risks only so basing decision-making on calculated risks seems unfeasible.

## 5. Integrated control systems

All of the above-mentioned integrated management systems use a process-based approach. All of them follow the schemes of the unavoidable ISO 9001. All of the other management systems (ISO 14001 for enviromental control, ISO 27001 for information security, and so on) usually integrate into ISO9001.
It is easy to state that trasparent operation is important for every organization and not just for those operating critical ifrastructures. Companies have a recognized right to keep their internal processes secret (as part of the competitiveness). Another natural need is to be sure that their partners (supplyers, resellers, etc.) are trustworthy. It is easy to see taht data handled by a partner shoud be just as safeas the data handled by ourselves. If our partner is ISO27001 certified, we are sure that it can meet these expectations and the organization puts weight on information security even if we do not see the exact inside processes.

## 6. BCP and DRP

Maintaining normal operations in any circumstance requires a written documentation defining how operations are to be re-established after an unexpected event. The main purpose of this document is to define all neccessary tasks in advance to possibly prevent ad-hoc decision-making in a stressful situation. In this way the re-establishment of sevice (ideally) becomes an automatic step-by-step process. It has some clear advantages:

- As the re-establishment (or the implementation of a workaround) becomes a step-by-step process with clear checkpoints, the possibility of making a mistake is dramatically decreased
- All the neccessary and only the neccessary underlying infrastrucure elements will be restored to maintain core business processes.
- Prioritizing among processes of the company is not the decision of the staff operating the underlying technical infrastructure (and doing the actual restoration). Predefined priorities eliminate the need of communication between different sub-organizations: the technical staff are able to restore business on their own.

Business Continuity Planning (BCP), sometimes also called Business Continuity and Resiliency Planning (BCRP), helps a company to continue operations under adverse conditions, such as a disaster afflicting the company’s headquarters. It does this by identifying the core underlying processes of the organization which directly affect

the bottom line and by finding alternate or back-up processes in the event of disruption. The business continuity plan itself is exactly what it looks — it is a plan or roadmap for the business to follow in a situation which threatens the continuity of business. (Charles Intrier, 2013)

Business Impact Analysis – BIA – This analysis is for collecting the relevant features of business processes in order to assess the damage caused by any disturbance in each of the processes. The result of the analysis:

- list of processes
- their monetary and non-monetary value
- allowed maximum downtime
- list of the resources required by the process
- interdependencies of processes

Disaster Recovery Plan (DRP) It is supposed to define procedures to follow in case of an unexpected event. It typically provides alternatives which enable the IT system to serve business processes, at some (even reduced) level. Its basic concept is to minimize damage coming from the stoppage of business processes defined according to BCI/BIA.
When creating a DRP, it is a typical mistake to concentrate on the information serving infrastructure only. In this case all business processes are considered equal, everything is equally important, everything must work. The order of restoration is not based either on the business impact of the processes served or iterdependencies. However, it is much better than nothing, and it can even be sufficient in some cases when the only purpose is the restoration of required service in the shortest possible time.
In an ideal case, DRP relates to the BCP plan: it is exploring organizational processes and considers their connections and the effects they make on each other. A really good DRP plan requires the exploration of all organizational processes.

## 7. Information security and the human factor

The need for information security in an organization usually comes from IT, and during organizational evolution, remains on this level for a long time. This approach is usually the technocratic kind: strongly concentrates on data storage, regualr backup, firewalls and virus protection… On the other hand, it typically neglects the risks of the human factor, and physical protection is also reduced to an alert and entry system for the office building. On this level, information has two classification

categories: important (with backup save) and not important. In a less than ideal case, everything is backed up and no classification is done. It is a common mistake with critical infrastructures, too. („everything is important, no need for classification"). However, at this point we must already see that this approach is essentially wrong: it does not allow the detection of effects exerted on procedures and thus precludes risk handling.

However, risks are mostly caused by the human factor. Even though standards and regulations are placing emphasis on both physical defence and the human side, this issue is usually neglected. As Pál Michelberger states: "They [the errors coming from the human factor] can not be fully eliminated but it is possible to reduce them by a good human resources policy. Information security considerations can and should be integrated into the regulation of selecting, admitting and dismissing employees."

The training and awareness of employees (mostly employees involved in operating and emergency response) is very important, however, in my opinion, it is much more effective to build a system which requires only a minimal amount of thinking in the case of a catastrophy, during the implementation of a DRP plan. Of course there are events not covered the DRP, and in these cases, the efffectivity of salvaging depends heavily on the knowledge and routine of implementing employees. However, in general, a system which is covering events by written procedures has a much better stability.

If we set aside special cases and concentrate on normal business we still find that a significant part of threats to information infrastructure are caused by amployees (Michelberger et al., 2013). These threats can not be fully eliminated but they should be minimalised. The training of users is vital. The danger caused by a negligent administrator is totally different from that of a vengeful system administrator. It is an interesting issue that generation gap might play some role in information security as a part of the human factor.

According to sociologist and marketing professionals, employees may fall into any of the following five characteristic categories by date of birth (Lancaster-Stillmann, 2010):

- veterans
- „baby boom"generation (born between 1946 és 1965)
- generation X (born between 1965-1980)
- generation Y (born between 1980-1995)
- generation Z (born after 1995)

There are no general rules, and there are a lot of exceptions, however, each group has a specific approach to information technology, so categorization might be useful for IT security aspects in case of a large number of employees. Veterans were born long time ago and they were already quite old when information technology became widespread. Using modern communication and information technology is a challenge for them. Most of them are already retired. embers of the baby-boom generation are usually loyal to their employer but it is difficult for them to follow the constant development of information technology. They may also have deficiencies in their technical knowlenge so they can create damage by mistake.
The tipical member of generation X is independent. They usually throw away the security regulations („They know it better"). They have the knowlenge so they may create damage by malice. The memebers of Generation Y are the children of the Information Age. They are the people who rather use Google instead of waiting for a call center in Bangladesh. They frequently download, without encryption, confidential corporate information to their private mobile devices.
The members of generation Z are born into the world of internet, they expect and require a constant online presence. A traditionally high-security workplace is tearing them out of their natural medium.
Generation differences and age group caharacteristics must be considered when regulating information security (Kelemen, 2008).

## 8. Training and education

As I have already pointed out, the technical staff operating the information technology are usually aware of threats, even if they do not acknowledge its non-technical side. The biggest threat for the information vault of an organization is usually not deliberate sabotage but the lack of security awareness and prudence. Improving information security awareness is vital. Internet has become the primary source of information and paper-based catalogues have practically diappeared. Information comes from the manufacturer's web page but even supply chains rely heavily on Internet (e.g. webEDI). Nowadays it is almost impossible for an organization to exclude internet, even without the protest of X and Z generation members.
The most neglected part of information technology investments is the education of users. Trainings rarely consider the special needs of organizational units, and system administrators who typically manage internal trainings are not necessarily prepared in training methodologies. Follow-up trainings are usually forgotten too. It is very common to try handling basic problems with technology: too simple and

rarely changed passwords with authentication hardware and single-use passwords; logging-in with someone else's user by biometric identification, etc. However, these methods are only aimed at the symptoms. This might help to force users to use secure passwords but it does very little to improve awareness.

**Summary**

In my study I have reviewed the widely used de facto and de jure standards in the field of information security while also investigated the experience with them. It can be stated that today's process-based approach is able to cater for the special requirements of critical infrasrtuctures.
However they might need a little adjustment: It is not always reasonable to handle some types of costs as „infinite" (e.g. COBIT's snallest harm). It is a much better solution to create categories for the needs and place each of them into the right category. (ISO/IEC 14598)
The future belongs to process-based, integrated qualtiy control systems. I hink that information security can be handled well within the scope of existing information security standard ISO/IEC 27xxx while we can handle the specialities of the critical infrasturcures with special BCP / DRP plans which are more detailed than the usual ones.

**References**

[1] Dr. Michelberger Pál - Lábodi Csaba: Vállalkozásfejlesztés a XXI. Században, Budapest, 2012.

[2] Godányi Géza: Katasztrófavédelem és üzletmenet folytonosság az információtechnológiában (A DR/BC tervezés alapjai). Híradástechnika, LIX. ÉVFOLYAM 2004/4, pp. 47-52.

[3] Pál MICHELBERGER, József BEINSCHRÓTH, Gergely Krisztián HORVÁTH: THE EMPLOYE – AN INFORMATION SECURITY RISK. Acta Oeconomica, Universitatis Selye, 2013, Komárno, pp. 187-200

[4] Tóth Tibor (szerk.): Minőségmenedzsment és informatika, Műszaki Könyvkiadó – Magyar Minőség Társaság, Budapest, 1999

[5] Dr Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23.

[6] Ji-Yeu Park – Robles, Rosslin John - Chang-Hwa Hong – Sang-Soo Yeo –Tai-hoon Kim: IT Security Strategies for SME's, International Journal of Software Engineering and its Applications, Vol. 2. No. 3., July. 2008, pp. 91-98

[7] Lynne C. Lancaster (Author), David Stillman (Author): The M-Factor: How the Millennial Generation Is Rocking the Workplace, HarperCollins, 2010

[8] Kelemen László: Nem sztereotípiák, IT-business, 2008. szeptember 28, VI évf. 37. sz. 32. oldal

[9] http://www.iso27001security.com/ Retrieved 18 December 2013.

[10] European Network and Information Security Agency – ENISA (November 2010): How to Raise Information Security Awareness (The new users' guide p. 140). Available at: http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide letöltés: 2013 november

[11] Intrieri, Charles (10 September 2013). "Business Continuity Planning". Flevy. Retrieved 18 December 2013.

***Prisznyák Szabolcs[22]: A BVOP informatikai rendszerének kockázatelemzése***

**Absztrakt**
*A cikk bemutatja a büntetés-végrehajtási szervezetnél megvalósított informatikai fejlesztést. A centralizált rendszerek üzemeltetése során újabb kockázatok váltak ismertté. Ezt követően ismerteti a Büntetés-végrehajtás Országos Parancsnokságának informatikai rendszerére vonatkozó kockázatelemzést. Az elemzés az ISO/IEC 27005 (2008) szabvány előírásai szerint készült. A cikk végén összegzi a tapasztalatokat, továbbá ismerteti a szükséges fejlesztési lehetőségeket.*

**Abstract**
*The article presents the IT-development at the Hungarian Prison Service. At the operational of centralized IT-system transpired several new risks. After then the author shows the risk analysis of headquarters of Hungarian prison system by ISO/IEC 27005 (2008) standard. The author concludes the article by summarising the experience gained and outlining the prospects for further development.*

## 1. Bevezetés

A büntetés-végrehajtási szervezet informatikai történetében mérföldkőnek számít a „Felelősen, felkészülten a büntetés-végrehajtásban” elnevezésű, EKOP-1.1.6-09-2009-0001 azonosítószámú, az Európai Unió támogatásával megvalósult informatikai fejlesztési projekt [1]. A projekt keretében közel 1,5 milliárd forint értékben megújult a büntetés-végrehajtási szervezet teljes informatikai rendszere. A fejlesztés azonban olyan rendszertechnológiai változásokat is magával hozott, amely újabb feladat elé állítja a szakembereket a nagy rendelkezésre állású központi informatikai üzemeltetés megvalósítása során.
Jelen publikációban bemutatom a megvalósított fejlesztés elemeit, illetve ismertetem, hogy ennek – *és a változásokhoz illeszkedő rendszerlogikai módosítások* - eredményeként összességében milyen rendszertechnológiai, logikai változások következtek be[2]. Az erősen centralizálttá vált rendszer esetében kulcsfontosságú, hogy a Büntetés-végrehajtás Országos Parancsnokságának (BVOP) informatikai központja nagy rendelkezésre állással szolgálja ki a teljes szervezet információigényét. A rendelkezésre állás biztosításához szükséges felmérni a BVOP-n meglévő kockázatokat. A felmérés első lépéseként az egyes helyiségeket kockázati csoportokba kell sorolni az informatikai rendszer működése

[22] prisznyak.szabolcs@bv.gov.hu

szempontjából megvalósított funkcióik szerint. Ezt követően történhet meg a funkciók szerint csoportosított helyiségek kockázatelemzése az IEC/ISO 27005 (2008) szabvány szerint. A kockázatelemzést teljes egészében a központi gépterem esetében végzem el, minden további helyiségcsoport esetében csak a releváns és/vagy fejlesztésre szoruló elemeket ismertetem.

Összképet adok a nagy rendelkezésre állást biztosító működés feltételeinek meglétéről, illetve ismertetem a szükséges fejlesztéseket.

A cikk elkészítéséhez feldolgoztam a témakörrel kapcsolatos tudományos publikációkat, valamint a kapcsolódó jogszabályokat. Az objektív kockázatelemzéshez figyelembe vettem Kerti András közleményében foglaltakat.[3] Tanulmányoztam a jelzett fejlesztés során keletkezett műszaki dokumentációkat. A több éves projektben, mint a BVOP informatikai fejlesztési osztályvezetője vettem részt. Ennek következtében munkám során a legfontosabb támaszomat a megvalósítás és az üzemeltetés során szerzett személyes szakmai tapasztalatok jelentették.

## 2. A büntetés-végrehajtás szervezeti felépítése

A büntetés-végrehajtás állami, fegyveres, rendvédelmi szerv, amely külön jogszabályban meghatározott szabadságelvonással járó, büntetéseket, intézkedéseket, valamint büntetőeljárási kényszerintézkedéseket, továbbá elzárást hajt végre [4].
A büntetés-végrehajtási szervezet kormányzati irányítását a Belügyminisztérium végzi. A büntetés-végrehajtási szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, amely főosztályai révén a büntetés-végrehajtási intézetekben folyó szakmai munka felügyeletét, ellenőrzését végzi. A büntetés-végrehajtási intézetek ellátják a büntetések és intézkedések végrehajtásával kapcsolatos feladatokat. A büntetés-végrehajtás a legtöbb magyarországi közigazgatási és rendvédelmi szervezettől eltérően nem három, hanem kétszintű szervezet. A központi (országos) szervezet alárendeltségébe közvetlenül a területi jogállású szervezetek tartoznak. Nem jelennek meg a helyi szervezeti egységek, ellentétben pl. a rendőrséggel vagy a katasztrófavédelmi szervezettel. [5]
Magyarországon 28 önálló jogállású büntetés-végrehajtási intézet, öt – *egészségügyi és oktatási* – intézmény, valamint 11 gazdasági társaság működik. Az informatikai szakterület kompetenciája a gazdasági társaságokra nem terjed ki,

azok a büntetés-végrehajtási szervezet informatikai rendszerétől független önálló, elszigetelt rendszereket alakítottak ki. [6]

## 3. A fejlesztés megvalósítása

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtási szervezet eddigi legnagyobb és legátfogóbb informatikai beruházása. Ha hálózatokról beszélünk, külön kell választani a helyi hálózatokat (LAN), és a táv-adatátviteli hálózatot (WAN). Az EKOP-1.1.6 projekt keretében a helyi hálózatok fejlesztésére volt lehetőség. A táv-adatátviteli (WAN) hálózatot külső – *kormányzati* – szolgáltató üzemelteti, ugyanis a 346/2010 (XII.28.) Kormányrendelet 3.§ (1) bekezdés értelmében „…kormányzati célú hírközlési tevékenységet kizárólag a kormányzati célú hírközlési szolgáltató és az elkülönült hírközlési tevékenység végzésére jogosultak végezhetnek.” [7] A hivatkozott kormányrendelet nevesíti a kormányzati célú hírközlési szolgáltatót, amely a Nemzeti Infokommunikációs Szolgáltató Zrt. A helyi hálózatok fejlesztésénél elsődleges cél volt a homogén aktív eszköz park kialakítása. Ennek értelmében valamennyi switch cserére került, az új eszközök azonos gyártónak a termékei. Végeredményben modern, szabványos helyi hálózatok álltak rendelkezésre, amelyek kialakítása szakszerűen, igényesen történt. A szerverpark kialakítása során a BVOP-n – *a már meglévő gépteremben, amelynek kialakítására 2007-ben került sor* – egy blade centerben 10 db új szerver üzembeállításával történt a központi infrastruktúra kialakítása. Az intézetek részére összesen 128 db rack szekrénybe helyezhető szerver került beszerzésre. Ez intézetenként 4 db szervert jelent (a pályázat benyújtásának időpontjában működő 32 intézettel számolva). Munkaállomás oldalon szintén a szerverekkel azonos gyártótól kerültek beszerzésre az eszközök. A projekt keretében összesen 1200 db vékonykliens, 300 db asztali munkaállomás, valamint a működésükhöz szükséges 1500 db LCD monitor illetve 100 db notebook került beszerzésre. A fejlesztéssel elértük, hogy egységes szerver infrastruktúra áll rendelkezésre, amely konszolidált módon, valamennyi helyszínen klimatizált gépteremben került elhelyezésre. A munkaállomások nagy része cserére került, így a karakteres Unix terminálok helyett megjelentek a grafikus operációs rendszerek és felhasználói programok futtatására is alkalmas eszközök. Az azonos gyártótól származó eszközök biztosítják a homogenitást, interoperabilitást, a felcserélhetőséget, átcsoportosíthatóságot. A rendelkezésre állást biztosító eszközcsoport részeként beszerzésre került valamennyi szerverpark mellé 1 db szünetmentes tápegység, amely áramkimaradás esetén – *terheléstől függően* – 5-15 percig képes a folyamatos működést biztosítani. Ez elegendő lehet a pillanatnyi áramkimaradások áthidalására, illetve hosszabb

áramkimaradás esetén elegendő áthidalási időt biztosít az áramfejlesztő készülék (aggregátor) indulásáig. Egységes platformra került az intézeti adatmentés is, egy jó minőségű hálózati mentőegység beszerzésével, és üzembeállításával. Ez az eszköz elegendő a teljes intézeti adatvagyont növekményes mentésére, szükség esetén visszaállítására. A BVOP-n pedig egy nagy teljesítményű áramfejlesztő berendezés került telepítésre, amely áramkimaradás esetén a központi gépterem mellett a telefonközpont, valamint a 24 órában üzemelő ügyeleti helyiségek informatikai és biztonságtechnikai eszközeit is képes kiszolgálni.
A szoftver alapinfrastruktúrát tekintve a korábbi heterogén működés felszámolásra került. Kialakítottuk az országos címtárat, amelyet Microsoft Active Directoryval valósítottuk meg. Valamennyi szerveren Microsoft Windows Server 2008R2 operációs rendszer fut. Munkaállomás oldalon a vastag klienseken Windows 7 Professional operációs rendszer és Microsoft Office 2010 irodai programcsomag került telepítésre. A vékonyklienseken egy speciális Linux típusú operációs rendszer – *eLux RL Lite* – fut, amelynek alapfunkciója, hogy RDP kliensként képes terminal szerverhez kapcsolódni. Fontos eredmény, hogy valamennyi adat és program központi tárolásúvá vált, így lehetőség nyílt az adatvagyon képzésre, ennek redundáns tárolására, mentésére. Az állománystruktúra a büntetés-végrehajtási szervezet Szervezeti Működési Szabályzatnak [8] megfelelő hierarchia szerint került kialakításra.
Az alkalmazásfejlesztések során megvalósult a FŐNIX rendszer, amely a korábbi fogvatartotti alrendszer korszerűsítése, rendszertechnológiai megújítása, funkcionális bővítése.
Szintén megvalósult a humán erőforrás adminisztrációt támogató alrendszer korszerűsítése, funkcionális bővítése. Ez a rendszer egy általános személyügyi rendszer követelményein túl megfelel a büntetés-végrehajtási szervezet – *jogszabályból következő [9]* – speciális igényeinek is, ennek alapján a következő modulokból épül fel: személyügyi modul, szolgálatszervezési modul, fegyelmi modul, egészségügyi-, fizikai-, pszichikai állapotfelmérés nyilvántartása modul. Mindkét rendszer esetében azonos a központban történő programfuttatás, adattárolás, valamint a szerepkörök szerinti differenciált hozzáférés, amelynek alapja az Active Directory.

## 4. A BVOP helyiségeinek besorolása funkciók alapján

A fejlesztés eredményeként a büntetés-végrehajtási szervezet teljes informatikai környezete megváltozott. A korábbi decentralizált szigetszerű informatikai rendszerek helyett egy erősen központosított megoldás került kialakításra. Az új

megoldás egységes, homogén rendszer, azonban üzemeltetési szempontból kulcsfontosságúvá vált a BVOP informatikai központjának elérése. A minél nagyobb rendelkezésre állás biztosításához szükséges a BVOP kockázatelemzése az informatikai rendszer vonatkozásában. A kockázatelemzés során legcélszerűbb az IEC/ISO 27005 (2008) szabvány előírásait alkalmazni. A kockázatelemzés megkezdése előtt a BVOP helyiségeit az informatikai üzemeltetés szempontjából betöltött funkcióik szerinti csoportokba kell sorolni, hiszen, az egyes helyiségekre funkcióik szerint értelmezhetők a kockázatok. A helyiségek csoportokba sorolása az alábbi táblázatban látható.

**BVOP helyiségeinek kategóriákba sorolása**
az informatikai rendszer működésének szempontjából betöltött funkció szerint

| funkció meghatározása | helyiség | megjegyzés |
|---|---|---|
| az informatikai rendszer működése szempontjából kulcsfontosságú helyiség | központi gépterem | földszinti elhelyezkedés |
| | telefonközpont | - |
| kulcsfontosságú támogató berendezések | szünetmentes tápegység helyisége | pince szinten elhelyezve |
| | aggregátor helyiség | pince szinten elhelyezve |
| | klímaberendezés (kültéri egység) | kültéri légudvarban elhelyezve |
| kulcsfontosságú helyi és távoli kommunikációt biztosító helyiségek | rack szekrény (vidéki kapcsolat) | - |
| | rack szekrények (helyi hálózat) | az épületben több helyen |
| kulcsfontosságú szolgálati helyiségek (24órás szolgálat) | ügyeletes tiszti helyiség | |
| | kapuügyelet | földszinti elhelyezkedés |
| általános célú szolgálati helyiségek | valamennyi iroda és egyéb célú helyiség | - |

A BVOP Budapesten található az V. kerület Steindl Imre utca 8. szám alatt. Az épülethez tartozik a szomszédos Steindl Imre utca 10. szám alatt található épület is. Az épületek teljes beépítésű területen találhatóak, így teljesen egymáshoz épültek. Mindkét épületben találhatók irodák, illetve az informatikai működést befolyásoló helyiségek. A legfontosabb helyiség a központi gépterem, amelyben az informatikai működés központja található, kiesése a büntetés-végrehajtási szervezet informatikai működését rövid időn belül ellehetetleníti. Szintén fontos a telefonközpont, amely a kommunikáció alapját jelenti. A fontossági sorrendben az üzemeltetés alapjait képező rendszerek után azok a gépek, berendezések, megoldások következnek, amelyek az üzemeltetést biztosítják valamilyen rendkívüli helyzetben. Egy informatikai rendszerben *különösen egy erősen centralizált környezetben* – kulcsfontosságú a hálózatok működése, hiszen nélkülük nem érhetők el a központi adattárak, programok, ezért a hálózati aktív eszközök (útválasztók, kapcsolók) külön egységet képeznek. A szervezet dolgozói által használt helyiségek – *irodák és egyéb célú helyiségek* – közül a szervezet rendeltetésszerű működése szempontjából kiemeltek a 24 órás ügyeleti szolgálati tevékenységet folytató állomány elhelyezését, munkavégzését biztosító helyiségek.

## 5. A BVOP kockázatelemzése

A kockázatok elemzését az ISO/IEC 27005 (2008) szabvány C függelékében foglalt „Leggyakoribb fenyegetések” alapján végzem [4]. Az elemzés rendszer szintű kockázatelemzés, bizonyos esetekben – *amennyiben az szükséges* – részletes kockázatelemzésre is sor kerülhet. Az egyes fenyegetések bekövetkezésének valószínűségét 1-5 skálán sorolom be, ahol a bekövetkezés legkisebb valószínűsége 1. Ezt követően ismertetem a környezeti tényezőket és/vagy a tett intézkedéseket. Amennyiben szükséges ismertetem a kockázatok valószínűségének és/vagy hatásának csökkentéséhez esetlegesen szükséges további intézkedéseket.

**Központi gépterem**

**Fizikai károk**

*Tűzkár:* bekövetkezés valószínűsége: 2

A helyiségnek megtörtént a tűzveszélyességi besorolása, a helyiségben éghető anyagok tárolása nem történik, a helyiség tűzálló ajtóval védett. A helyiségben automatikus oltóberendezés működik.

További intézkedés nem szükséges.

*Vízkár:* bekövetkezés valószínűsége: 1

Sem a helyiségben, sem a közvetlen környezetében – *alatta, fölötte, mellette* – nincs vízvezeték. A helyiségben nincs központi fűtés. A helyiség vízszint érzékelővel felszerelt, amely – *a padozaton víz jelenléte esetén* – riasztást végez. További intézkedés nem szükséges.

*Szennyezés okozta kár:* nem releváns esemény, bekövetkezés valószínűsége: 1.

*Berendezések megrongálódása, elvesztése:* bekövetkezés valószínűsége: 3.

Az informatikai berendezések használat során tönkremehetnek, ennek ellensúlyozására a rendszerek szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre.

Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén.

*Por, rozsda, fagyás okozta károk:* bekövetkezés valószínűsége: 1

A por és rozsda okozta károk nem releváns események. A fagyás valószínűsége is rendkívül alacsony, szükség esetén a redundáns klímaberendezések fűtésre is alkalmasak.

**Természeti esemény**

*Éghajlati jelenség*: Magyarország éghajlata kontinentális, szélsőséges éghajlati jelenségek előfordulása nem jellemző, így a kockázat nem releváns.

*Szeizmikus jelenség:* Magyarországon a szeizmikus jelenségek (földrengések) nem jellemzőek, így a kockázat nem releváns.

*Vulkanikus jelenség:* Magyarország területén nincs működő vulkán, a kockázat nem releváns.

*Meteorológiai jelenség:* bekövetkezés valószínűsége: 1

A meteorológiai jelenségek közül a villámcsapás, amely lehetséges fenyegetés, ellene az épület villámvédelmének kiépítésével védekezünk, amely megfelelő műszaki színvonalon megoldott.

További intézkedés nem szükséges.

*Árvíz okozta károk:* bekövetkezés valószínűsége: kevesebb, mint 1.

Az árvíz nem releváns fenyegetés, mert a BVOP épülete magasabban fekszik, mint a legmagasabb mért árvíz plusz egy méter, nagyon alacsony kockázati tényezőt jelent, hogy az épület a Dunától kb. 150 méter távolságra található, így esetleges kockázatot jelenthet egy árvíz másodlagos hatása.

További intézkedés nem szükséges.

**Kulcsfontosságú szolgáltatás kiesése**

*Légkondicionáló vagy a vízvezeték rendszer meghibásodása okozta kár:* bekövetkezés valószínűsége: 2

A vízvezetékrendszer meghibásodása nem releváns az informatikai rendszer működése szempontjából.

A gépterembe 2013-ban új légkondicionáló berendezések kerültek telepítésre. A berendezések rendszeresen ellenőrzöttek karbantartottak. Két berendezés működik párhuzamosan, egyik kiesése esetén a tovább működő egység képes biztosítani a megfelelő működési hőmérsékletet.

További intézkedés nem szükséges.

*Áramellátás hibája (áramszünet):* bekövetkezés valószínűsége: 3

A BVOP épülete a múlt század elején épült, villamosítása az 1940-es, 1950-es években történhetett, azóta csak egyes szakaszok újjáépítése, javítása, bővítése történt meg. Az épület teljes elektromos felújítására évtizedek óta nem került sor. A kockázatot tovább növeli, hogy a belvárosban az épület környékén több nagy volumenű ingatlanfejlesztés is zajlik, és az építkezések során több esetben előfordul figyelmetlenségből vagy a megfelelő műszaki dokumentumok hiányából adódó vétlen nagyfeszültségű vezetékrongálás, amely áramkimaradást eredményezhet.

A kockázatot csökkenti, hogy az informatikai központ teljes nagyfeszültségű kábelrendszere megújításra került, a BVOP épületének további rendszeritől függetlenítve. Beszerzésre került egy szünetmentes tápegység, amely a központi géptermet ellátja. Szintén beszerzésre került egy nagy teljesítményű áramfejlesztő berendezés (aggregátor), amely áramkimaradás esetén is biztosítja a központi gépterem áramellátását.

További szükséges intézkedések: szünetmentes tápegység kapacitásának növelése.

*Telekommunikációs berendezések meghibásodása:* bekövetkezés valószínűsége: 3

A telekommunikációs berendezések a BVOP telefonközpont rendellenes működéséből következhetnek.

A telefonközpont redundáns. Meghibásodás esetén a tartalékegység (amely egy büntetés-végrehajtási intézetben található) automatikusan átveszi a vezérlést.

További szükséges intézkedések: a telefonközpont teljes és alapos felülvizsgálata az üzemeltető NISZ Zrt. által a hibás működés esetszámának csökkentése érdekében. A redundancia logikájának felülvizsgálata, az automatikus folyamatok üzembiztos működésének kialakítása érdekében (jelenleg a rendellenes működést követő helyreállítás legtöbb esetben manuális beavatkozást igényel).

**Sugárzás miatti zavar**

*Elektromágneses sugárzás okozta kár*: a kockázat nem releváns.
*Hő sugárzás okozta kár*: a kockázat nem releváns.
*Elektromágneses impulzus okozta kár*: nem releváns.

**Információ kompromittálódás**

*Kompromittáló kisugárzott jelek elfogása*: a bekövetkezés valószínűsége: 1

A BVOP nem alkalmaz vezeték nélküli eszközöket. A gépterem az épület belső részén helyezkedik el. Az ingatlan területére ellenőrzötten, dokumentáltan történik a beléptetés. A múlt századi építészeti megoldások következtében a 80-100 cm-es falvastagság is csökkenti a jelfelderítés valószínűségét.

További intézkedés nem szükséges.

*Távoli kémkedés okozta kár*: a bekövetkezés valószínűsége: 1

A BVOP a kormányzati hálózat része, amelyet a NISZ Zrt. üzemeltet. A hálózat a távoli behatolás ellen több szintű logikai és fizikai védelemmel ellátott.

További intézkedés nem szükséges.

*Lehallgatás okozta kár:* a bekövetkezés valószínűsége: 1

A lehallgatáshoz a hálózatra fizikailag kell rácsatlakozni. Az épület fent ismertetett védelme jelentősen csökkenti a kockázatot.

További intézkedés nem szükséges.

*Média (adathordozó) vagy dokumentumok ellopása:* a bekövetkezés valószínűsége: 2

A kockázatot elsősorban a saját dolgozók jelentik. Az épületbe, az informatikai helyiségekbe a belépés korlátozott. Az adathordozók biztonságosan tároltak (lemezszekrény, páncélszekrény). A dolgozók tájékoztatása, oktatása megtörtént.

További szükséges intézkedések: Az informatikai biztonsági oktatások számának növelése, rendszeressé tétele, a megszerzett ismeretek ellenőrzése. A dolgozókban a felelősségtudat kialakítása.

*Berendezések ellopása: a bekövetkezés valószínűsége: 2*

A tett és a szükséges intézkedések azonosak a fenti pontban megfogalmazottakkal.

*Kidobott, újrafelhasznált média (adathordozó) helyreállítása:* a bekövetkezés valószínűsége: kevesebb, mint 1

Minden használatból kivont adathordozó esetében adat helyreállítást lehetetlenné tevő roncsolásra kerül sor.

További intézkedés nem szükséges.

*Árulás, információk közzététele:* a bekövetkezés valószínűsége: 2

A dolgozók felkészítése, oktatása megtörtént.

További szükséges intézkedés: további rendszeres oktatások a dolgozók részére, a tudatos magatartás kialakítása.

*Megbízhatatlan forrásból származó adat:* a bekövetkezés valószínűsége: 2

A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe.

További szükséges intézkedések: tudatos magatartás kialakítása oktatással.

*Hardverek működésének befolyásolása*: a bekövetkezés valószínűsége: 2

A központi gépteremben található hardverekhez csak a kijelölt állomány férhet hozzá.

További szükséges intézkedések: tudatos magatartás kialakítása oktatással.

*Szoftverek működésének befolyásolása:* a bekövetkezés valószínűsége: 2

A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A szoftverekhez csak a kijelölt állomány férhet hozzá. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek.

További szükséges intézkedések: tudatos magatartás kialakítása oktatással. A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – *szoftvereket telepítő, üzemeltető* – partnerek esetében a megfelelő együttműködés kialakítása.

*Pozíció (hely) kinyomozása*: a bekövetkezés valószínűsége: 1

A BVOP elhelyezkedése ismert, nyilvános információ, de ebből nem következik egyenesen a központi gépterem elhelyezkedése. A kockázatot csökkenti az épület védelme, a ki- és beléptetés szabályrendszere, annak betartása.

További intézkedés nem szükséges.

**Technikai meghibásodás**

*Eszközök, berendezések meghibásodása*: a bekövetkezés valószínűsége: 2

Az informatikai eszközök, berendezések használatuk során meghibásodhatnak, ennek kezelésére a központi rendszer elemei szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre.

Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén, a rendelkezésre állás további növelése.

*Üzemzavar, hibás működés:* a bekövetkezés valószínűsége: 2

A fenti pontban megfogalmazottakkal azonos intézkedések történtek és szükségesek.

*Információs rendszer telítettsége:* a bekövetkezés valószínűsége: 1

A rendszer folyamatosan ellenőrzött, mind automatikusan, mind humán erőforrás bevonásával. Szükség esetén a rendszerek automatikus megelőző figyelmeztetést küldenek.

További intézkedés nem szükséges.

*Szoftverek hibás működése:* a bekövetkezés valószínűsége: 2

A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek.

További szükséges intézkedések: A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.

*Az információs rendszer helyreállíthatóságának megsértése:* a bekövetkezés valószínűsége: 2

Az adatbázisokról, adatállományokról rendszeres, automatikus, több generációs mentéssel rendelkezünk. A mentések megfelelő helyen őrzöttek. Szükséges intézkedések: mentési rendszer kialakítása távoli telephelyre.

**Illetéktelen cselekedetek**

*Illetéktelen eszközhasználat*: a bekövetkezés valószínűsége: 2

Az eszközök be- és kivitele az épületbe történő be- és kiléptetés során ellenőrzésre kerülnek. A gépterembe történő belépés korlátozott. Az eszközök hálózatra csatlakoztatása sem lehetséges a fizikai címre (MAC address) történő szűrés alapján. Egyes esetekben kockázatot jelenthet az USB alapú eszközök használata.

Szükséges intézkedések: az USB alapú eszközök egyedi azonosító alapján személyekhez rendelt módon történő központi felügyeletének kialakítása.

*Szoftverek illegális másolása*:

nem releváns esemény, bekövetkezés valószínűsége: 1

*Hamis szoftverek használata*: nem releváns esemény, bekövetkezés valószínűsége: 1

*Adatok elrontása (meghamisítása):* a bekövetkezés valószínűsége: 1

A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe.

További szükséges intézkedések: tudatos magatartás kialakítása oktatással.

*Illegális adathasználat (adatfeldolgozás)*: fentivel azonos.

**Funkció kompromittálódása**

*Használat közbeni hiba*: a bekövetkezés valószínűsége: 3

A központi rendszer elemei szinte valamennyi funkciót tekintve redundánsak, illetve szükség esetére tartalék eszköz, alkatrész áll rendelkezésre.

További szükséges intézkedések: újabb redundáns megoldások kialakításának folyamatos vizsgálata.

*Jogokkal való visszaélés*: a bekövetkezés valószínűsége: 2

A jogosultsági rendszer úgy került kialakításra, hogy minden felhasználó csak a munkavégzéséhez szükséges jogosultsággal rendelkezik.

További szükséges intézkedések: tudatos, felelősségteljes magatartás kialakítása oktatással, ellenőrzéssel.

*Jogokról való megfeledkezés*: a bekövetkezés valószínűsége: 2

Fentivel azonos kockázat és intézkedések.

*Tevékenység megtagadás*: a bekövetkezés valószínűsége: 1

A szervezet jellegéből adódóan nem releváns kockázat.

További intézkedés nem szükséges.

*Személyes hozzáférés megakadályozása*: a bekövetkezés valószínűsége: 1

Több személy is rendelkezik rendszerfelügyeletet és rendszerkonfigurációt biztosító jogosultságokkal. A rendszerek jól dokumentáltak. Amennyiben fizikai hozzáférési probléma történik (pl. elromlik a központi gépterem ajtajának zárja és az nem nyitható), annak kijavításáig távoli adminisztrációval biztosítható a rendelkezésre állás. További intézkedés nem szükséges.

**Telefonközpont**

**Fizikai károk**

A fizikai károk közül a tűz okozta kár a legnagyobb kockázatú – *a további felsorolt károk bekövetkezése nem releváns* – bekövetkezésének valószínűsége 3.

További szükséges intézkedések: a központi gépteremhez hasonló tűzvédelemi rendszer kialakítása, úgy, mint tűzbiztos bejárati ajtó, automatikus oltóberendezés.

**Természeti események okozta károk**

Nem releváns.

**Kulcsfontosságú szolgáltatás kiesése okozta károk**

A jelzett elemek közül gyakorlatilag csak az áramkimaradásnak van kockázata. A berendezés szünetmentes tápellátással biztosított, de a biztosító rendszer több esetben rendellenesen működik. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: áramellátás felülvizsgálata a helyiségben.

**Sugárzás miatti zavar**

Nem releváns.

**Információ kompromittálódás**

Azonos kockázatok a központi gépterem esetében felsoroltakkal.

**Technikai meghibásodás**

Azonos kockázatok a központi gépterem esetében felsoroltakkal, azzal az eltéréssel, hogy a telefonközpontot a NISZ Zrt. üzemelteti, így a kockázatok – *részben* – náluk jelentkeznek.

**Illetéktelen cselekedetek**

Azonos kockázatok a központi gépterem esetében felsoroltakkal.

**Funkció kompromittálódása**

Azonos kockázatok a központi gépterem esetében felsoroltakkal.

**Kulcsfontosságú támogató berendezések**

Ezen helyiségek esetében kockázatot jelentenek a fizikai kár jellegű fenyegetések, azonban ezek bekövetkezésének valószínűsége alacsony. Valamennyi berendezés az iparági szabványoknak, előírásoknak megfelelően védett. Az aggregátor helyiségében megfelelő füstgázelvezetés, tűzbiztos bejárati ajtó és automatikus oltóberendezés található. A klímaberendezés esetében a fagyás és a víz (csapadék) okozta károk jelenthetnek minimális kockázatot, de ezek ellen a berendezés elsősorban konstrukciójából következően, másrészt szakszerű telepítéséből és rendszeres időközönként történő ellenőrzéséből, karbantartásából következően védett.

**Kulcsfontosságú helyi és távoli kommunikációt biztosító helyiségek**

A hálózati eszközök (switchek, routerek) esetében kockázatként jelentkezik az áramkimaradás során – *illetve azt követően az áramellátás helyreállása esetén* –

bekövetkező működési problémák, mivel a rack szekrények nem rendelkeznek szünetmentes tápellátással. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: szünetmentes áramellátás biztosítása a hálózati elosztó szekrényekhez.

További kockázatot jelenthet az illetéktelen eszközhasználat, hiszen több rack szekrény a folyosón – *nem zárt területen* – található. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: a rack szekrények zárjainak megerősítése, a hálózati eszközökhöz a fizikai hozzáférés korlátozása, jelző, érzékelő berendezések alkalmazása, a szekrények sértetlenségének rendszeres ellenőrzése.

**Kulcsfontosságú szolgálati helyiségek (24órás szolgálat)**

Ezekben a helyiségekben 24 órás folyamatos munkavégzés zajlik, a helyiségek szünetmentes tápellátással biztosítottak, a kockázatok nem relevánsak.

**Általános célú szolgálati helyiségek**

A kockázatok nem relevánsak, hiszen a rendszer kialakításának köszönhetően adattárolás csak központilag történik, a felhasználói jogosultságok erősen korlátozottak – *kizárólag a szolgálati feladatok elvégzését biztosítják* – így szinte valamennyi kockázat a központi gépteremre vonatkozóan jelentkezik.

## Összegzés

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtás történetének eddigi legnagyobb informatikai fejlesztése. Ebből következően – *mivel az informatika szinte valamennyi munkafolyamat támogatásában érintett* – döntően befolyásolja a szervezet működését. A fejlesztés rendszertechnológiai változásokat is magával hozott, amelynek következtében megváltoztak az informatikai rendszer működésének, elérésnek feltételei is.

Az új – *erősen centralizált* – környezetben kulcsfontosságú, hogy a központi rendszer a lehető legnagyobb rendelkezésre állású legyen. A rendelkezésre állás biztosításához, növeléséhez elengedhetetlen a teljes rendszer, illetve annak egyes elemeinek a felülvizsgálata. Az egyes kockázatok elemzéséhez, a kockázatok bekövetkezési valószínűségének csökkentéséhez, illetve a bekövetkezett események hatásának csökkentéséhez megtett és a jövőben szükséges intézkedések meghatározásához a nemzetközileg elfogadott ISO/IEC 27005 (2008) szabványt választottam. Bízom benn, hogy elemzésem eredményeként rávilágítottam a fejlesztendő területekre, és felszínre kerültek olyan problémák is, amelyek a szabvány következetes – *pontról pontra* – történő alkalmazása nélkül

csak egy már bekövetkezett esemény után derültek volna ki. Véleményem szerint a kockázatelemzés eredményét és módszerét célszerű figyelembe venni más rendvédelmi (és/vagy közigazgatási) szervezet hasonló volumenű informatikai fejlesztése, vagy a meglévő rendszerek vizsgálata során. A szabványban meghatározott elvek és módszerek alkalmazásával magasabb rendelkezésre állású, biztonságosabban üzemeltethető informatikai infrastruktúrák alakíthatók ki.

**Felhasznált és hivatkozott irodalom:**

[1] SEBESTYÉN Attila: *Büntetés-végrehajtás informatikai fejlesztési projekt.* = Kommunikáció 2009, 2009 Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó - ISBN 978-963-7060-70-0

[2] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[3] KERTI András: Az információbiztonsági kockázatkezelés oktatásának buktatói in: Kommunikáció 2013: Communications 2013, 2013 Nemzeti Közszolgálati Egyetem, pp. 53-60. - ISBN:978-615-5305-16-0

[4] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről

[5] Dr. Rajnai Zoltán, Bleier Attila: **Technical problems in the IP communication systems of the Hungarian Army**, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., ZMNE, Budapest, 2010

[6]346/2010 (XII.28.) Kormányrendelet a kormányzati célú hálózatokról 3.§ (1)

[7] A büntetés-végrehajtás országos parancsnokának 1/2011. (V.6.) BVOP utasítása a Büntetés-végrehajtás Országos Parancsnoksága Szervezeti és Működési Szabályzatának kiadásáról

[8] 1996. évi XLIII. törvény a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

[9] International Standard ISO/IEC 27005 Information technology – Securtity techniques – Information security risk management

***Dr. Kerti András - Szente András: Információbiztonsági szabványok***

**Absztrakt**
*Az azonos tevékenységeket folytató szervezetek működésének összemérhetőségének biztosításához különböző szabványokat hoztak létre a különböző szabványosítási szervezetek. Ebben a cikkben a különböző információbiztonsági szabványokat foglaljuk össze.*

**Abstract**
*Comparable to the functioning of the organizations engaged in the same activities to ensure the various standards established by the various standardisation organizations.*
*In this article, a variety of information security standards are summarized.*

## 1. Bevezetés

Az információbiztonsággal foglalkozó szabványok, szervezetek száma és sokszínűsége dinamikusan fejlődött az utóbbi ötven évben. Ennek szükségszerűségét a műszaki, informatikai fejlődés indokolta. Kapcsolatrendszerük, tartalmi összetevőik feltérképezése jogi és műszaki ismereteket egyaránt megkövetel.
A Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO) 1947-es megalakulásakor az IEC-vel (International Elektrotechnika Comission, Nemzetközi Elektrotechnikai Bizottság, 1906) társulási megállapodást kötött. Az ISO munkáját az egyes szervezetek által delegált tagokkal kibővített Technikai Bizottságokban (TC-k) végzik. Az ötvenes évektől az egyes szakterületek tovább specializálódtak, ezért - a munka hatékonyabbá tétele és gyorsítása érdekében - a TC-ken belül albizottságok (Sub-Committees, SC-k) alakultak. A tagszervezetek egyre több nemzetközi TC/SC-titkárság működtetését vállalták fel, az adott ország ipari érdekeiknek megfelelően. Olyan javaslatok kerülnek szabványosításra az ISO-ban, amelyet legalább a tagországok 75% - a elfogad.

## 2. Mi a „szabvány”, miért volt szükség a szabványosításra?

Magyarországon az 1995. évi XXVIII. írja elő a nemzeti szabványosítást, és így fogalmaz: "A szabvány elismert szervezet által alkotott vagy jóváhagyott, közmegegyezéssel elfogadott olyan műszaki (technikai) dokumentum, amely

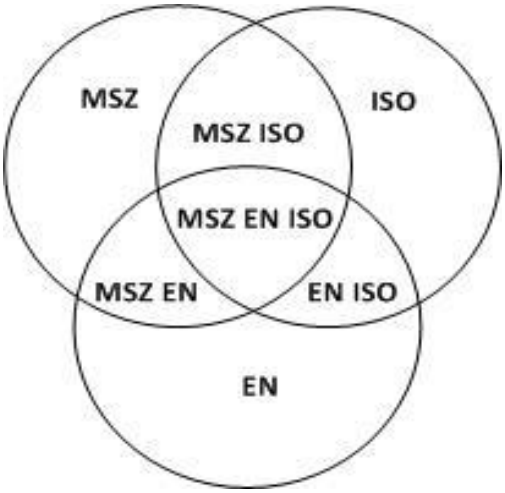
tevékenységre vagy azok eredményére vonatkozik, olyan általános és ismételten alkalmazható szabályokat, útmutatókat vagy jellemzőket tartalmaz, amely alkalmazásával a rendező hatás az adott feltételek között a legkedvezőbb". A szabványok sorolhatók vállalati, iparági, nemzeti, regionális, illetve nemzetközi kategóriákba.

A szabvány a minőség alappillére, amellyel a termékre, szolgáltatásra nézve minőségi követelményeket írunk elő, betartásával a gyártó és felhasználó előnyöket élvez. Ilyen előnyök, előnyös tulajdonságok: kompatibilitás, cserészabatosság, azonosíthatóság, termékvédelem, biztonság, környezetvédelem, választékrendezés, azonos módon elvégzett bevizsgálás, rendeltetésszerű használatra való alkalmasság igazolása, kölcsönös megérhetőség. A Magyar Szabványügyi Testület (MSZT) az IEC teljes jogú tagja. Az IEC szabványtervezetek hazai észrevételezése, szavazása az MSZT elektrotechnikai területen működő 44 db műszaki bizottságának (MSZT/MB-nek) a feladata. E bizottságok az IEC TC/SC-k „tükörbizottságaiként" is dolgoznak; egy-egy MSZT/MB általában több IEC (illetve európai szinten CENELEC) TC/SC szakterületét fogja át. Az IEC-munkában való részvétel nagyon lényeges, ennek során van lehetőségünk a hazai érdekek európai szintű érvényesítésére is, ugyanis a kötelezően bevezetendő európai elektrotechnikai (CENELEC) szabványok 77%-a az IEC - szabványok (jóváhagyó közleményes) átvétele. A hazai szabványok jele MSZ, ezt követi a sorszáma, esetleg szabványon belüli szabványként új törés, majd a kibocsátás éve. Az 1995 évi törvény szerint a nemzeti szabványosítással kell elősegíteni:

- az általános és ismételten alkalmazható eljárások, műszaki megoldások közrebocsátásával a termelés korszerűsítését, a szolgáltatások színvonalának javítását,
- a nemzetgazdasági igények érvényesítését a nemzetközi és az európai szabványosítási tevékenységben,
- a kereskedelem műszaki akadályainak elhárítását,
- a műszaki fejlesztés eredményeinek széleskörű bevezetését,
- az élet, az egészség, a környezet, a vagyon, a fogyasztói érdekek védelmét és a biztonságot,
- a megfelelőség tanúsítás követelményrendszerének kialakítását,
- a hazai termékek és szolgáltatások nemzetközi elismertetését.

A regionális szabványosítás színtere Európa, szervezetei a CEN (Comité Européen de Normalisation), mely az Unión belüli szabványokat adja ki a tagországok beleegyezésével, a CENELEC (Comité Européen de Normalisation Électrotechnique), az európai villamos szabványok kibocsátója, és az ETSI (Eurpean Telecommunications Standards Institute) a távközlési szabványokat adja ki. Az

európai szabványosítás főbb alapelvei: nyitottság és áttekinthetőség, közmegegyezés, minden érdekelt fél részt vehet a fejlesztésében, nemzeti elkötelezettség. A nemzetközi, európai, és hazai szabványok viszonyát az 1. ábra szemlélteti (forrás: http://mmfk.nyf.hu/min/alap/15.htm).




1. sz. ábra

Az információbiztonság szabványai közül mérföldkőnek tekinthető az ISO 27000 család, a COBIT, a Common Criteria, valamint a PCI DSS. Az ISO/IEC 27000-es szabványcsalád alapjául a Brit Szabványügyi Hivatal (BSI - British Standard Institute) által 1999-ben kiadott BS 7799 szabvány szolgált, mely több frissítési generáció után vált a Nemzetközi Szabványügyi Szervezet (ISO) által kiadott információ biztonság területén nemzetközileg is elfogadott és elismert ISO szabvány sorozatba illeszkedő gyűjteménnyé. (A szabványcsalád elemeinek felsorolása, valamint az ISO informatikai bizottságainak felsorolása a mellékletben található). Az ISO/IEC informatikai bizottságai közül az ISO/IEC JTC1 (ISO/IEC Informatikai Egyesült Technológiai Bizottsága) feladata IT rendszerek fejlesztése, tervezése. Ezen rendszerek minőségének, teljesítményének, biztonságának folyamatos növelése, egységes eszközpark, környezet, szókincs kidolgozása. Felhasználói felületek felhasználócentrikus, ergonómiai jellemzőinek javítása. Alapelvei: üzleti megközelítés (költséghatékonyság), minőségi termékek és szolgáltatások, multikulturális környezetben történő megfelelőség biztosítása. Más szervezetek munkájának elismerése, beépítése, továbbfejlesztése, szabványosítás, a termékek nemzetközi kereskedelmének előmozdítása.

A bizottságok alatt albizottságok működnek. Az ISO és IEC közös műszaki bizottságának (JTC1) SC27 nevű albizottsága, ahol a legtöbb és legátfogóbb, az információvédelem minden szintjére kiterjedő, kiemelkedő nemzetközi jóváhagyást élvező szabványt jelentetnek meg az információvédelem területén.
Az SC27 alapján az információvédelem munkaterületei:

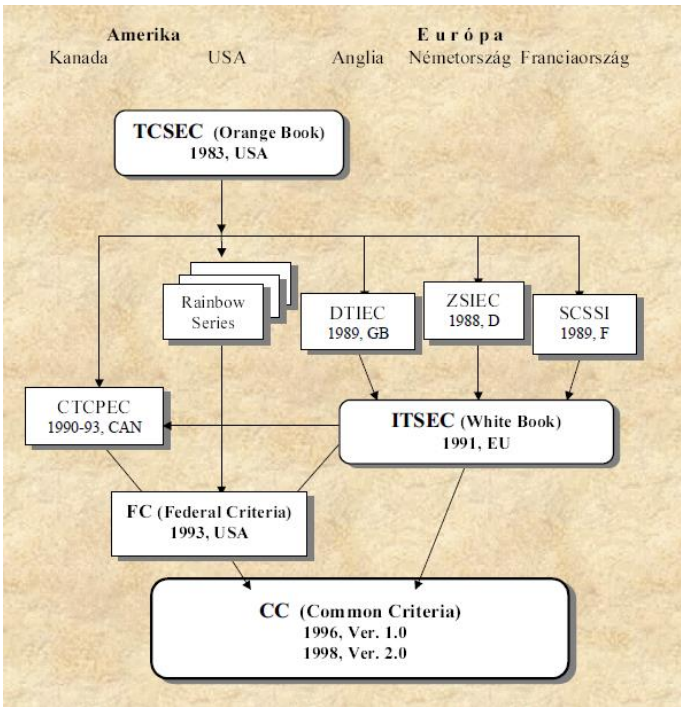
| | |
|---|---|
| ISO/IEC JTC 1/SC 27/WG 1 | Információbiztonsági irányítási rendszerek (ISO/IEC 27001) |
| ISO/IEC JTC 1/SC 27/WG 2 | Kriptográfia és biztonsági mechanizmusok |
| ISO/IEC JTC 1/SC 27/WG 3 | Biztonsági értékelés, tesztelés, specifikáció |
| ISO/IEC JTC 1/SC 27/WG 4 | Biztonsági ellenőrzések és szolgáltatások |
| ISO/IEC JTC 1/SC 27/WG 5 | Személyazonosság kezelés |

A **Common Criteria** honlapja, a http://www.commoncriteriaportal.org **főoldal** tartalmazza az általános bemutatást, a tanúsítványt jóváhagyó, illetve felhasználó országokat. Itt található a minősített laboratóriumok felsorolása és elérhetősége, országonként. Maga a dokumentum, a CC 2.3 változat, illetve a CC 3.1 verzió 3-as és 4-es kiadása. Betekinthetünk a **CC** valamint a **CEM** (Ez a „közös szempontrendszer" kiértékelést szabályzó kézikönyv) karbantartási, fejlesztési folyamatába, valamint a **CCRA** (Ez a CC Irányító Bizottság), illetve **CCMC** (CCRA ügyvezető testület) munkájába. Az „**about the CC**" tartalmazza a megállapodás célját, itt található válasz a CC létrehozásának legfőbb okára: legyen egy általánosan elfogadott követelményrendszer az informatikai rendszerekkel szemben. A Common Criteria előírja, hogy hogyan kell értékelni és tesztelni az informatikai rendszereket, hogy azok biztonságáról meggyőződjünk. A **publikációk** menü alatt is megtalálhatóak a CC (aktuális és eggyel korábbi verziói: CC3.1 Release 4, CC3.1 Release 3, CC2.3) és CEM, valamint az ezeket megalapozó dokumentumok. A megalapozó dokumentumok „CcdB – dátum" azonosító alatt tartalmaz követelményeket, osztálya lehet javaslat vagy kötelező érvényű. A **műszaki bizottság** menü alatt a CCMC üléseinek összefoglalója, továbbá az úgynevezett „Átmeneti terv", található, amelyben táblázat foglalja össze a CCRA szabályainak elfogadási ütemezését egy adott tagállam esetében. A **tanúsított termékek** pont alatt hét könyvtárba rendezve (hozzáférés vezérlő eszközök és rendszerek, 78 termék, biometrikus rendszerek és eszközök, 3 termék, határvédelmi eszközök és rendszerek, 111 termék, adatvédelmi eszközök, 77 termék, adatbázisok, 45 termék, érzékelő eszközök és rendszerek, 45 termék, intelligens kártyák és kapcsolódó eszközök, valamint rendszerek, 703 termék) a minősített hardver és szoftver eszközök felsorolása áll rendelkezésünkre, a minősítés szintjével, dátumával, és a minősítő nemzet jelével. A táblázatban egyenként megnyithatók a tanúsítási

jelentések, a biztonsági célkitűzés, valamint a védelmi profil is. A **védelmi profilok** menüpont tizenkét könyvtárban, védelmi profil szerinti bontásban tartalmazza a tanúsított termékeket, szintén elérhető módon a tanúsítási jelentéssel. Az **ICCC** alatt az eddigi nemzetközi CC konferenciák időpontja és video anyaga érhető el, a **hírek** menüben pedig az aktuális hírek, események, az ügyvezető testület közleményei és hírlevelek.

## 3. Mi az a CC?

Az informatikai rendszerek fejlődése maga után vonta a biztonsággal kapcsolatos informatikai értékelési módszerek fejlődését is. Kialakult az igény a korábban nemzeti, biztonsági fogalmak, eljárások, tanúsítványok egységesítésére, közös kialakítására. Kialakulásának folyamatát az 2. ábra mutatja, a korábbi USA, kanadai, angol, német, francia fejlesztések eredményeként. Azóta létezik a 2.2, 2.3, 3.1 verzió Release 3, valamint a **jelenleg érvényes 3.1 verzió Release 4** (2012. szeptember) változata is.




*1. ábra CC kialakulási folyamata*

## 4. A Common Criteria, „Közös Követelményrendszer” (az IT biztonság értékeléséhez)

Egyre inkább nemzetközileg elismert **biztonsági szabálygyűjtemény**. Eredetileg az 1980-as években az amerikai Orange Book-ból indult, majd nemzetközi kereszt-elismerési szerződések révén egyre nagyobb tekintélyt szerzett.
A CC az az informatikai biztonsági termékszabvány, amely ma az informatikai biztonság területén etalonnak tekinthető, a világon egyre szélesebb körben elfogadott és folyamatos fejlesztés alatt áll. 1.0-ás változatát az Európai Közösség, az Amerikai Egyesült Államok és Kanada együttesen fogadták el, 2.0-ás verziója **ISO/IEC 15408** jelzettel de jure nemzetközi szabvánnyá vált. Az aktuális és a megelőző változat szabadon elérhető a http://www.commoncriteriaportal.org/ oldalról. A CC magyar érdekessége, hogy 1.0 változatát az Informatikai Tárcaközi Bizottság **16. számú ajánlásaként** magyar nyelven közreadta, majd az **MSZ ISO/IEC 15408** jelzetű szabvány is lefordításra került.
A CC hatóköre kiterjed az informatikai eszközökre, rendszerekre és termékekre. Az információbiztonságot fenyegető tényezőket megnevezi, ezek közül azokkal foglalkozik, melyeket az IT eszközöknek kell kivédeniük. Részletesen foglakozik a környezeti biztonsággal, szervezetbiztonsággal, IT hozzáférés biztonsággal, szoftverfejlesztés minőségellenőrzésével, speciális biztonsági mechanizmusok értékelésével. A CC hatókörén kívül esik, pl. az adminisztratív biztonsági intézkedések, környezeti biztonság értékelése, a kriptográfiai algoritmusok és azok belső jellemzőinek értékelésére vonatkozó kritériumok. Ennek ellenére például a CC előírja, hogy az értékeléshez a kriptográfiai algoritmusokkal is kell foglalkozni.
A Common Criteria alkalmazása előtt definiálni kell, hogy milyen szoftvert vagy informatikai rendszert kívánunk tesztelni. Ezt nevezzük az értékelés tárgyának. Meghatározzuk azokat a felhasználói követelményeket, más néven biztonsági funkciókat, amiket az értékelés tárgyának tudnia kell. Ezeket védelmi profilokba gyűjtjük. Ezek alapján készül a biztonsági rendszerterv. A Common Criteria azt írja le, hogy hogyan kell a biztonsági rendszertervben leírt biztonsági funkciókat tesztelni. **Ehhez 7 úgynevezett értékelési garancia szintet** határoz meg. Minden szint leírja, hogy milyen garanciális biztonsági követelményeket kell teljesíteni az értékelés tárgyának, hogy az adott szintnek megfeleljen. Minél magasabb értékelési garancia szintet ér el egy szoftver, annál biztonságosabbnak gondoljuk, habár a magasabb szint csak azt jelenti, hogy többféle szempontból és nagyobb szigorral tesztelték a biztonsági rendszertervben leírt funkciókat.
**ÉT** – Értékelés Tárgya (TOE – Target of Evaluation): Az a szoftver vagy informatikai rendszer, amely biztonságát vizsgáljuk a Common Criteria segítségével. Fontos

megjegyezni, hogy a Common Criteria nem foglalkozik az ÉT környezetével, pl. az épület biztonsággal.

**VP** – Védelmi Profil (PP – Protection Profile): A VP egy dokumentum, amelyet általában felhasználói csoportok alakítanak ki a **saját elvárásaiknak megfelelően** egy informatikai rendszerrel kapcsolatban. Létezik VP például a tűzfal vagy az intelligens kártya termékekhez. A VP biztonsági követelmények gyűjteménye. Egy szoftvercég dönthet úgy, hogy a termékét egy VP-nek megfelelően fejleszti ki és az ott meghatározott követelményeket implementálja. A VP-k alapján írhatják a szoftvercég szakemberei a biztonsági rendszertervet (lásd lent), de ez nem kötelező, figyelmen kívül is hagyhatják azokat.

**BRT** – Biztonsági Rendszerterv (ST – Security Target): A BRT egy vagy több, esetleg nulla VP alapján jön létre. Az ott megfogalmazott biztonsági követelmények alapján sorolja fel azokat a biztonsági funkcionális követelményeket (lásd lent), amiket tesztelni fogunk. Fontos kiemelni, hogy az ÉT-t csak ezek ellen teszteljük. A Common Criteria rugalmasságát az adja, hogy nem ad semmilyen előírást a BRT tartalmára, így két teljesen különböző IT terméknek (pl. egy tűzfal és egy online bolt) két teljesen eltérő BRT-je lehet. Sőt két ugyanolyan típusú IT terméknek is lehet két teljesen különböző BRT-je. A BRT általában nyilvános, így a vevők tudják, milyen biztonsági funkciói vannak az ÉT-nek.

**BFK**-ek – Biztonsági Funkcionális Követelmények (SFRs – Security Functional Requirements): A BFK-ek általánosan megfogalmazott biztonságra vonatkozó funkcionális követelmények. Például lehessen a felhasználót beléptetni. A Common Criteria sok BFK-t sorol fel. Ezek közül semmit sem tesz kötelezővé, de a köztük fennálló összefüggésekre rávilágít. Például a felhasználó beléptetéséhez jelszót kell kérni, a jelszavakat kódolva kell eltárolni.

**GBK-ek** – Garanciális Biztonsági Követelmények (SARs – Security Assurance Requirements): A GBK-ek olyan követelmények, amelyeket a fejlesztés során vagy a tesztelés során kell kielégíteni annak érdekében, hogy a vállalt biztonsági funkciókat tudja teljesíteni az ÉT. Ezeknek a követelményeknek számszerűen mérhetőnek kell lenniük. GBK lehet például, hogy a forráskódot verziókövető rendszerben kell tárolni. A szabvány felsorol sok GBK-t, sőt azokat csoportokba szervezi.

**ÉGSz – Értékelési Garancia Szint (EAL – Evaluation Assurance Level)**: A Common Criteria alkalmazásának eredményeként az ÉT egy ÉGSz-t kap 1-től 7-ig. Minden ÉGSz egy GBK csomag, amely az ÉT teljes fejlesztését lefedi különböző szigorúsággal. **A legmegengedőbb az 1-es szint, a legszigorúbb a 7-es**. Minden szint eléréséhez teljesíteni kell az előzőeket is. Ugyanakkor a magasabb ÉGSz szint nem feltétlenül jelenti, hogy egy termék biztonságosabb. Csak annyit, hogy a BRT-ben leírt

biztonsági funkciók szigorúbban lettek tesztelve. Ha az ÉGSz mellett látható egy pluszjel is, akkor az azt jelenti, hogy teljesítette az adott ÉGSz elvárásait és a magasabb szintekről is néhány GBK-t. Így van például ÉGSz4+ szint is, ilyet kapott a Windows XP operációs rendszer, ami azt jelenti, hogy teljesítette az ÉGSz4 elvárásait és a magasabb szintekről is néhány GBK-t.
Tehát a Garancia Szint (EAL) azt fejezi ki, hogy az értékelés tárgyának (ÉT) vizsgálatát milyen mélységben, milyen erőforrás ráfordítással végezték. Nem minden feladat, védelmi igény kíván meg nagy vizsgálati ráfordításokat, hiszen a magasabb garanciaszinteken nagyon nagy költségű vizsgálatok jelenhetnek meg.

A növekvő értékelési erőfeszítés az alábbi területeken nyilvánul meg:

- hatókör, azaz további erőfeszítéseket teszünk, hogy a termék vagy rendszer tartalmának nagyobb részét értékeljük
- mélység, azaz járulékos erőket vonultatunk fel, hogy nagyobb tervezési és megvalósítási részletezettséggel értékeljünk
- szigorúság, azaz járulékos erőfeszítést használunk, ha több kutatási eszközt és technikát alkalmazunk, hogy a kevésbé nyilvánvaló hiányosságokat, „rejtett hibákat” is felderítsük, vagy csökkentsük ezek megmaradásának valószínűségét

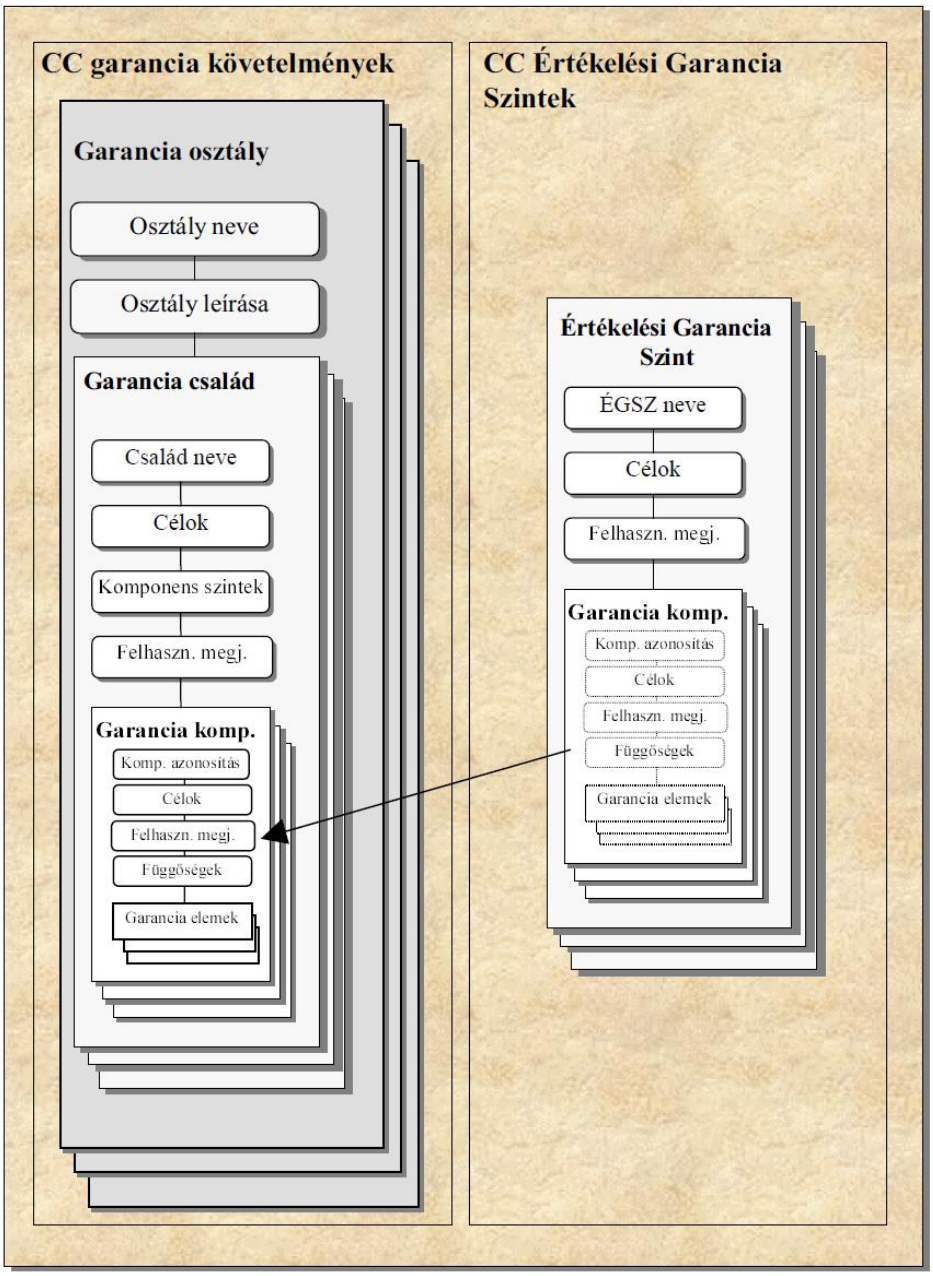
Minél magasabb ÉGSz-t szeretne elérni egy szoftverfejlesztő cég, annál több és részletesebb dokumentációt kell elkészítenie a szigorú tesztek alapján, ami egyre drágább. Ugyanakkor a cégeket motiválja, hogy a magas ÉGSz magas vásárlói bizalmat is jelent. Általában állami / katonasági megrendelések feltétele a Common Criteria alkalmazása. Általában az ÉGSz4 szint felett már nem éri meg a befektetés, kivéve néhány nagyon érzékeny alkalmazási területet, pl. atomerőművek, ahol elvárt a magasabb ÉGSz szint.

Az ÉGSz szintek a következők:

- ÉGSz1: Funkcionálisan tesztelt (EAL1: Functionally Tested)
- ÉGSz2: Strukturálisan tesztelt (EAL2: Structurally Tested)
- ÉGSz3: Módszeresen tesztelt és ellenőrzött (EAL3: Methodically Tested and Checked)
- ÉGSz4: Módszeresen tervezett, tesztelt és áttekintett (EAL4: Methodically Designed, Tested, and Reviewed)
- ÉGSz5: Félformálisan tervezett és tesztelt (EAL5: Semiformally Designed and Tested)

- ÉGSz6: Félformálisan igazolt terv és tesztelt (EAL6: Semiformally Verified Design and Tested)
- ÉGSz7: Formálisan igazolt terv és tesztelt (EAL7: Formally Verified Design and Tested)

A CC II. rész, III. Garancia követelmények 3.1, 3.2 fejezetei tartalmazzák az egyes garanciaosztályokban, az egyes garanciaszintekhez tartozó elvárásokat, a 3.3 fejezet a Garanciaszinteket. Fentiek egymáshoz viszonyított helyét szemlélteti a 3. ábra. A 4. ábra foglalja össze, hogy az egyes, rövidített névvel feltüntetett garancia családok a különböző (1-től 7-ig terjedő) garanciaszinten milyen garancia komponenssel rendelkeznek, ahol rendelkeznek. Az osztályon belüli család rövidítések értelemszerűen definiálva lettek, továbbá a következő fejezetben mind a hét garanciaszinten belül a 3. ábra táblázatának megfelelő garanciakomponens megnevezésre kerül. Például az ötös garanciaszinten (ÉGSZ-5) az **életciklus támogatás** család, ALC_DVS.1 „A biztonsági intézkedések meghatározása”, ALC_LCD.2 „Szabványosított életciklus modell”, valamint az ALC_TAT.2 jelű, „Megvalósítási szabványok teljesítése” garanciakomponensek szerepelnek. Az ÉGSZ növelésének - a 4. ábra táblázatában jobbra haladva - metodikája, hogy az adott garanciakomponenst **hierarchikusan magasabb garanciakomponensre** cseréljük, vagyis növeljük a szigorúságát, kiterjedését, mélységét, **vagy plusz garanciakomponenst** adunk hozzá, ezesetben új követelmény hozzáadásával érünk el eredményt. A III-4 fejezet részletezi a garanciaosztályok, családok, komponensek lineárisan hierarchikus felsorolását, mélységi szinten növekvő számozással ellátva. A III-5 fejezet az ÉGSZ 1-2-3-4 szintjeire definiálja részletesen az egyes garanciakomponenseket. A négyes garanciaszint felett nincs hazai informatikai fejlesztés, sem tapasztalat, a Hunguard fordítása sem tartalmazza. Ezen garanciatartomány (ÉGSZ 5-6-7) jelentőségének növekedése várható a közeljövőben, kritikus infrastruktúrák, veszélyes létesítmények informatikai rendszereinek esetében, így a terület kutatása nem elhanyagolható.




*2. ábra Garancia és Garancia Szintek összefüggése*

| Garancia Osztály | Garancia Család | Garanciakomponensek az Értékelési Garancia Szint szerint | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | ÉGSZ 1 | ÉGSZ 2 | ÉGSZ 3 | ÉGSZ 4 | ÉGSZ 5 | ÉGSZ 6 | ÉGSZ 7 |
| Konfiguráció-kezelés | ACM_AUT | | | | **1** | 1 | **2** | 2 |
| | ACM_CAP | **1** | 1 | **2** | **3** | 3 | **4** | 4 |
| | ACM_SCP | | | **1** | **2** | **3** | 3 | 3 |
| Szállítás és működtetés | ADO_DEL | | | | | | | |
| | ADO_IGS | | **1** | 1 | 1 | 1 | 1 | 1 |
| Fejlesztés | ADV_FSP | **1** | 1 | 1 | **2** | **4** | **5** | **6** |
| | ADV_HLD | | **1** | **2** | 2 | **3** | **4** | **5** |
| | ADV_IMP | | | | **1** | **2** | **3** | 3 |
| | ADV_INT | | | | | **1** | **2** | **3** |
| | ADV_LLD | | | | **1** | 1 | **2** | 2 |
| | ADV_RCR | **1** | 1 | 1 | 1 | **2** | 2 | **3** |
| Útmutató dokumentumok | AGD_ADM | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Életciklus támogatás | ALC_DVS | | | **1** | 1 | 1 | **2** | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | **1** | **2** | 2 | **3** |
| | ALC_TAT | | | | **1** | **2** | **3** | 3 |
| Tesztek | ATE_COV | | **1** | **2** | 2 | 2 | **3** | 3 |
| | ATE_DPT | | **1** | **2** | 2 | **3** | 3 | **4** |
| | ATE_FUN | | **1** | 1 | 1 | 1 | 1 | 1 |
| | ATE_IND | **1** | 1 | **2** | 2 | 2 | 2 | **3** |
| Sebezhetőség felmérése | AVA_CCA | | | | | **1** | **2** | 2 |
| | AVA_MSU | | | **1** | **2** | 2 | 2 | 2 |
| | AVA_SOF | | **1** | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | **1** | 1 | **2** | **3** | **4** | 4 |

*3. ábra Garanciaszintekhez tartozó garanciakomponensek*

**Rövidítések, magyarázatok:**

MSZT: Magyar Szabványügyi Testület

ISO International Organization for Standardization (Nemzetközi Szabványügyi Szervezet) Nyelvtől, kultúrától, jogi környezettől független minőséget garantáló rendszer**.**

IEC International Electrotechnical Commission (Nemzetközi Elektrotechnikai Bizottság) AZ elektrotechnika rohamos fejlődése keltette életre, 1906 - ban, 13 ország részvételével. Köztük volt Magyarország is. A szervezet szabványosító (műszaki) bizottságait kezdetben AC - nek (Advisory Committe), Tanácsadó Bizottságnak nevezték.

CEN (European Committee for Standardization) Európai Szabványügyi Bizottság

CENELEC Európai Elektrotechnikai Szabványügyi Bizottság

**A 27000 család elemeinek jegyzéke:**

ISO 27000:2009 – Információ technológia, Biztonsági technikák, ISMS – áttekintés és magyarázatok

ISO 27001:2005 - MSZ ISO/IEC 27001:2006 – Információbiztonsági Irányítási Rendszerek követelmények

ISO 27002:2005 – Gyakorlati kézikönyv az ISMS rendszerek kialakításához

ISO 27003:2010 – Bevezetési útmutató

ISO 27004:2009 – Szabvány az információbiztonság számszerűsítéséről és mérési lehetőségeiről

ISO 27005:2011 – Információ biztonsággal kapcsolatos kockázatok kezelése

ISO 27006:2011 – Tanúsító és auditáló szervezetek számára előírt követelmények

ISO 27007:2011– Útmutató ISMS rendszerek auditálásához

ISO 27008:2011– Útmutató ISMS auditoroknak az információbiztonsági ellenőrzésekről

ISO 27009 – Nincs kiosztva

ISO 27010 – Ágazatok és szervezetek közötti kommunikáció szabályozása információbiztonsági szempontból

ISO 27011:2008 – A telekommunikáció információbiztonsága

ISO 27012 – Nincs kiosztva

ISO 27013 – Útmutató az ISO/IEC 27001és ISO/IEC 20000-1 szabványok integrált bevezetéséhez

ISO 27014 – Az információbiztonság irányítása

ISO 27015 – Javaslat a pénzügyi szervezetek és biztosítók információbiztonsági rendszereiről
ISO 27016 – Információbiztonság irányítása: szervezeti gazdaságtan1
ISO 27017-1 – Nincs kiosztva
ISO 27017-2 – Útmutató az információbiztonsági kontrollok használatára felhő alapú szolgáltatásoknál
ISO 27018 – 27030 – Nincs kiosztva
ISO 27031:2011 – Biztonsági technikák: útmutató az információs és kommunikációs technikák felkészültségéről az üzletfolytonosság megközelítésében
ISO 27032 – Biztonsági technikák: útmutató a kibervédelemhez
ISO 27033-1:2009 – Hálózati biztonság: áttekintés és fogalmak
ISO 27033-2.2 – Hálózati biztonság: hálózati felépítések referencia: fenyegetések, tervezési elvek és ellenőrzések
ISO 27033-3 – Nincs kiosztva
ISO 27033-4 – Hálózati biztonság: gatewayekkel összekötött hálózatok közötti biztonságos kommunikáció
ISO 27033-5 – Hálózati biztonság: VPN - nel összekötött hálózatok közötti biztonságos kommunikáció
ISO 27033-6 – Hálózati biztonság: biztonságos IP vezeték nélküli hálózat kialakítása
ISO 27033-6 – Hálózati biztonság: vezeték nélküli rendszerek
ISO 27034-1:2011 – Alkalmazás biztonság: áttekintés és alapfogalmak
ISO 27034-2 – Alkalmazásbiztonság: szervezeti normatív keretrendszer
ISO 27034-3 – Alkalmazásbiztonság: alkalmazásbiztonsági irányítási folyamatok
ISO 27034-4 – Alkalmazásbiztonság: alkalmazások biztonságának érvényesítése
ISO 27034-5 – Alkalmazásbiztonság: protokollok és alkalmazásbiztonsági adatstruktúra
ISO 27035:2011 – Információbiztonsági incidenskezelés
ISO 27036-1 – Információbiztonság szállítói kapcsolatokban: áttekintés és alapfogalmak
ISO 27036-2 – Információbiztonság szállítói kapcsolatokban: általános követelmények
ISO 27036-3 – Információbiztonság szállítói kapcsolatokban: útmutató ICT (information and communications technology) szállító láncok biztonságához
ISO 27037 – Útmutató az elektronikus bizonyítékok azonosításához, összegyűjtéséhez, megszerzéséhez és tárolásához
ISO 27038 – Specifikáció a digitális szerkesztéshez
ISO 27039 – Behatolás jelző rendszer kiválasztása, bevezetése és működtetése
ISO 27040 – Biztonsági technikák: háttértárak biztonsága

ISO 27041 – Útmutató a nyomozási eljárások megfelelő lefolytatásához
ISO 27042 – Útmutató az elektronikus bizonyítékok analizálásához és bemutatásához

**ISO/IEC informatikai bizottságai:**

| | |
|---|---|
| ISO/IEC JTC 1 | ISO/IEC közös informatikai bizottság |
| ISO/IEC JTC 1/SC 2 | Kódkészletek |
| ISO/IEC JTC 1/SC 6 | Rendszerek közötti távközlés és információcsere |
| ISO/IEC JTC 1/SC 7 | Szoftverek |
| ISO/IEC JTC 1/SC 22 | Programnyelvek, környezetük és rendszerszoftver-interfészeik |
| ISO/IEC JTC 1/SC 23 | Optikai lemezek információcseréhez |
| ISO/IEC JTC 1/SC 24 | Számítógépi grafika |
| ISO/IEC JTC 1/SC 25 | Információtechnikai készülékek összekapcsolása |
| ISO/IEC JTC 1/SC 27 | IT-biztonsági technikák |
| ISO/IEC JTC 1/SC 28 | Irodagépek |
| ISO/IEC JTC 1/SC 29 | Hang,- kép-, multimédia és hipermédia-információ kódolása |
| ISO/IEC JTC 1/SC 31 | Önműködő azonosító és adatfogadási technikák |
| ISO/IEC JTC 1/SC 32 | Adatkezelés |
| ISO/IEC JTC 1/SC 34 | Leíró- és kezelőnyelvek |
| ISO/IEC JTC 1/SC 35 | Felhasználói interfészek |
| ISO/IEC JTC 1/SC 36 | Informatika. Tanulás, oktatás és tréning |
| ISO/IEC JTC 1/SC 37 | Biometria |
| ISO/IEC JTC 1/SC 38 | Elosztott alkalmazás; platformok és szolgáltatások |
| ISO/IEC JTC 1/SC 39 | Fenntarthatóság és informatika |

**Összegzés**

Jelen cikkünk átfogó képet adott a szabványokról.

**Felhasznált irodalom**

[1] http://www.commoncriteriaportal.org
[2] http://wiki.hup.hu/index.php/Common_Criteria
[3] www.ekk.gov.hu/hu/kib/archivum/itb
[4] Szádeczky Tamás „Szabályozott biztonság” PhD értekezés
[5] http://hadmernok.hu/archivum/2007/1/2007_1_kerner.html

[6] Dr. Kusper Gábor és Dr. Radványi Tibor /Eszterházy Károly Főiskola Matematikai és Informatikai Intézet/ Jegyzet a projekt labor című tárgyhoz
[7] Dr. Rajnai Zoltán, Bleier Attila: Technical problems in the IP communication systems of the Hungarian Army, ACADEMIC AND APPLIED RESEARCH IN MILITARY SCIENCE 9: (1) pp. 15-23., ZMNE, Budapest, 2013
[8] http://www.itb.hu/ajanlasok/a16/
[9] http://www.hunguard.hu
[10] http://mmfk.nyf.hu/min/alap/15.htm
[11] Krasznai Csaba: Szabványok, ajánlások, modellek

***Éva Fábián[23]: The downfall of the Fourth Republic of France***

**Abstract**
*The North African territory came again to the front of the world's attention because of the „jasmine revolution" in Tunisia at the end of the year 2010 and also because of the proceeding and nowadays events in the region. Due to the constant problem of the ever-grownig number of North African immigrants living in the European territory, these events belong to the sphere of interests of the European Union as well as of Hungary. In my opinion, the great variety of diplomatic and business cooperation between the EU (and Hungary) and the North-African states as well as NATO's Mediterranean Dialogue, initiated by the North Atlantic Council in 1994, justify the need to analyze the history of the North African region. These recent events known as „the Arabian spring" provided us with reference to all economic and social problems of these nations, and also pointed out the weaknesses and the defects of their political systems. All these occurences and the current situation in the Arabian countries present not only security risks but also problems to resolve in terms of politics as well as economics, finance, social and religious matters.*

## 1. Introduction

In the aftermath of WWI, the de-colonialist ambitions first appeared only in the cities and within narrow bounds in the North African territory. The process accelerated only after the Second World War II, and the countries of the African continent, which had so far been under foreign political and military control, became – with or without revolution, and often with a lot of casualties – an independent and active part of the international community. Of all the so-called Maghreb[24] countries, Algeria – which had for long been considered an integral part of France – won its independence on 3 July, 1962. France – with its long colonialist history – found it hard to part with its North African territories, especially with Algeria, since the number of French people living here – compared with other French territories in this region – used to be much higher, and also because the French saw great economical potential in Algeria – after the opening of the oilfields in the Sahara, hoping to recover its lost prestige in international politics.

[23] A Nemezeti Közszolgálati Egyetem Ph.D hallgatója.
[24] This expression means 'west' (where the Sun sets), and signifies Arabian countries west of the valley of the Nile, spreading to the Atlantic Ocean. Morocco, Algeria and Tunisia are unambiguously Maghreb countries. They are referred to as *Maghreb* in French literature.

The more or less aggressive suppressing of activities to win independence in the North African region, which were receiving more and more international subventions, as well as the general behaviour of France – *concerning decolonization* – left its mark not only on the liberated territories, but also on the European and French political life and on the subsequent French-African relationships.

## 2. Between the two world wars

The de-colonialist movements were rather unorganized between the two world wars. However, many of their representatives were later to play a great part in establishing the most elaborated form of the nationalist program as well as in creating the independent Algeria.
For instance, the Association of Representatives was founded by representatives of the Algerian political life in 1927, the leader of which was Ferhat Abbas. This organization represented assimilationist tendencies, whose members imagined "the future Algeria" as a territory of France. The role of the communists in this period was not negligible either, both in terms of ideology and the creation of the organizational framework of the independent groupings. The North-African Star[25] [ENA] was established with their active help in Paris in 1926, which played a significant role in the Algerian nationalist movement with its membership of about 300,000 immigrant workers living in France. Its leader was Messali Hadj, who was regarded as "the father of the Algerian nationalism". With the changing of the communists' point of view the ENA came more and more into conflict with the party.
The Association of Muslim Algerian Ulema was founded by Abdelhamid Ben Badis in 1931. It first became popular among the supporters of the national independence movements, and was established with the aim of helping the intellectual, economical and social education of the Algerian Muslims. Despite their former popularity, after WWII this association was not politically significant any more. The confrontation between Ben Badis's and Ferhat Abbas's principles took place in 1936 with a historic moment: Ben Badis was the first to declare the independence of the Algerian nation.
Among other political organizations of the Algerian independence movement, the Algerian Communist Party[26], established in 1936, also played an increasingly

[25] Étoile Nord-Africaine – ENA
[26] Partie Communiste Algérienne – PCA

important political role after the '40s, with its increasing membership. Politically speaking, this party had a lot in common with the Democratic Union of the Algerian Manifesto[27]; nevertheless, these political organizations drifted away from each other because of the radical changes in the Communist Party after the end of the '40s.

## 3. Algeria during World War II

The racist laws issued by the Vichy-government, the French resistance as well as France's entire attitude to its colonies in general were altogether more than disappointing for the colonials during WWII. It directly resulted - *among others* - in the change of Ferhat Abbas' policy. It was made clear in his work[28] known as Manifesto that the nationalist movement aimed to liberate the nation and achieve sovereignty. Published at the beginning of 1943, it was specified even further by his followers that May. Catroux, governor of the time – *on behalf of the French settlers* – did not fail to respond, and arrested Abbas. Following his release, the Algerian politician established a party called Friends of the Manifesto and Liberty[29], based on the doctrines of the Manifesto, and gained in popularity ever increasingly.
Tensions between the Algerian masses – *fuelled with radical claims* – and the French settlers were increasing before the end of WWII. The goal of Messali Hadj and his party called the Movement for the Triumph of the Democratic Liberties[30] was full independence, which became rather popular among the natives. In the light of these precedents, the outbreak of the Algerian uprising on 8 May 1945 came by no means as a surprise. It started out with a Muslim nationalist demonstration in Setif claiming the release of Messali Hadj[31], and celebrated the defeat of fascism as well as the end of colonialism. The clash between the Algerian insurgents and the French police led to bloody and armed combats, which slowly infected other cities in Algeria. This revolt was suppressed by about 10,000 soldiers of the French land army, also involving the French air force and navy, and demanded ten thousand casualties of Algerian Muslims; in addition, it meant a

[27] Union Démocratique du Manifeste Algérien – UDMA
[28] *„Algeria before the global conflict, the manifesto of the Algerian people"*
[29] Amis du Manifeste et de la Liberté – AML
[30] Mouvement pour le Triomphe des Libertés Démocratiques – MTLD; Its illegal para-militarist unit was the Special Organization (Organisation Spéciale – OS). It was founded by the most radical core of the party in spite of the protest of Messali Hadj. Their aim was to prepare armed revolt. Its members were continuously pursued by the French.
[31] He was in prison in Brazzaville that time.

turning-point in the history of the Algerian nationalist movement: the natives began to realize that the overseas policy of the French state had not changed the slightest.

## 4. The aftermath of WWII

This insurrection was a great success. It showed that the decolonization was in progress and the colonies could not possibly be governed according to the old methods anymore. However, it took some time the French settlers to understand and accept the inevitability of their colonial territories' becoming independent. This behaviour foreshadowed the downfall of the French Fourth Republic.
Nevertheless, the reasons for France's behaviour also have a lot to do with it. Due to a resolution of the French Parliament on 20 September 1947, Algeria remained an integral part of France, obtaining the status of an overseas counties - *as opposed to the two neighbouring countries, Tunisia and Morocco* -, which meant a stronger attachment to the motherland than a protectorate[32]. Also, the number of French[33] living in Algeria was much higher than in other Maghreb countries; in addition, Algeria – *owing to the long common history* – constituted an integral part of French economy. Besides, the gas and oil fields – *discovered in the Sahara during the '50s* – greatly increased France's ambition as well as their strong adherence to the land. With the ever-increasing role of raw materials after WWII, to own and exploit them at their own disposal meant for France the chance of economical and political independence as well as recovering their lost prestige in international politics.

## 5. The Algerian war of independence

The main driving force of the Algerian nationalist movement after WWII was the alliance between the modern political movements in the cities and the potential of the fellah masses in the villages. France's defeat in Indochina – *which served as a good example for the colonialism to be overthrown* – gave stimulus to the Algerian movement. The leaders of the nationalist movement had a meeting during the night of 22 October, 1954, and founded the National Liberation Front[34] and the National Liberation Army[35] there and then. The most significant

[32] Morocco and Tunisia became protectorates.
[33] It meant approximately one million Europeans living in Algeria in the mid-fifties, the majority of whom were French. On the other hand, approximately 600,000 European settlers lived in Tunisia and in Morocco. (LENGYEL, 2006, p. 65.)
[34] Front de Libération Nationale – FLN

characters of the Algerian nationalist movement, namely Hocine Aït Ahmed, Mohamed Boudiaf, Ahmed Ben Bella, Mourad Didouche, Rabah Bitat, Larbi ben M'Hidi, Krim Belkacem and Mohamed Khider fixed 1 November 1954 to be the starting date of the revolt. Having no particular action-plan, they only wished to achieve the independence of Algeria with the growing help of the native Algerians.

The French authorities considered this armed uprising initially as a question of internal security until the turning-point, i.e. events occurring on 20 August 1955, when the rebels launched attacks in regular units against 27 settlements, which lasted for several days. Algeria was split in two and the skirmishes – *which gradually spread to almost every part of the country* – demanded more and more casualties on both sides, and the rebels – *called guerrillas* – received more and more political, moral and material aid from the neighbouring countries as well as from the states of the Arabian League, with political parties, organizations and their leaders joining the revolt continuously. The revolt soon became internationally recognized. At the same time, the French army's regular and cruel retaliation and especially the increasing number of French soldiers in Algeria evoked antipathy and protestation in the French society against the war. The French peace-movement due to the rejection of the war against Algeria generated a significant crisis in the internal political life of France.
The aggression and the various strategic methods of the French colonists were not effective enough to isolate and dissolve the rebels. The power of the National Liberation Front was growing at a great extent: its members managed to organize their first – *obviously illegal* – congress in Kabylie on 20 August 1956, establishing their main organizational units, i.e. the National Council of the Algerian Revolution[36] and the Coordinating and Executing Committee[37].
At the same time, in January 1956 the Guy Mollet government, receiving the most votes with its peace program in the French parliamentary elections, first negotiated with the members of the National Liberation Front, yet they changed their opinion in a short time and began to assist the extremist policies of the right-wing, and further increased the number of the French soldiers stationed in Algeria. In addition, the aircraft which transported the leaders of the National Liberation Front – among others, Ahmed Ben Bella, Hocine Aït Ahmed, Mohamed Khider and

[35] Armée de Libération Nationale – ALN
[36] i.e. Parliament
[37] i.e. government

Mohamed Boudiaf –, was hijacked by the French on 22 October 1956, and the leaders were arrested, violating the international law.

## 6. The return of Charles de Gaulle to the French political life: the resolution

The Algerian war already regularly appeared on the agendas of the UN[38]'s General Assembly, with the actors of the international political life claiming for resolution, but there were no changes. This situation became unmanageable and beyond control for the French government. On top of that, a group of French officers of the extreme right-wing executed a coup d'état on 13 May 1958, seizing power in Algeria and even threatening Paris. France, which was clearly drifting towards a civil war, called back General Charles de Gaulle – investing him with full powers as the single person who could solve this problem. As a result, it became obvious that the unstable Fourth Republic of France lost the colonialist war against the country where it was actually established in 1944.

The return of de Gaulle was by no means an immediate success: his so-called Constantine Plan[39] – *which was proclaimed on 3 October 1958* – did not fulfil French hopes. De Gaulle declared the right of the Algerian people to self-determination on 16 September 1959, and the first provisional government was formed with the leadership of Ferhat Abbas. After all, the Algerian independence movement – *which had learned a lot from its own mistakes as well as consumed all its availability to press France to accept the Algerians' right to self-determination* – won and gradually achieved the appreciation and the support of the international public. The Algerian nation's right for self-determination as well as for independence was acknowledged on the session of the UN's General Assembly on 20 December 1960.

The negotiations between French and Algerian delegates were accompanied by political mass demonstrations in the period of 1961-1962, which were numerously interrupted by bombings of the ultra's secret army[40] and also by the military revolts of the generals who supported them. Finally, the agreements on ceasefire and on the relations between France and Algeria, based on mutual compromises, were signed in Evian on 18 March 1962. Nevertheless, they ensured France significant economical, military and cultural influence in Algeria.

[38] United Nations
[39] It contained both economic and social reforms.
[40] Organization of Secret Army; Organisation Armée Secrète – OAS

There were referendums concerning the independence of Algeria in both countries, which was finally declared on 5 July 1962[41]. 80-90 percentage of the death toll was Algerian casualties, and the infrastructure also suffered greatly from the enormous damage of the war, which also caused the European settlers to leave the North African country in large numbers, mainly due to the activities of the Organization of Secret Army, thus leaving Algeria with no professionals. Moreover, industrial plants were severely damaged, and the former agricultural structure was in ruins, since the farmers already moved to the cities. After his release in 1962, Ahmed Ben Bella, who became Algeria's first prime minister and later the first president of the independent Algerian republic from 1963, had ahead of him a great number of problems to solve.

**Summary**

France's behaviour as regards the process of decolonization after WWII put France, which then had a lot of internal and international problems anyway, in an even more awkward and disadvantageous position. Apart from not being able to understand the unavoidability and the necessity of what was going on the French political elite also underestimated the experiences of their colonized nations, obtained during the conflicts in WWI, and especially in WWII. The reasons for their forceful adherence made their behaviour understandable, and from many points of view the process of decolonization in the French colonies was not completely loaded with violence. The case of Algeria was clearly an exception, which also created an internal crisis for France. It meant both economical and financial crises as well as labour shortage, inflation and problems in the foreign trade, not to mention the moral and political problems.
In this situation there was only one man who could bring solution for the restoration of the paralyzed French political life: Charles de Gaulle, who retired from politics in 1946. He still meant to the French people the person who could worthily represent the historical greatness and the national interests of the Gallic state. As he wrote in his work, titled *Memoirs of Hope: Renewal, 1958-1962*: 'In fact, however depressing it seemed to us, we understood that the maintenance of our domination over the peoples who do not accept us is such a risk, with the taking of which we win nothing but we lose everything."[42]

[41] 132 years after the landing of the French expeditionary forces.
[42] DE GAULLE, 2003, p. 34.

The Arabian states are located in the territory spreading from the Atlantic Ocean to the Persian Gulf, i.e. basically the south-western part of Asia and North-Africa. Although this region is full of contradictions, it, however, plays an important role in world-history as well as in the international affairs, and has raised numerous viewpoints and prejudices. Beside the traditional images of the desert and the camel caravans as well as today's oilrigs, tragic events can also be associated with the region, such as war-conflicts and terrorist activities. The boundaries of the Maghreb states, in other words the „Island of the West" are „…washed by sea-water from the north and from the east and by the sea of sand from the south"[43], as István Lengyel put it. However, they will not blur our knowledge of history embedded in the pages of books and in the people's mind, and keep influencing the life of the nations living in this region as well as our present time.

**References**

CHARLES DE GAULLE (2003): *A reménység emlékiratai. 1. kötet. Az újjászületés 1958-1962.* Gradus ad Parnassum Könyvkiadó, Szeged, ISBN 963 9184 14 4

ENDRE SÍK (1964): *Fekete-Afrika története II.* Akadémiai Kiadó, Budapest

GÁBOR BÚR (2011): *Afrika-történeti tanulmányok.* Mundus Novus Kft., ISBN 978 963 9713 32 1

HENRI ALLEG (1958): *Vallatás.* Kossuth Kiadó

ISTVÁN LENGYEL (2006): *Országok az Atlasz vonzásában (A Maghreb Arab Unió esélyei).* Kairosz Kiadó, ISBN 963 7510 53 2

JÓZSEF BENKE: *Az arab országok története, II. Kötet.* Alexandra Kiadó, ISBN 963 367 281 3

JULIEN PAPP: *A francia ellenállás és a szövetséges hatalmak (1940-1944).* Internet: http://tortenelemszak.elte.hu/data/25746/PappJulien.pdf (27 April 2012)

LÁSZLÓ J. NAGY (1997): *Az arab országok története a XIX-XX. században.* Eötvös József Könyvkiadó, Budapest, ISBN 963 9024 16 3

LÁSZLÓ J. NAGY (2009): *Az ummától a nemzetállamig (Az arab országok a 19-20. században).* SZTE Juhász Gyula Felsőoktatási Kiadó, Szeged, ISBN 978 963 7356 99 5

LÁSZLÓ J. NAGY, PÉTER ÁKOS FERWAGNER (2004): *Az arab országok története 1913-2003.* JATEPress Kiadó, Szeged

CHARLES DE GAULLE (2003): *Memoirs of Hope. Volume I: Renewal. 1958-1962.* Gradus ad Parnassum Kiadó, Szeged, ISBN 963 9184 14 4

[43] LENGYEL, 2006, p. 13.

ENDRE SÍK (1964): *The History of Black Africa, Volume II.* Akadémiai Kiadó, Budapest
ENDRE SÍK (1972): *The History of Black Africa, Volume III.* Akadémiai Kiadó, Budapest
ENDRE SÍK (1973): *The History of Black Africa, Volume IV.* Akadémiai Kiadó, Budapest
FERENC GAZDAG (2011): *The History of France between 1918 and 1995.* Kossuth Kiadó, ISBN 978 963 09 6498 2
FREGAN BEATRIX: Un personnage éminent de l'histoire de la défense hongroise, HÍRVILLÁM - SIGNAL BADGE 200: (1) pp. 302-305., ZMNE, Budapest, 2010
GÁBOR BÚR (2011): *Studies on African History.* Mundus Novus Kft., ISBN 978 963 9713 32 1
HENRI ALLEG (1958): *Interrogation.* Kossuth Kiadó
ISTVÁN LENGYEL (2006): *Counties in the Allurement of Atlas (The Outlooks of a Maghreb Arab Union).* Kairosz Kiadó, ISBN 963 7510 53 2

***Zoltan Rajnai - Attila Bleier: Planification of a transmission network***

**Abstract**
*This paper describes in detail a traffic optimization in a live network. The paper suggests a methodology for the project management of an optimization project and contains results from a real network. In the optimization we used simplifications which allowed us to solve a simplified Linear Programming (LP) problem instead of an Non-Linear Programming (NLP). In this given situation we could use this optimization methodology and in practice it is often suggested to use these simplifications. Using these methods could bring benefits in the network of the Hungarian Armed Forces.*

## 1. Introduction

U.S. Defense Agency, D.A.R.P.A. has recently issued a tender called CORONET, for it's next generation core network environment. The RFQ contains strict requirements for the transmissionation network, and will pave the way for the new technologies to be deployed in ten years timeframe in the U.S, and perhaps 12–15 years in Europe. The requirements are strict in terms of bandwidth, reliability, scalability and network quality of service providing capabilities. Building up such a network with today's technology would be extremely challenging, and is far and away from real world scenario, where technology, resources, and several other constraints limit the possibilities. Two well defined paths lead to such an advanced network:

1. good definition of backbone network requirements, and forward-looking architecture design,
2. leveraging present resources as long as it can be done.

The following paper will describe the second option how to leverage and design, based on a scientific basis, and will show the findings of a real-life optical transmission network audit and redesign project. The paper discusses a transmission network optimization project. The paper is organized in a way that it starts with a general overview, then goes into more details, and finally shows one practical example.

## 2. Phases of a network optiization project

A network optimization is a general term. The process itself can have a number of different meaning depending on the network environment, and the goal of project. Without going into details (because [1] is entirely dedicated to optimization of networks), a few cases will be listed up in order to show its complexity. The term network itself can be different depending on its type: e.g. it can be transportation network, a telecommunication network or network model of a phenomenon, or device. Each have its on characteristics, in this chapter we are focusing on telecommunication networks in general.
Telecommunication networks can also be very different depending on the technology being used. The paper later will focus on a subclass of telecommunication networks, namely traffic demand optimization of transmission networks. In this chapter, we are focusing on the common characteristics of Telecommunication network optimization. Not only the term network, but the term optimization can mean a number of things, depending on the goal of the optimization, and the optimization environment. Greenfield optimizations differ greatly from optimization of an existing network, and the parameter (e.g. network parameter as link capacity, delay etc.) to be optimized greatly influence the end result and the methods to be used. Further in this chapter we will focus mainly on optimization of an existing network, and the main parameter to be optimized is link capacity.

To make the paper more understandable we would like to remark the following terminology related things: further in this paper I will use need or needs as customer requirements, and demands as traffic demands between two points. A network optimization project contains several phases – either stated in the project specification, or contains these parts as logical steps of the optimization. These phases are common in most network optimization projects.

**Phase 1 – Defining the requirements**
In the first phase of a network optimization project we need to find out the following:

- what the objective of the project is
- what the required input information should be

These have to be stated as clearly as possible, as the goal is to build up a model based on the information we received. So the first phase of a network optimization

project is finding out what the current needs are. This can be done by making a survey of current and future needs.
The survey starts with an informal understanding of problem. So that it can work efficiently a workgroup (of team members) needs to be set up, and the following topics are to be discussed:

1. The purpose of the project – this has a huge impact on the whole process. This defines what to optimize the project for – e.g. the aim of the project.
2. Current and/or future needs: the discussion within the workgroup has to cover what the current needs are, the possible future needs as well as the important perspectives and characteristics of the demands.
3. Introducing characteristics of the topology: this should cover what the main characteristics of the topology, e.g. what sort of network and traffic type is being discussed (IP/Transmission Network/Circuit switched network/ATM/MPLS), and those characteristics that are the specific nature of the topology (Tree networks/rings/meshed networks).
4. Additional needs regarding QoS: Different traffic profiles need to be defined in this case in the network, and there specific QoS needs: this highly effects the classification.
5. Protection mechanisms to be used: it has to be addressed clearly, what sort of protection mechanisms are to be used and for which traffic flows/demands should these protection mechanisms used.

The result of this survey and discussions need to be put into a formal document (e.g. Customer Requirements Document. Further in this document the required data from the customer need to be specified.)
These are only the most important aspects that have to be covered in the first phases of the discussion. Besides these many other important questions can be discussed e.g. characteristics of traffic types, special customer requests regarding nodes, traffic demands and so on. After the defining the aim of the project, and clarifying the current requirements a snapshot of the network is needed.
This can be achieved a number of ways – *if there is an inventory management system available, the most obvious idea is to take a snapshot of the actual status of the inventory management system. This will form the basis of the next Phase. In case of a green-field deployment, there is no current network* – so there is nothing to take a snapshot of.

**Phase II – Feasibility study**

The main purpose of this Phase is to find out, whether it worth making a network optimization, or the network is in a state that efforts spent on optimization (and possible commission of the optimized network) will overweight the benefits. This is more of a business benefit which is worth taking a look at. This Phase might not be needed, in case there is a clear decision that the optimization is needed.

At the beginning phase the topology of the network should be clearly visible with all its pros and cons. From the data acquired, after preprocessing probably it turns out that some optimization parameters are far from the optimum. This have a number of reasons, most important of which is that the demands are changing over a certain time period, and a solution being appropriate in a certain stage of network development, might seem awkward or improper in a latter stage. Of course, these assumptions can not form the basis of feasibility study – a very rough search for optimization must be done in this Phase, in order to be in a position to clearly state how much benefit an optimization can bring to the network. The result of such a rough estimation can – *by no means* – be the optimal network structure – it is to be reached in the next Phase, but it must be good enough to be able to make an effort estimation/how much benefit can the optimization bring. We have to select some criteria, that will form the basis of our study

a. it has to show approximately how far the network parameter to be optimized is from the optimum,
b. from this criteria we need to be able to estimate the efforts required to fulfill the optimization and rerouting phases – e.g. the following phases. Selection of such criteria is to be covered later.

**Phase III – Optimization**

Using a scientific approach for finding an optimum is necessary, because the optimization problem is too complex once the network size has reached a certain limit (10xn nodes+), and the problem has further constraints. This problem will be described further in Methods for transmission network optimization. This is the main purpose of the Optimization phase. The purpose of this Phase is to do the actual optimization, e.g. to find a reconfiguration of the network close to an optimum, that is acceptable. The optimization itself is usually a very complex problem – *depending on the network type and objective of the optimization it can be an NP* – complete problem. The effectiveness of the network optimization highly depends on a number of factors – *number of nodes, edges, and demands in the network, as well as the requirements. Before this Phase, a new snapshot of the*

*network is needed* – which will form the basis of the optimization, because there could be several changes since the previous snapshot in a real life network. The reason for this step is that significant amount of time might have passed between the previous phase, and this phase. Finding the optimum method for developing the optimum includes theoretical research, development of algorithms, testing, and actual running of the algorithm itself.

Due to the long-lasting nature of finding, or developing a method for finding the optimum it is important to develop a method for the project that is repeatable. It is important to note that – *during the time of the actual optimization* – the network itself is subject to change, so what actually will be optimized is a different network to what the network is at the end of the network. The change (whether it is change in topology or traffic demand, or any relevant network parameter)in most cases is not so significant, but it is important to note. If it is a factor to count with, therefore it is important that after the initial development of an optimum finding algorithm, using the optimum on a slightly modified traffic demand matrix should not take significant amount of time.
At this Phase, in order to be able to find the correct mathematical model for the optimization, the following criteria should be met:
1. Topology of the network has to be available
2. Traffic demands must be available
3. Objective function must be selected

These are the preliminary requirements for finding a good mathematical representation of the network – that can form the basis of the optimization. The optimization model is also highly dependent on the purpose of the project, e.g. in our understanding, what would be an optimal network (objective).
Different models are being used for topology optimization or traffic demand optimization, or any other optimization problem. The different models are well described (e.g. in Ref. 1.)

The mathematical model used for such an optimization will be discussed in the chapter **Methods for transmission network optimization**.

**Phase IV – Commissioning the changes**
The whole purpose of network optimization is to reach an optimum state of network parameter(s) but a very important aspect should not be forgotten. After the network optimization there will be an optimal network available – on paper, or

on computer, but not in the real network. Depending on the complexity and amount of work of commissioning the changes in the network, commissioning work itself could be a very important part of a Network optimization project. In certain cases, the amount of commissioning work, after doing a optimization of the network, will be so much that

1. Will never be done (in case Phase II is done well, this should not happen because in Phase II a good estimation is given for optimum, and the efforts);
2. Must be done automatically somehow because the manual commissioning is such a tedious work – and manually could take too much time and effort.

**Phase V – Conclusions**

After the optimization is done, a very important Phase has to be done: the result must be evaluated. Questions to be answered are: is the result is according to what was expected. Should the process be made a regular process, if so how often is to be repeated. What conditions should occur to do a network optimization project once more (if not done regularly).

## 3. Transmission network traffic optimization

Transmission network optimization is subclass of network optimizations. The general phases of such a project have been covered in the previous chapter. In this chapter, the specific characteristics of a traffic demands optimization are covered. Transmission network providers often reach a state of the network after few years of service, when they figure out that the current state of the network – *due to the network evolution over the years* – is far from being the optimum. Network owners are sometimes aware of this fact but they do not know, how much effort would be required to rearrange the network.

**Characteristics of the transmission network optimization project**

As the title implies, the current section deals with the *optimization* of existing network link capacities. This is an important characteristic of the problem because it means that there are *capacity constraints* on the network, imposed by current network resources (more on this in the section: Methods for transmission network optimization), which must be taken into account in the mathematical model. This is one important characteristic of such a problem. The second important characteristic of the project is that the optimization is a link capacity optimization task. Demands are given as certain traffic between the nodes, and the optimum

routing is to be found in the network, given there are certain link capacities as constraints. The link capacities are modular.

Third important characteristic is that this is a *transmission network* with its network topology and all the characteristics for protection and quality characteristics. It is important, that protection and quality requirements must be discussed. (Only one aspect of quality, demand availability is understood in this case), in certain cases like the one discussed in this paper, it is subject to optimization as well.
In short:

- modular link capacities are constraints in the optimization problem
- optimum routing is to be found for the traffic demands
- characteristics of the transmission network are to be taken into account.

**Availability and protection as a subject to optimization**

Protection and availability is an inherent nature of transmission networks. Transmission network designers, and engineers in many cases think that all traffic should be protected. This is very good, from the availability perspective – it provides the well known 99,999% availability for the path. This might be very good from the technical perspective – on the other hand path protection is an overkill, from the network capacity perspective, whether this is economically viable is up to the service provider to decide. A huge amount of network capacity can be saved by rethinking the current strategy for protecting certain traffic. E.g. it is a viable alternative, to lose some traffic in case of node or link outage from the business perspective, if on the other hand we save a lot of link capacity. Of course this highly depends on customer requirements.

The questions is now what is the acceptable availability (as a measure of demand quality), and how it should be decided what to protect, and what shouldn't. In order to be able to decide we need to classify the traffic. A certain suggestion will be discussed here, how to do this classification. By no means this is the only possible way of classifying, this is one method, that can be used. In this case, we are considering a multi service provider, that provide voice, and data services, and the majority of the revenue comes from a voice traffic.

We have considered 3 different traffic types for classification:

a. Signalling traffic, signaling does not require too much bandwidth in a typical network however it carries very important traffic. It is a very risky not to

protect signalling traffic – with very few business benefits. Signalling traffic should be protected.

b. Voice traffic: This brings most of the revenues for most service providers, however this requires most of the traffic also. A clear decision must be made how much, and what sort of traffic should be protected (Voice Switches are usually configured in load balancing fashion, e.g. only part of the traffic is lost, at a single link.). Of course the characteristics of the core voice network need to be taken into account The traffic is to be classified how important it is.
c. Data traffic: Data services at the concerning service provider are anyhow only 99,9% availability services. Because of the lower availability requirement in most cases they should not be protected.

## 4. Methods for transmission network optimization

Optimization problems are in general LP/MIP [*Linear Programming (LP), Mixed Integer Programming (MIP)*] problems. In general Transmission network optimization problems are Mixed-Integer Problems (see Ref. 1). Because of this fact they are NP-Complete, which results in the following: solution time increases exponentially with the number of nodes. It is important to highlight this – and its effect on a real example is to be discussed further in the chapter **One practical example**.

**Linear Programming (LP), Mixed Integer Programming (MIP)**

LP, IP, MIP problems are the subject of OPERATION research theory, and they formulate problems that needed to be optimized within certain boundaries. According to Reference 2, can be formulated as follows:

LP Problem:

*indices:*

j = 1, 2, ..., n variables
i = 1, 2, ..., m constraints

*constants:*

aij coefficient for variable j in constraint i
bi right-hand side of constraint i
cj cost coefficient of variable j

*variables:*

xj j-th variable objective
min z =_*cj xj*

*constraints:*

*_aijx j_ bi*

i= 1, 2, ..., m.

In ordinary words it can be formulated so: we have a vector of variables (xj), which is with certain weight values (aij) is bounded by another vector (bi). These inequalities are the constraints. The goal of the problem is to find a feasible variable vector x (e.g. an x that fulfills all inequalities), that is optimal.
The criterium for optimality is to minimize (or to maximize) a certain function called objective function.

If all xj are real numbers then it is a *linear problem*.
If some xk of xj can only be integers, then it is a *Mixed Integer Problem (MIP)*. If all xj can only be integers then it is *Integer Problem (IP)*.

**Models for transmission network optimization**

Three design problems have been taken into consideration, the mixed integer problem (Modular Flow Allocation) uncapacited problems and capacited problems. (See Reference 1 pp. 106–115). These problems are discussed in the following section.

**Mixed integer Problem Modular Flow Allocation**

"The requirement of integral flow arises naturally when we wish to allocate demand volumes in certain demand modules. For example, in transmission networks, demand volume is usually given in terms of modular units such as the number of Optical careers OC-3s needed between two nodes." (See Reference 1 pp. 123–125). Its mathematical model is as follows.

MIP: A/MFA
Modular Flow Allocation
*constants:*

dedp = 1 if link e belongs to path p realizing demand d; 0 otherwise
Ld = demand module for demand d
Hd = volume of demand d expressed as the number of demand modules
hd = demand volume (hd= Ld Hd)
ce = capacity of link e

*variables:*

xdp = flow allocated to path p of demand d (continuous non-negative)

udp = non-negative integral variable associated with variable xdp
*constraints:*
xdp=Ld*udp, d = 1,2,…, D; p=1,2,… Pd.
*_xdp = hd* d = 1,2,…, D
___*edp xdp* £ *ce* e=1, 2,…, E

Please note that there is no objective function selected for the MIP problem. At this stage this is purposely done so, this will be discussed in Section Objective function. In the following 2 sections we have covered two simplification of this problem – in order to get through the NP – Completeness barrier, which significantly limit the number of nodes.

**Uncapacited problem – LP – Simple Design Problem**
The goal of the uncapacited problem, is to find an optimal solution to the transmission network optimization problem, without the link capacity constraints fixed. The formulation of the uncapacited simple design problem was the following, that we considered. The mathematical formulation will be as follows (See Reference 1 pp 108–110):

LP:D/SDP: Simple Design Problem
*indices:*
d = 1,2, … D demands
e = 1,2, … E edges /arcs/links
v = 1,2, ... V nodes, vertices
*constants:*
$a_{ev}$ = 1 if link e originates at node v; 0 otherwise
$b_{ev}$ = 1 if link e terminates at node v; 0 otherwise
$s_4$= source node of demand d
$t_d$ = sink node of demand d
$h_d$ = volume of demand d
ξe = unit cost of link e
*variables:*
$x_{ed}$ = flow realizing demand d allocated to link e (continuous non-negative)
$y_e$ = capacity of link *e* (continuous non-negative)
*objective:*
minimize $F = \Sigma \xi_e y_e$
*constraints:*
$\Sigma a_{ev} x_{ed} - \Sigma b_{ev} x_{ed} =$

= a. $h_d$ = if v= $s_d$
b. 0 if v<> $s_d$, $t_d$ v=1,2…V d = 1,2…D
c. –$h_d$ = if v= $t_d$
$\Sigma x_{ed}$ $\Sigma y_e$ e=1,2,…., E

Please note that in this particular case there is an objective function. This is due to the fact that there is no capacity limit imposed on the links (or the capacity limits are also variables).

**The capacited problem – LP – Pure Allocation Problem**
The capacited problem, is basically the Linear variant of the MIP, without the modular nature of transmission network.
The formulation of the problem we considered for the transmission is the following:

LP:A/PAP: (Pure Allocation Problem)
*constants:*
$\delta e_{dp}$ = 1 if link e belongs to path p realizing demand d; 0 otherwise
$h_d$ = volume of demand d
$c_e$ = capacity of link e
*variables:*
$x_{dp}$ = flow allocated to path p of demand d (continuous non-negative)
$\Sigma x_{dp} = h_d$ d = 1,2,…, D
$\Sigma\Sigma \delta_{edp} x_{dp} \leq c_e$ e=1,2,…, E

Please note two things. 1 objective functions is not selected, and 2 the similarities, and the key
differences with Mixed integer Problem Modular Flow Allocation.

**Objective function**
So far we have not selected an objective function. The selection of an objective function in itself can be a challenging task. The literature (See Reference 3 pp. 114) referred to in his book, suggests an objective function:
minimize $F=\Sigma\phi_{dp}\Sigma_{px}$
where $\phi_{dp}= \Sigma r_e \delta_{edp}$ is the unit revenue from path Pdp of demand d in terms of link revenue re.
However this is by far not the only objective function that can be used, but a well usuable one. So we will use a modification this (the sum of all number of hops of all demands).

**Simplifying the network**

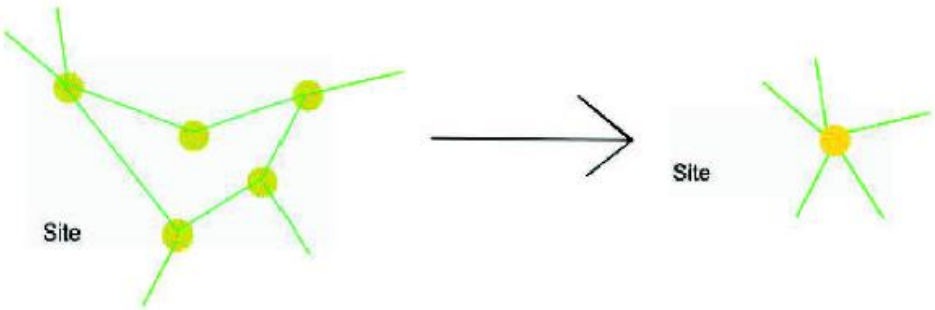
As the number of nodes in the real life problem is several hundreds it is important to think over what sort of modifications of the network can be used. A few of these modifications are:

a. removal of non-sink and non-source nodes with exactly 2 edges. (These are the so called boosters or repeaters) or 2 degree nodes

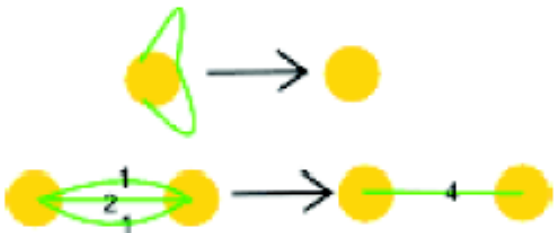
b. aggregating of some sources and demands into a supernode aggregating sources and demands.

They have a drawback also: the interconnection traffic might not be correctly calculated between such nodes. In our network a simplification of a different kind has been used:

a. the nodes at each site have been merged into a supernode (see figure)




b. the trivial links have been removed (see figure)




c. we substituted the n parallel links with one link with the sum of the original capacities (see figure)

## 5. One practical example

The following chapter deals with the practical results of an optimization project. Our goal in this chapter is to show that optimization techniques are beneficial to network operators. The measure that we are going to take into consideration is the comparison of the network to an optimum stage, where the link capacities (according to our objective function) are at a minimum level, while fulfilling the demand, and link capacity constraints.
The quality measure that we used in the network to present the quality is the average length of the paths – *as they are somehow in connection with link capacities. This quality measure is a general unit for measurement, by no means the only possible measurement unit, however* – as our figures will show, it gives an easy comparison for the results.

## Summary

Our intention with this paper was to give a systematic overview of network optimization, and to introduce some methods we have used in a live network. In this paper we have covered:

- A systematic approach and project phases for a network optimization project in the chapter

**Phases of a network optimization project**

- Characteristics of a transmission network traffic optimization project in the chapter

**Transmission network traffic optimization**

- Mathematical methods for transmission network traffic optimization in the chepter **Methods for transmission network optimization**
- Results based on this methodology in a live network in the chapter **One practical example.**

In this latter chapter we tried to show that using well built mathematical models for optimization results in an optimum network in terms of link capacity. This has brought up to 30% better utilization in the given network, which results in cost savings mostly in Capital Expenditure (CAPEX), and with in case it is used well it can help network designers in finding free capacities in the network – which helps network designers when planning future extensions and investments. In short, using this methodology a set of tools can be built up for the transmission network

designers, that enable them to use their own network resources in a more efficient way. An even better performance can be achieved by applying automatic methods for rerouting.

**References**

1. M. PIÓRO, D. MEDHI: *Routing Flow and Capacity Design in Communication Networks*, Morgan and Kaufman, June 2004, pp. 625–638.
2. PIÓRO, Medhi: *Routing Flow and Capacity Design in Communication Networks*, pp. 153–154.
3. SZLOVENCSAK, A., GODOR, I., HARMATOS, J., CINKLER, T.: Planning reliable UMTS terrestrial access networks. Ericsson Res, In: *Communications Magazine*, IEEE, 40 (2002) 66–72.
4. TAMÁSI Levente, JÓZSA Balázs Gábor, ORINCSAY Dániel: *Kommunikációs hálózatok költséghatékony tervezése a forgalomeloszlás periodikus változásainak figyelembevételével*, Híradástechnika, 2004.
5. SZIGETI, J., TAPOLCAI, J., CINKLER, T., HENK, T., SALLAI, G.: Stalled information based routing in multidomain multilayer networks, In: *11th International Telecommunications Network Strategy and Planning Symposium.* NETWORKS 2004, pp. 297–302.
6. ORINCSAY Dániel, JÓZSA Balázs Gábor: *Kommunikációs hálózatok költséghatékony tervezése*, Híradástechnika, 2003.

***Dorkó Zsolt[44]: Szervezetek struktúrája-I.***

**Absztrakt**
*A cikk bemutatja a PhD jelölt értekezésének egy részét.*

**Abstract**
*The article presents parts of thesis PhD candidate's.*

## 1. Bevezetés

Anyagom alapvetésként fogadtam el azt a feltevést, miszerint a szervezet működését alapvetően meghatározza a szervezeti felépítés jellege, a feladatrendszere, illetőleg a gazdálkodásának a keretei. Az előző részekben már foglalkoztam a költségvetési szemléletet középpontba állító rendőrségi gazdálkodással, amelyben azt mutattam be, hogy milyen pénzeszközökkel, mekkora gazdálkodási mozgástérrel látja el a rendőrség, mint költségvetési szerv a feladatait. Konkrét példákon keresztül bemutattam a rendőrség, illetve a NAV szervezetét, azok szervezeti- és irányítási elemeit, alá-fölérendeltség viszonyait. Ezzel párhuzamosan elemeztem a vizsgált szervezetek feladat- és hatásköreit abból a szempontból, hogy milyen ügyeket lát el, és milyen szolgáltatásokat nyújtanak. Mindezen szempontok alapján vizsgáltam a szervezetek informatikai feladatokat ellátó elemeit.
Az értekezés ebben a részében a szervezetek általános felépítésével, illetve annak elméleti megközelítésével, optimalizálásának lehetőségével foglalkozom, továbbra is az informatikát állítva vizsgálat középpontjába. A szervezeti felépítésre vonatkozó alapvetésem, tehát az, hogy a költségvetési szervezetek struktúrája hat a működésük hatékonyságára. Ebből következően az optimális szervezeti felépítés támogatja a vezetést és ezáltal pozitívan befolyásolja a hatékonyságot, míg a nem megfelelően felépített szervezeti struktúra csökkenti a hatékonyságot és rontja a szervezet eredményességét.
A szervezeti felépítés elméletének vizsgálatánál elsősorban Dobák Miklós és munkatársai által megírt Szervezeti formák és vezetés című kiadványra,[45] mint a szakirodalmakban gyakran hivatkozott műre, illetve a tanulmányaim során elsajátított ismeretekre támaszkodtam. Dobák szerint „ *A szervezetek hatékonysága döntően azon múlik, hogy milyen a struktúrájuk, hogyan illeszkednek*

[44] Heves Megyei Rendőr-főkapitányság osztályvezető
[45] Dobák Miklós és munkatársai: Szervezeti formák és vezetés - Közgazdasági és Jogi Kiadó - Budapest, 1996 - ISBN 963 224 376 5

*egymáshoz a működési folyamataik, milyen vezetési elveket és módszereket alkalmaznak, mennyire támogató jellegű a szervezet kultúrájuk.*"[ 23.o.] Ez egybevág az általam is elfogadott alapvetés azon részével, miszerint a szervezet működését alapvetően meghatározza a szervezeti felépítés jellege. A két meghatározás közelítése érdekében az értekezésem ezen szakaszában a szervezeti felépítést és a szervezeti struktúrát szinonimaként használom. A szervezeti struktúrák jellemzői, a munkamegosztás, a hatáskörmegosztás, a koordinációs eszközök, illetve a konfiguráció.

## 2. Munkamegosztás

A munkamegosztás a szervezet feladatainak részfeladatokra való bontását és a részfeladatok egyes szervezeti egységekhez való telepítését jelenti, amely a szervezet belső tagolásának alapját képezi. Az így kialakított szervezeti egységek által elvégzett feladatok tovább oszthatók, ennek megfelelően beszélhetünk elsődleges, másodlagos stb. munkamegosztásról. A munkamegosztás a legáltalánosabb felosztás szerint lehet, funkcionális, tárgyi vagy területi elv szerint. A funkcionális elv szerint a homogén szakterületeket, a tárgyi elv alapján a homogén input, illetve output csoportokat, a területi elv szerint a földrajzilag elkülönülő szervezeti egységeket különítenek el egymástól. Azokat a szervezeteket amelyekben kizárólag a fenti három elv egyike alapján történik a munkamegosztás egydimenziós szervezeteknek nevezzük. Amelyeknél az elsődleges munkamegosztás szintjén párhuzamosan alkalmazzák az elkülönítés elveit, két- és többdimenziós szervezetnek nevezzük. Ezek alapján egydimenziós szervezetnek tekinthetjük az elsődleges munkamegosztás alapján elve szerinti a lineáris, a funkcionális, valamint a divizionális szervezeteket, többdimenziósnak nevezzük a mátrix szervezeteket.

## 3. Hatáskörmegosztás

A hatáskörmegosztás a szervezetrendszerben érvényesülő munkamegosztásból kiindulva közelíthető meg. A munkamegosztás alapján a szervezeti egységekre háruló feladatokat csak akkor tudják ellátni, ha ahhoz megfelelő hatáskörrel rendelkeznek. A hatáskörmegosztás a döntési és utasítási jogköröknek a felosztását jelenti a vezetés és az alárendelt szintek között. Megkülönböztetünk egyvonalas, illetve többvonalas szervezeteket. Egyvonalas szervezetekről akkor beszélünk, ha az alárendelt egységek csak egy szervezeti egységtől kaphatnak utasítást. Az egyvonalas szervezetekhez tartozik a lineáris szervezet és a divizionális szervezet.

Többvonalas szervezetekben az alárendelt egységeket két vagy több szervezeti egység vagy személy is utasíthatja. E csoportba tartoznak a funkcionális szervezetek és a később kialakult mátrix típusú szervezeti formák.

## 4. Koordinációs eszközök

A koordinációs eszközök vizsgálata előtt célszerűnek tartom a koordináció, illetve a koordinálás kifejezések lexikon szerinti értelmezését elővenni. A latin coordinatio eredeti jelentését keresve a *„rendezettség, összerendezettség”*[46] *„egymás mellé rendelés; összehangolás, összeegyeztetés - az azonos feladatkörű vagy ugyanazon a területen működő szervek működésének összeegyeztetése”*[47] kifejezéseket találjuk. A munkamegosztás és a hatáskörmegosztás mellett alapvető strukturális jellemző a koordináció. A szervezeti koordináció az eltérő feladatokkal és hatáskörökkel rendelkező, de egymással kapcsolatban álló szervezeti egységek működésének a szervezeti célok teljesülése érdekében történő összehangolását jelenti, amely napjainkra stratégiai jelentőségűvé vált. Dobák, Khandwalla (1975) osztályozását [51.o.] emeli ki, mely megkülönböztet személyorientált, technokratikus és strukturális koordinációs eszközöket. A személyorientált koordináció az egyének szervezettel való azonosulását célozza meg. A technokratikus típusú koordinációs eszközök a szabályzatok utasítások tervek programok. Strukturális koordinációs eszközök csoportját a különböző egységek közötti kapcsolatok, csoportok, projektszervezetek határozzák meg.
A személyorientált koordinációnak elsősorban az a funkciója, hogy segítse az egyének azonosulását a szervezettel, a célokkal és a feladatokkal, illetve fokozza az elkötelezettségét. A személyorientációt egyrészt az egyéneket közvetlenül ösztönző, ráhangoló, kényszerítő eszközök, másrészt pszichológiai és ideológiai befolyásolások jelentik. Az egyéneket közvetlenül ösztönző, motivációs eszközök lehetnek a képzés, továbbképzés, vezető kiválasztás, a kényszerítő eszközök lehetnek a vezetői hatalom egyes eszközei, a ráhangolás eszköze lehet többek között a meggyőzés. A pszichológiai és ideológiai befolyásolást jelentősen meghatározza a szervezet belső értékrendje, szervezeti kultúrája. Amennyiben nem a szervezet, hanem a vezetés szempontjából vizsgáljuk meg a koordinációt, mint a vezetés egyik funkcióját[48], akkor azt látjuk, hogy a koordináció a vezetői

[46] Révai nagy lexikona 1915
[47] Új magyar lexikon 1962
[48] Henry Fayol (1916) a következő vezetési funkciókat különbözteti meg: tervezés, szervezés, közvetlen irányítás, koordinálás, ellenőrzés. Dobák a vezetési funkciókat a következőképpen osztotta fel: célkitűzés és stratégiaalkotás, szervezés, munkatársak közvetlen irányítása, kontroll.

tevékenység egyik legfontosabb része. Az hogy a vezető milyen módon gyakorolja a szervezetben a vezetés különböző funkcióit, közvetve hatással lehet a szervezeti struktúrára is. A vezető tehát a vezetés koordinációs funkciójának gyakorlásakor biztosítja szervezet összehangolt működését. Ezek a koordinációs mechanizmusok szorosan kötődnek a vezető személyéhez, elsősorban a személyes vezetés gyakorlása révén érvényesülnek. Ebben az értelemben a közvetlen irányítás, vagy személyes vezetés kapcsán, elsősorban személyorientált koordinációs eszközök gyakorlásáról beszélhetünk, de a vezetés célkitűző és stratégiaalkotó funkciója gyakorlásakor is működteti a személyorientált koordináció eszközeit.

A technokratikus típusú koordinációs eszközök főként a menedzsmentkonroll és controlling lényegi elemeit tartalmazzák. Jellemzően formalizált, dokumentumokban rögzített előírások, amelyek a munkavégzés tárgyára, kívánatos módjára vagy elvárt eredményére vonatkoznak. Leggyakoribb megjelenési formáik az alapító okirat, szervezeti és működési szabályzat, egyéb szakmai szabályzatok és eljárásrendek, stratégiák, fejlesztési programok, operatív tervek, költségvetések, pénzügyi elvárások, írásos vezetői utasítások, rendelkezések, intézkedése, belső tájékoztató anyagok. A szervezetek működését, különös tekintettel a vizsgálatom tárgyát képező költségvetési szervezetekre, számos egyéb jogi norma is meghatározza, amelyeknek a belső szervezeti szabályok és utasítások nem mondhatnak ellent. A technokratikus eszközök legnagyobb előnyei az egyértelműség, a kiszámíthatóság. A vezetés koordinációs funkciójának gyakorlása során működteti a technokratikus koordinációs eszközöket is. A vezetés célkitűző, stratégiaalkotó és kontroll funkciója is működteti a technokratikus típusú koordinációs eszközöket.

A strukturális típusú koordinációs eszközök az adott szervezeti struktúra keretei között olyan pótlólagos koordinációt jelentő megoldásokat jelentenek, amely az adott struktúra lényeges átalakítása nélkül biztosítják a megnövekedett koordinációs igényt. A szervezeti struktúrára jellemző munkamegosztás és a szervezetrendszerben érvényesülő hatáskörmegosztás alapján megvalósuló hierarchia révén létrejövő szolgálati út[49], önmagában is jelentős koordinációs eszközként jelenik meg. A strukturális koordinációs eszközöket általában ezen felül értelmezik. Ezek *„..a szervezet alapstruktúrájába beépülő, az elsődleges munkamegosztást és a hatáskörök megosztását nem vagy csak átmenetileg módosító…”[52.o]* eszközök, amelyek rásegítő megoldásokként, a meglévő szervezeti struktúra esetleges koordinációs hiányosságait pótolják. Ilyen eszközök a

[49] A szolgálati út az ügyek intézésének az a módja, melyen keresztül fokozatosan jut el az ügy alulról felfelé vagy felülről lefelé ahhoz, akinek az ügyben döntési, utasításadási joga, illetőleg intézkedési, végrehajtási kötelessége van.

projektek, a teamek, az ad hoc és állandó bizottságok, a törzskarok, valamint az általam nem elemzett termékmenedzseri rendszer.

A projektben a szervezet különböző hierarchiaszintjein, szakterületein tevékenykedő, a kitűzött cél eléréséhez szükséges speciális ismeretekkel rendelkező szakemberek csoportja, a meglévő szervezeti struktúra átalakítása nélkül hajtja végre feladatát. A projektre jellemző, hogy az elvégzendő tevékenységek egymással összefüggenek, egy konkrét eredmény elérésére irányulnak, meghatározott idő alatt végzendő el, és költségvetésük többnyire adott keretek között van.

A team a projekthez hasonlóan a szervezet különböző hierarchiaszintjein, szakterületein tevékenykedő személyekből álló feladatorientált és autonóm egység, amelyet probléma megoldására, illetve állandó vagy ideiglenes feladat elvégzésére hoznak létre. A projektszervezettel ellentétben nem csak új és egyedi problémák megoldására hozzák létre, és az időkorlát sem jellemző rá. A teameknek főleg a döntés-előkészítés és a többtényezős döntés szakaszban van meghatározó szerepük. Belső felépítésük nem hierarchikus belső, többnyire formális vezető nélkül látják el feladatukat.

Ad hoc és állandó bizottságok fent ismertetettekkel ellentétbe általában nem speciális tevékenységet végeznek, inkább a belső kommunikációt segítik elő a szervezet különböző szintjei, szakmai területei között. A bizottságokra jellemző, hogy tevékenységük egyaránt lehet időben korlátozott vagy állandó, összetételük heterogén, a tagok eredeti státuszukat az eredeti szervezeti egységükben mindvégig megtartják, belső szervezetük nem hierarchikus, a felső vezetés mellett működnek annak tehermentesítése érdekében. A bizottságokat tanácsadó, információs, döntéshozó, és végrehajtó funkcióval bízhatják meg.

A törzskarok a stratégiai döntések előkészítését, a vezetési tevékenység közvetlen támogatását végrehajtó szervezeti egységek, a vezető közvetlen alárendeltségében. A törzskaroknak döntési utasítási jogkörük nincs. A vezető befolyásolásával vesz részt a döntések előkészítés, a döntés, a végrehajtás és az ellenőrzés egyes fázisaiban. A törzskarok feladatrendszerükben csökkentik a vezető túlterheltségét, fokozzák a döntések szakmai színvonalát, elősegítik a szervezetben jelentkező sokrétű problémahalmaz szakmailag megalapozott kezelését. Kialakításukkal egy új hatalomgyakorlási és érdekérvényesítési forma jelent meg, ami magával hozta a szakmai és irányítási koordináció szétválását is. Továbbra is követve a többi koordinációs eszköz vizsgálatának metodikáját, megállapítom, hogy a vezetés koordinációs funkciójának gyakorlása során működteti a strukturális koordinációs eszközöket is. A vezetés célkitűző, stratégiaalkotó és szervezési funkciója is működteti a strukturális típusú koordinációs eszközöket.

Elsősorban a strukturális koordinációs eszközök kapcsán, a kommunikációs utak iránya szerint vertikális és horizontális típusú koordinációt különböztethetünk meg. A kommunikációs utak iránya jelzi a hierarchia irányát is. A vertikális koordináció elsősorban az egymás alá-fölérendelt egységek közötti kommunikációt jelenti, amelynek formális megnyilvánulása az utasítás, illetve a jelentés. A horizontális koordináció pedig az azonos tevékenység és hatásköri szinten lévő szervezeti egységek közötti kommunikációhoz kapcsolódik.

**5. Konfiguráció, mint másodlagos strukturális jellemző**

A fentiekben kifejtett strukturális jellemzők, a munkamegosztást, a hatásköri rendszert, és a koordinációs eszközöket, elsődleges strukturális jellemzőnek tekintjük, mivel önmagukban kialakítják a szervezet struktúrájának vázát, azaz a konfigurációt. Ezzel szemben a konfiguráció másodlagos strukturális jellemző. Az első három ugyanis gyakorlatilag kialakítja a szervezet struktúrájának vázát. A konfiguráció meghatározható a szervezet mélységi, illetve szélességi tagoltságával, valamint az egyes szervezeti elemek méretével. Másképpen fogalmazva a hierarchikus szintek száma, az egyes hierarchia szintjén, az egy vezető alá közvetlenül tartozó alárendeltek száma, és az adott egységhez tartozó foglalkoztatottak száma segítségével, gyakorlatilag a szervezeti konfigurációt alkotjuk meg, amely a korábbiaknak megfelelően szintén egy strukturális jellemző.

**6. Szervezeti formák**

A fentiekben bemutattam a szervezeti struktúrák jellemzőit. A funkcionális, tárgyi vagy területi elv szerinti elsődleges munkamegosztás alapján megkülönböztettem az egydimenziós, illetve a két- és többdimenziós szervezeteket. Egydimenziós szervezetnek tekinthetjük a funkcionális és a divizionális szervezeteket, többdimenziósnak nevezzük a mátrix szervezeteket. A hatáskörmegosztás, azaz a döntési és utasítási jogkörök a felosztása alapján különbséget tettem az egyvonalas, illetve többvonalas szervezetek között. Egyvonalas szervezetekként értelmezzük a lineáris és a divizionális szervezeteket, többvonalas szervezetekként a funkcionális és a mátrix típusú szervezeti formákat. A koordinációs eszközök elemzésénél a bemutattam az adott szervezeti alapstruktúra megváltoztatása nélkül működtethető szervezeti elemeket, a teameket, a bizottságokat, illetve a törzskarokat. Bemutattam azt, hogy a konfiguráció, hogyan határozza meg a szervezet mélységi, illetve szélességi tagoltságát, valamint az egyes szervezeti elemek méretét.

A fenti jellemzők alapján áttekintem a legelterjedtebb szervezeti formákat. Nem célom valamennyi szervezeti forma részletes bemutatása, mivel az értekezésem szempontjából szükségtelen a rendvédelem területén nem alkalmazható struktúrák elemzése. Elsősorban azokat az alaptípusokat tekintem át, amelyek szervezeti formák fejlődése során alapvetően meghatározzák vagy, a jövőben megváltoztathatják rendvédelmi szervek elsősorban a rendőrség szervezetét. Ezek közül megvizsgálom a lineáris, a törzskari, a funkcionális, a divizionális, és a mátrix szervezeteket.

## 7. A lineáris szervezet

A lineáris struktúra a legegyszerűbb szervezeti forma, gyakran egyszerű struktúrának is nevezik. A fent tárgyalt strukturális jellemzők szerint a lineáris szervezetek munkamegosztás szempontjából egydimenziósak, a hatáskörmegosztás szempontjából erősen centralizált, egyvonalas struktúra. A koordinációt főként a vertikális kommunikáció biztosítja, a feladatszabás és a végrehajtás jelentése, ugyanazon a vonalon, a szolgálati úton történik. A horizontális kapcsolatok megvalósítása csak informálisan lehetséges ezért esetlegesek és, nehézkesek.
A tisztán lineáris szervezet *„…fő elve a vezetés szigorú egysége…”*,[NKE jegyzet 43.o.] amelyben nem válik el egymástól az munkáltatói jogkörök gyakorlása és a szakmai felügyelet a szakirányítás. Az egyvonalas szervezetek legnagyobb előnye az egyszerűségből adódó áttekinthetőség. A vertikális irányú információáramlás miatt egyértelműek a függelmi viszonyok, az utasítások címzettjei, a felelősség, ezáltal egyszerű a számonkérés. A szervezet horizontális és vertikális tagozódása az erőforrások allokációja könnyen változtatható, ha a feladatok mennyisége, vagy minősége megváltozik, ezáltal egyszerűen kielégíthetőek az újonnan jelentkező szakmai igények. A megváltoztatott szervezet továbbra is megtartja a lineáris formát, mert szervezeti hierarchiában nélkülözhetetlen az egyértelműen tisztázott, függelmi kapcsolatok érvényesítése. Az egyvonalas kommunikáció miatt azonban a horizontális kapcsolat, bonyolult és nehézkes, a szervezet reakcióideje és az információáramlás lassú, a szervezeti elemek egymással nem kommunikálnak, jelentősen megnő az információtorzulás, illetve a bizonytalanság esélye. A tisztán lineáris formában kialakított szervezetekben a vezetőnek teljes mértékben ismernie kell az alárendelt szervezeti egység feladatrendszerét, hiszen mindenben a vezető dönt, ezért az összetett koordináló-irányító tevékenysége miatt rendkívül leterhelt. Az ilyen szervezet elsősorban feladat orientált, ahol vezetői akarat maximálisan érvényesül, az új ismeret iránti fogékonyság is alapvetően a vezető személyétől függ, ami nagyban befolyásolja az alulról jövő jó kezdeményezések, illetve az

innováció érvényesülését. Az erősen hierarchikus szervezet növekedése bürokratizálódást és befelé forduló szemléletet eredményezhet, a függelmi kapcsolatok kizárólagossága kiváltja a „rang" iránti igényeket és személyes függőséget hozhat létre a vezető és a beosztottak között. A rendvédelmi szervezetek részben még ma is leginkább e modell szerint működnek. Ennek a legfőbb oka, hogy *„...a linearitás egyszerű, könnyen áttekinthető belső kapcsolatokat, valamint az alá- és fölérendeltségi viszonyok egyértelműségét jelenti."* [Dobák 46.o.]

## 8. Törzskari szervezetek

Ahogy a tisztán lineáris szervezetnél bemutattam, az ilyen típusú struktúránál a legnagyobb problémát a szervezeti méret növekedése jelenti. A szervezet méretbeli fejlődésének kezdeti szakaszában a folyamatok könnyen átláthatóak, a vezetők a vertikális kommunikációs csatornákon, viszonylag egyszerűen tudják koordinálni a szakmai tevékenységet, illetve el tudják látni a munkáltatói kötelezettségeiket, azonban a szervezet méretbeli növekedésével új kihívásokkal kell szembenézniük. A lineáris szervezet ezen problémája kezelésének legegyszerűbb módjának egy törzskari jellegű szervezet létrehozása mutatkozik. A strukturális típusú koordinációs eszközök elemzésénél már bemutattam a törzskarok működtetésének az előnyeit. Ezeket az előnyös lehetőségeket használja ki a törzskari jellegű szervezet is. A törzskari szervezetek munkamegosztás szempontjából egydimenziósak, a hatáskörmegosztás tekintetében egyvonalas struktúra. Fontos azonban megjegyezni, hogy ez csak a tisztán lineáris struktúra törzskarral történő kiegészítése esetén igaz. A későbbiekben bemutatom a funkcionális szervezetet is, ahol szintén működhet törzskar azonban ezt a szervezeti formát a hatáskörmegosztás tekintetében többvonalas struktúrának kell tekinteni.
A törzskari típusú szervezeti egység létrehozásával a felső vezetés mellett létrehoznak egy úgynevezett törzskart. A törzskar a vezetés munkáját segítő, a felsővezetői döntéseket befolyásoló az egyes szervezeti területek összehangoló tanácsadó jellegű szervezeti egység. A törzskaroknak leginkábba a döntések előkészítésében van a legnagyobb szerepük. Működése révén biztosítható a döntések vezetés szakmai megalapozottsága. A törzsek figyelemmel kísérik a különböző szinteken folyó munkát, ismerik annak minden szakmai jellegű részletét, összetett ismeretrendszerének köszönhetően érvényre juttathatják a többszempontúságot. A hierarchiában elfoglalt sajátos helyzetüknek köszönhetően munkakapcsolatban állnak a szervezet felső vezetéssel, biztosítva ezzel stratégiai elképzelések alsóbb szinteken való megjelenítését, illetve a lehetőségek

közvetítését a felső vezetés felé.[Dobák 53.o.] A törzskar a szervezeti egységeket érintően nem rendelkezik függelmi vagy szakmai irányítási jogkörrel, szándékait csak a szervezet vezetőjén keresztül tudja érvényesíteni. A törzskarok létrehozása tehát az adott szervezet hatásköri és felelősségi rendszerét formálisan nem változtatja meg. Törzskart nem csak a csúcsvezetés szintjén lehet létrehozni, hanem egyéb vezetői szinteken is, azonban ennek előnyei és hátrányai is lehetnek. A törzskari modell előnye, hogy a törzsben képviselt szakterületek komplexitása miatt emelkedik a vezetés szakmai színvonala. A törzs vertikális és horizontális kapcsolatainak köszönhetően, a vezetés támogatást kap, a stratégiai feladatok érvényesítéséhez. Ez hozzájárul a horizontális vezetői szemlélet kialakulásához is. A hatékonyabb információáramlás és a kommunikáció érzékenyebbé és rugalmasabbá teszi azt a modellt a tisztán lineáris modellnél.
Hátránya a struktúrának, hogy az új szervezeti elem belépésével bonyolultabbá válik. A törzskar befolyása utasítási jog nélkül esetleges. További hátránya, hogy nem csökkenti a vezetés terhelését, sőt az információáramlás vezetőn áttételeződő volta miatt a vezetők személyes irányítási feladata növekszik.

## 9. Funkcionális szervezet

A tisztán lineáris típusú struktúra, szervezeti méretének növekedésére a törzskari modell nem mindig jelent megoldást. A szervezet méretbeli fejlődésének kezdeti szakaszában nincs szükség a tevékenységek csoportosítására, a szervezet tagoltságának megváltoztatására, adminisztratív intézkedések növelésére. A szervezet növekedése azonban rákényszeríti a vezetést, hogy a működés hatékonyságának megtartása érdekében változtasson a szervezeti struktúrák jellemzőin. A lineáris modell többféle irányban fejlődött tovább. A koordinációs problémák feloldásának másik útja a funkcionális szervezeti felépítés megjelenése.[50] A vezetés elkülönítette egymástól a homogén szakterületeket melyek irányítását a terület szakértőjére bízta, megteremtve ezzel a funkcionális szervezetek kialakulásának lehetőségét. Ennél a struktúránál egyszerre vannak jelen hierarchikus függelmi kapcsolatok, és szakirányítási kapcsolatok. Éppen azért mert a függelmi kapcsolatok linearitása megmaradt ezt a struktúrát a szakirodalomban[51] gyakran nevezik lineáris-funkcionális szervezeteknek

[50] A témával foglalkozó szakirodalmakban több helyen a funkcionális szervezeti modell szervezeti eleme a törzs is, de az értekezésem jelenlegi szakaszában a tisztán lineáris szervezet törzs nélküli fejlődési irányát mutatom be.

[51] A Nemzeti Közszolgálati Egyetem az Általános közigazgatási ismeretek tananyagában is ezt használja. Dobák Miklós szerit „elméletileg nem teljesen megfelelő” ez a megfogalmazás

A funkcionális struktúra az egyik legrégebbi szervezeti forma. A strukturális jellemzők szerint a funkcionális szervezetek munkamegosztás szempontjából egydimenziósak, az elsődleges munkamegosztás a szervezeti funkciók segítségével történik. A hatáskörmegosztás tekintetében többvonalas struktúra. A döntési jogkörök a tisztán lineáris formánál kevésbé centralizáltak, erőteljes szabályozottság mutatkozik mind a munkamegosztásra, mind a hatáskörükre vonatkozóan. A koordinációt itt is a vertikális koordináció biztosítja, amely elsősorban a hierarchia vonalán épül fel. A stratégiai kérdésekben a hierarchia csúcsán lévő felső vezetés dönt, mivel csak itt állnak rendelkezésre az ehhez szükséges információk. A horizontális koordinációt technokratikus típusú koordinációs eszközök, illetve pótlólagos strukturális eszközök, projektek, teamek, törzskarok és bizottságok biztosítják, amelyek fokozott felsővezetői tevékenységet kívánnak meg. A szakirányítás nem jelent függelmi kapcsolatot, ezzel a szervezet alaptevékenységével összefüggő felelősségvállalás elválik a szakirányítás felelősségétől, mondhatjuk úgy, hogy a szakirányítás szerepe inkább a tanácsadás, szakmai segítségnyújtás, nem pedig a utasítás, rendelkezés. Tehát funkcionálisan szervezeti egységnek szakmai kérdésekben is megmarad döntési kompetenciája és az ehhez rendelt felelőssége. A szervezet alapvető konfliktusforrása, hogy a szakmai irányítás tanácsait, kvázi szakmai döntéseit, a függelmi irányítás felülbírálhatja, amely hatalmi villongásokhoz vezethet, ez esetben a felsővezetőre hárul a döntés felelőssége, elvonva figyelmét a stratégiai irányítástól. A funkcionális szervezeti felépítés elmélete a lineáris struktúra problémáinak kiküszöbölése érdekében jelentősen megváltoztatta a tisztán lineáris struktúra felépítését. Előnye ennek a formulának, hogy kialakul egyértelmű szervezeti specializáció, amelynél megjelenik a szakmailag felkészült vezető és szakmai szervezet, ez egyértelműen növeli a szakszerűséget és a produktivitást, segíti a technikai fejlődést és biztosítja a szakmai fejlődés és karrier a specializált területeken dolgozóknak. Ez a struktúra enyhíti a lineáris struktúra növekedési korlátait, biztosítja a nagyszámú és sokrétű feladat folyamatos végrehajtását, standardizálását, ezáltal csökkenhetnek a koordinációs költségek. A speciális ismeretekkel rendelkező dolgozók alkalmazása erősíti a koordinációt az irányítást és a több szempontú döntések meghozatalát. A centralizált döntéshozatal a jól definiált funkciók révén elősegíti a stabil környezet létrehozását, ami egyszerűbb a stratégiakialakítást tesz lehetővé. A funkcionális munkamegosztás elve szerint munkamegosztás alapján növekedő szervezeti egységek azonban felszínre hozza a struktúra hátrányait. A funkcionális szervezeti egységek nem mindig mutatnak önmérsékletet, hajlamosak a funkciók további szűkítésére, ezáltal a szervezeti elemek növelésére, ami az adminisztratív létszám felduzzadásához, valamint a gazdaságossági szempontok háttérbe szorulásához

vezet. A szervezeti tagoltág fokozásával egy nehezen áttekinthető rendszer jön létre, amely szervezet meglehetősen rugalmatlan, nehezen tud alkalmazkodni a környezeti változásokhoz. A fokozódó diverzifikáltság miatt a szervezeti elemek elszigetelődnek egymástól, a „közös nyelv" hiánya miatt a horizontális kommunikációjuk esetleges, csak informális csatornákon keresztül történik, ez növeli a koordinációs igényeket és a vezetők túlterheltségét, ezért háttérbe szorul a felső vezetés stratégiai szemlélete. Általánosságban elmondható, hogy az funkcionális struktúrákban a szervezet növekedésével, tagoltságának fokozásával, csökken az integráltság foka, a funkcionálisan elkülönült szervezeti egységek elszigetelt szakterületekként működnek.

**10. Divizionális szervezet**

A lineáris, a törzskari és funkcionális szervezetei formáknál, a szervezet méretének növekedésével, a felső vezetés alapvető koordinációs problémákkal találta szembe magát. A szervezet tevékenységi körének növekedése, a tevékenységének fokozása, az összetett folyamatok ellátása, és a szervezet területi, regionális feladat ellátási igénye, vagy kötelezettsége miatti terjeszkedése új kihívásokat jelent. A dinamikusan változó környezet kihívásainak a kritikus méret felett, már nem tudnak hatékonyan megfelelni az ilyen struktúrákat alkalmazó szervezetek. Ezekre a kihívásokra adhat választ a szervezet divizionális struktúrába való átszervezése. A strukturális jellemzők szerint a divizionális szervezetek munkamegosztás szempontjából egydimenziósak, az elsődleges munkamegosztás tárgyi, vagy regionális elv alapján valósul meg, a hatáskörmegosztás szempontjából egyvonalas struktúra. Az irányítási feladatokat a központ látja el. A központ feladat a források elosztása, az egymástól független divíziók működési feltételeinek megteremtése, teljesítményértékelési rendszer kidolgozás és az ellenőrzés. A stratégiai döntések a központban születnek, irányítás elsősorban az elsőszámú vezetőn keresztül érvényesül, de az operatív irányítás joga, a divízióvezetők hatáskörébe tartozik azonban saját divíziójuk eredményessége érdekében stratégiai jellegű döntéseket is hozhatnak. A hatásköri decentralizáció a vertikális koordinációs tevékenységet szűk keretek közé szorítja. Ezért kiemelt jelentőségűvé válnak a divíziók közötti horizontális kapcsolatok. A horizontális koordinációt a strukturális, a technokratikus, és a személyorientált koordináció eszközök is segítik. A feladat- és hatáskörök tisztázásában, strukturális típusú kordinációs eszközként projektek, teamek, törzskarok és bizottságok segítik a koordinációt. A technokratikus eszközök elsősorban a pénzügyi folyamatok koordinálásánál kapnak kiemelt szerepet. A szervezeti struktúra sikerét alapvetően meghatározza divíziók vezetés, ezért

különösen fontos a vezetők személyének a kiválasztása mint a személyorientált koordinációs eszközök egyik megjelenési formája. A központi egységek a pénzügyi, a controlling, kutatás-fejlesztés, marketing, illetve humánpolitikai feladatokat ellátó egységek vagy személyek, ezek mellett a vezetés támogatása érdekében döntéstámogató egységeket is kialakítanak, amelyek lehetnek stratégiai, igazgatási, jogi, ellenőrzési, szervezetfejlesztési és egyéb szükséges elemek. Ezeket általában kiegészíti egy központi szolgáltatói egység, amely tartalmazza többek között az informatikai, az oktatási, logisztikai, és egyéb igény szerinti egységeket. A divíziók működését a szervezeten belül nagyfokú függetlenség jellemzi, a megfelelő színvonalú működést saját irányító és végrehajtó apparátusukkal biztosítják, melyet a funkció szerint munkamegosztás elve szerit alakítanak ki. Az operatív döntések szintje a divízió, melynek következtében a stratégiai és az operatív irányítás elválik egymástól, azonban a divíziók a szakterületük vonatkozásában stratégiai döntéseket is hozhatnak. A divíziókon belül a funkcióik alapján elkülönülő hierarchikus egységek vannak, melyek lineáris jellegű függelmi kapcsolatban állnak a divízió vezetőjével, tehát divízióvezető közvetlen alárendeltségében vannak. Az ilyen struktúrának az előnye hogy a fentiek szerint szétválnak a stratégiai és az operatív feladatok, ez egyrészt tehermentesíti a vezetést, másrészt erősíti a stratégiai és az operatív kontrollt.
A divíziók viszonylagos önállósága, elősegíti a vezetők általános fejlődését, fokozza a motivációjukat, egyszerűbbé teszi a belső kommunikációt, lehetőséget ad a gyors döntések meghozatalára, amely fokozza a hatékonyságot. Az egymástól független divíziók elősegítik a világos célmeghatározást, a szervezeti célokkal való azonosulást, a felelősségi rendszer kialakulását. Elősegíti a környezeti igényekhez, illetve változásokhoz, való alkalmazkodást, kivédi annak negatív hatását úgy, hogy a változások hatása közvetlenül nem az egész szervezetet, hanem csak az egyes divíziókat érinti. A struktúra hátránya, hogy a divíziók önálló apparátusainak működtetése növeli a különféle duplikációk következtében fellépő költségeket. Az viszonylag önálló divízióvezetők egoizmusának megnyilvánulása esetén a divíziócélok a szervezet céljai elé kerülhetnek, egészségtelen rivalizálás alakulhat ki a divíziók között. A decentralizáció miatt szervezeten belül csökken a vezetés komplex látásmódja ugyanakkor a divízión belüli hatásköri centralizáció fokozódása miatt funkcionális szervezte problémái divízió szinten újratermelődhetnek.

**11. Mátrixszervezet**

A funkcionális és a divizionális szervezeti formák nehezen alkalmazkodnak azokhoz a környezeti változásokhoz „…amelyek a szervezettől acélok és stratégiák

folyamatos módosítását, finomítását, valamint a vezetési-szervezeti struktúra rugalmasságát igénylik."[Dobák 88.o.] Ezekre a kihívásokra adnak egyfajta megoldást a mátrixszervezetek. A mátrixszervezetekben az elsődleges munkamegosztás szintjén egyszerre két munkamegosztási elvet alkalmaznak. Jellemzően a funkcionális munkamegosztást kombinálják a tárgyi, vagy regionális megosztással. Ezért a strukturális jellemzők szerint a mátrixszervezetek többdimenziós szervezetek, a hatáskörmegosztás szempontjából többvonalas irányítás érvényesül. A kettős szemléletű munkamegosztás miatt a mátrixszervezet struktúrájában kettős irányítás jön létre. Amennyiben a legáltalánosabb mátrixszervezetet a funkcionális-tárgyi ezen belül is a termékorientált szervezetet vizsgáljuk azt tapasztaljuk, hogy a funkcionális vezetők a szervezet teljes tevékenységi körében gondolkodnak míg a tárgyi, vagy termék elven kialakított szervezeti egység vezetői a termékkel kapcsolatos komplex tevékenységet állítják a feladatrendszerük középpontjába. Így alakul ki a szervezeten belüli a vertikális és a horizontális szemléletű irányítás. Tehát az egyes termékekkel kapcsolatos feladatrendszerek végrehajtásához szükséges döntéseket két azonos döntési- és felelősségi jogkörrel rendelkező vezető együttesen hozza meg. A vertikális és horizontális irányú döntési kompetenciák érvényesítésénél elkerülhetetlen a konfliktusok keletkezése, azonban ezek kezelésére a kompetenciák azonos súlya ad garanciát. Ezek alapján elmondhatjuk, hogy e struktúra koordinációját sok tekintetben maga az alapstruktúra biztosítja, hiszen a vertikális, illetve a horizontális irányítás döntéshozóinak, adott esetben eltérő érdekei ellenére is, kompromisszumos döntést kell hozniuk minden fontosabb kérdésben. Tehát a strukturális koordinációs eszközök hátérbe szorulnak.

A szabályozottság, a keretek pontos meghatározása, a folyamatok összefüggéseinek láthatóvá tétele a technokratikus koordinációs eszközökkel teremthetők meg. A konfliktusok megelőzése, megfelelő kezelése a mátrixszervezet hatékony működésének alapját jelenti, ezért kiemelten fontos a megfelelő vezető személyének kiválasztása és szervezeti koordináció erősítése, amely a személyorientált koordinációs eszközök fokozott igénybevételét jelenti. A mátrix szervezet előnye, hogy a feladatok eltérő nézőpontú, komplex meg közelítése garantálja a szervezet rugalmasságát, alkalmazkodóképességét. A feladatok végrehajtása során a vezetők egymásrautaltsága nyilvánvaló, ezért egy teljesen új vezetési kultúra alakul ki, ez versenyhelyzetet teremthet a probléma megoldásban, növeli a teljesítményt és emeli a motiváltság szintjét. A struktúra megköveteli a széleskörű felkészültséget, elősegíti a szervezeti befogadóképességét a növeli a vállalat innovatív képességét. Az elsődleges munkamegosztás különböző elveinek egyenlő súlyú figyelembevétele a hierarchia összezsugorodását eredményezi, ami

koordináció hatékonyságának növelését jelenti. A struktúra hátránya, hogy „intézményesíti a konfliktusokat" [Dobák 85.o.] ezek a konfliktusok bizonytalanságot eredményezhetnek, nehezíthetik az irányítást, ami valódi krízishelyzetet idézhet elő. A kettős irányítás kialakulása miatt megjelenik a vezetők rivalizálása, a döntéstől, a felelősségvállalástól való tartózkodás, amely különösen krízishelyzetben jelent veszélyt.
Szintén a szervezet kétdimenziós jellegéből adódik a túlhajtott csoportmunka, ami gátolhatja a gyors reakciót igénylő döntések meghozatalát.

**Összegzés**

Jelen cikk bemutatta a szerző PhD értekezésének egy részét, amely a szervezetek alapvető struktúráit mutatja be.

**Felhasznált irodalom**

A lábjegyzetekben, valamint:
[1] Négyesi Imre: Az Információ szerepe a Katonai-Vezetői Információs Rendszerekben (Hadtudományi Szemle on-line, II. évfolyam (2009) 1. szám, 119-125. oldal, HU ISSN 2060-0437)

***Dorkó Zsolt[52]: A NAV szervezete-II.***

**Absztrakt**
*A cikk bemutatja a PhD jelölt értekezésének egy részét.*

**Abstract**
*The article presents parts of thesis PhD candidate's.*

## 1. Bevezetés

Az előző számban megkezdett publikációm második részét ismertetem, amely a speciális rendészeti szerv felépítését és rendeltetését veszi számon.

## 2. Bűnügyi Főigazgatóság

A hatékony és eredményes bűnüldözési munka megvalósulása érdekében a NAV szervezeti struktúrájában önálló elemként jelenik meg a nyomozó hatóság. A törvény szerint[53] a NAV nyomozó hatósága a bűnügyi főigazgatóság és annak középfokú szervei.

## 3. Vezetés

A NAV Bűnügyi Főigazgatósága (továbbiakban, NAV BF) önálló jogi személyiség. A NAV vezetésének bemutatásánál ismertettem, hogy a főigazgatóságot az elnök által kinevezett főigazgató vezeti. Az elnök a NAV BF SZMSZ[54] szerint Bűnügyi Főigazgatóság felett szervezetirányítási és felügyeleti jogkörét közvetlenül vagy közvetve a Központi Hivatalon keresztül, a szakmai felügyeleti jogkörét a bűnügyi elnökhelyettes útján gyakorolja. A Központi Hivatal Bűnügyi Főosztály felügyeletet gyakorol a NAV BF és szervei szakmai tevékenysége felett. A bűnügyi főigazgatóság középfokú szerveit (regionális bűnügyi igazgatóságok) a főigazgató javaslatára az elnök által kinevezett igazgató vezeti az igazgatóhelyettesek közreműködésével. A főigazgatóság alsó fokú szervét (NAV Áru- és Bűnjelkezelő Hivatala) a főigazgató által kinevezett hivatalvezető vezeti.

---

[52] Heves Megyei Rendőr-főkapitányság osztályvezető
[53] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról 4. § (3)
[54] 1/2013. (II.22.) NAV utasítása a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóságának Szervezeti és Működési Szabályzatáról 2. § (2)

## 4. Gazdálkodás

A NAV BF a költségvetési szervek gazdálkodási besorolása szerint önállóan működő és gazdálkodó költségvetési szerv, amely a NAV költségvetési fejezetet önálló címet képez.[55] A NAV BF gazdálkodásban irányadó előírások természetesen a fejezetnél már kifejtett normákkal megegyezőek.

## 5. Szervezet

A Bűnügyi Főigazgatóság a NAV központi szerve. A NAV BF középfokú szervekkel és alsó fokú szervvel rendelkezik, melyek területi szervek. Középfokú szervei regionális bűnügyi igazgatóságok, alsó fokú szerve a NAV Áru- és Bűnjelkezelő Hivatala. A bűnügyi főigazgató a bűnügyi főigazgató-helyettes és az erőforrásokért felelős főigazgató-helyettes közreműködésével vezeti a főigazgatóságot. Közvetlenül irányítja a Főigazgatói Törzs, az Informatikai Főosztály és a Jogi, Igazgatási és Titkársági Főosztály tevékenységét. A törzs a bűnügyi főigazgató közvetlen irányítása és felügyelete alatt látja a feladatát melynek fő célja a bűnügyi főigazgató elsődlegesen koordinációs tevékenységének segítése. A törzs keretében működik a főigazgatói informatikai tanácsadó, a bűnüldözési belső adatvédelmi felelős, a bűnüldözési informatikai biztonsági referens a belső ellenőrzés, a Helyi Biztonsági Felügyelet és a biztonsági referens. A bűnügyi főigazgató-helyettes irányítja és felügyeli az alatt álló a Bűnügyi Koordinációs Főosztály, a Központi Nyomozó Főosztály, a Bűnügyi Ellátó Főosztály, és a Revizori Főosztály munkáját. Az erőforrásokért felelős főigazgató-helyettes közvetlenül vezeti a Pénzügyi és Gazdasági Főosztály és a Humánpolitikai Főosztály munkáját, és gazdasági vezetőként felelős a gazdasági szervezet jogszabályoknak megfelelő működéséért. A regionális bűnügyi igazgatóságot egyszemélyi felelős vezetőként az igazgató az Áru- és Bűnjelkezelő Hivatala főosztályvezetői besorolású hivatalvezető vezeti a hivatalvezető-helyettes közreműködésével.

A Bűnügyi Főigazgatóság mint központi szerv szervezeti egységei:

Informatikai Főosztály
Pénzügyi és Gazdasági Főosztály

[55] 1/2013. (II.22.) NAV utasítása a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóságának Szervezeti és Működési Szabályzatáról 4. § (1-2)

Humánpolitikai Főosztály
Jogi, Igazgatási és Titkársági Főosztály
Főigazgatói Törzs

A Bűnügyi Főigazgatóság középfokú szervei:

NAV Közép-magyarországi Regionális Bűnügyi Igazgatósága;
NAV Észak-magyarországi Regionális Bűnügyi Igazgatósága;
NAV Észak-alföldi Regionális Bűnügyi Igazgatósága;
NAV Dél-alföldi Regionális Bűnügyi Igazgatósága;
NAV Nyugat-dunántúli Regionális Bűnügyi Igazgatósága;
NAV Közép-dunántúli Regionális Bűnügyi Igazgatósága;
NAV Dél-dunántúli Regionális Bűnügyi Igazgatósága.

A NAV BF alsó fokú szerve

NAV Áru- és Bűnjelkezelő Hivatala

## 6. Feladata

A törvény [56] szerint a NAV bűnügyi főigazgatósága és regionális bűnügyi igazgatóságai feladata a büntetőeljárásról szóló törvény [57] által a NAV nyomozóhatóságainak hatáskörébe utalt bűncselekmények elkövetésének megelőzése, felderítése, megszakítása, az elkövető kilétének megállapítása, elfogása, tartózkodási helyének megállapítása, a bizonyítékok megszerzése. Feladatának sikeres ellátása valamint az eljárásban résztvevők védelmének érdekében a nyomozó hatóságnak lehetősége van a törvényben meghatározott keretek közötti titkos információgyűjtésre. A törvény lehetőséget biztosít arra, hogy a nyomozóhatóság az információt szolgáltató kisebb súlyú bűncselekmények elkövetőjével kapcsolatban a feljelentés elutasítását vagy a nyomozás megszüntetését kilátásba helyezze, ha az ezzel elérhető bűnüldözési célhoz fűződő érdek jelentősebb, mint a kisebb súlyú bűncselekmény elkövetőjével szemben fennálló állami büntetőjogi igény érvényesítéséhez fűződő érdek. A regionális bűnügyi igazgatóságok saját ügyrendjükben megfogalmazott szabályok alapján hatáskörükben végzik a kormányrendeletben [58] meghatározott kivétellel a büntetőeljárásról szóló törvényben meghatározott bűncselekmények megelőzését, felderítését, valamint nyomozását az erre vonatkozó jogszabályok rendelkezései szerint. Áru- és Bűnjelkezelő Hivatal feladata végzi a NAV vámigazgatási-, jövedéki

[56] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról 13. § (7)
[57] 1998. évi XIX. törvény a büntetőeljárásról
[58] 273/2010. (XII. 9.) 33.§ Korm. Rendelet a Nemzeti Adó- és Vámhivatal szervezetéről és egyes szervek kijelöléséről

igazgatási, fémkereskedelmi, szabálysértési és nyomozóhatósági jogkörében eljárva a NAV rendelkezése alá került dolgok kezelésével, valamint az elkobzott árukkal kapcsolatos, jogszabályban meghatározott feladatokat.

## 7. Informatikai támogatás

**Informatikai Főosztály**

Az Informatikai Főosztály a főigazgató közvetlen irányítása alatt végzi tevékenységét. Feladatait az Üzemeltetési Osztály és az Alkalmazás- Támogató Osztály segítségével látja el. A főosztály az utasításban[59] megfogalmazottak szerint felügyeli és ellenőrzi a bűnügyi szakterület informatikai rendszereit, valamint ellátja a szakterület informatikai tevékenységének felügyeletét. Közreműködik az informatikai tárgyú szabványok, eljárási rendek előkészítésében, a szakterület informatikai stratégia tervezetének kidolgozásával a NAV informatikai stratégiájának elkészítésében. Javaslatot tesz a közigazgatásban bevezetett informatikai módszerek alkalmazására. Biztosítja a szakterület informatikai tevékenységének szabványosítást, elvégzi az ellenőrzési tevékenységet megalapozó kockázatelemzési feladatokat az informatikai cél-és témavizsgálatait. Közreműködik a bűnügyi informatikai rendszerekhez kapcsolódó együttműködési megállapodások kialakításában az adatvédelemmel, informatikai biztonsággal kapcsolatos irányító eszköz kialakításában mind a NAV, mind a NAV BF tekintetében. Feladatkörében együttműködik a társszervek és a NAV informatikai szakterületeivel, valamint a bűnügyi szakterülettel. Szervezi a főosztály foglalkoztatottjainak szakmai oktatását, a bűnügyi szakterület felhasználóinak informatikai továbbképzését.

**Főigazgatói Törzs informatikai feladatai**

Főigazgatói Törzs a bűnügyi főigazgató munkájának segítése érdekében létrehozott funkcionálisan kialakított szervezet. A szervezet előnye, hogy a főigazgató közvetlen felügyelete és irányítása alatt nagyfokú, több területet is lefedő szakmai hozzáértés koncentrálódik. Ez lehetőséget ad a részfolyamatok teljesebb koordinációjára, a többszempontúság érvényesülésére. Mivel tagjai állandó kapcsolatban vannak a főigazgatóval, eredményesen közvetíthetik a vezetői elképzeléseket illetve a rendelkezésre álló lehetőségeket. A Törzs keretében a főigazgató informatikai szakterülethez kapcsolódó feladataiban, döntéseinek előkészítésében elsősorban a főigazgatói informatikai tanácsadó valamint a

[59] 5. függelék az 1/2013. (II.22.) NAV utasítás mellékletéhez

bűnüldözési informatikai biztonsági referens nyújt segítséget, de a törzs többi szervezeti elemének is van az informatikai szakterülethez köthető részfeladata.

**A főigazgatói informatikai tanácsadó**

A főigazgatói informatikai tanácsadó feladatait az utasítás[60] szerint a bűnügyi főigazgató közvetlen irányítása és felügyelete alatt a Főigazgatói Törzs szervezetén belül látja el. A főigazgató határozatlan időtartamra bízza meg az informatikai tanácsadót. Feladatkörében koordinálja a bűnügyi szakterület informatikai feladatait, a minősített adatok kezeléséhez kapcsolódóan az elektronikai rendszerbiztonság körébe tartozó informatikai feladatokat, valamint a bűnüldözési informatikai biztonsági referens és az Informatikai Főosztály feladatellátását. Ellátja az Informatikai Főosztály felügyeletét. Részt vesz az informatikai szakterület fejlesztési rendjének kidolgozásában, biztosítja az informatikai és szakmai egyeztetések lefolytatását. A főigazgató egyedi ügyekben adott felhatalmazása esetén utasítási jogkörrel rendelkezik feladatellátása körében.

**A bűnüldözési informatikai biztonsági referens**

A főigazgatói bűnüldözési informatikai biztonsági referense feladatait a bűnügyi főigazgató közvetlen irányítása és felügyelete alatt a Főigazgatói Törzs szervezetén belül látja el. A főigazgató határozatlan időtartamra bízza meg az bűnüldözési informatikai biztonsági referenst, aki felelős a bűnügyi szakterület minősített adatot nem kezelő informatikai rendszereinek fejlesztésével, működésével kapcsolatos informatikai biztonságot érintő koordinációs feladatok elvégzéséért. A utasítás[61] szerint az informatikai biztonság megvalósulása érdekében meghatározza a szakterület vonatkozásában az informatikai biztonsági elveket, célokat, feladatokat, előkészíti az ehhez kapcsolódó irányító eszközöket és figyelemmel kíséri azok alkalmazását. A bűnügyi szakterületen koordinálja az informatikai biztonsági tevékenységét, tervezi és végrehajtja az ezzel kapcsolatos ellenőrzéseket, meghatározza a prioritásokat, segítséget nyújt a szervezeti egységeknek az informatikai biztonsági követelmények meghatározásában. Közreműködik a bűnügyi szakterület vonatkozásában az adatvagyon kialakításával, kezelésével kapcsolatos feladatokban, a működésfolytonossággal és informatikai katasztrófa-elhárítással kapcsolatos feladatokban, végzi a szakterület tekintetében az informatikai kockázatelemzéssel kapcsolatos feladatokat. Feladatainak ellátása

[60] 1/2013. (II.22.) NAV utasítása a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóságának Szervezeti és Működési Szabályzatáról 46. §

[61] 1/2013. (II.22.) NAV utasítása a Nemzeti Adó- és Vámhivatal Bűnügyi Főigazgatóságának Szervezeti és Működési Szabályzatáról 51. §

során együttműködik a NAV BF és az irányítása alá tartozó szervek vezetőivel és a kiemelt felhasználókkal, a főigazgatói informatikai tanácsadóval, biztonsági vezetővel, az informatikai szakterülettel, valamint a bűnüldözési belső adatvédelmi felelőssel. Összehangolja a NAV BF és az irányítása alá tartozó szervek foglalkoztatottjainak informatikai biztonsági kérdéseket érintő, oktatását.

**Összegzés**

Az APEHés a VP összevonásával létrejött NAV az állam adóhatósági és vámhatósági feladatainak, hatékonyabb, átláthatóbb és költségtakarékosabb ellátása, és az ehhez szükséges információtechnológiai és műszaki háttér elvi megújulásának biztosítása, a központi költségvetés bevételi előirányzatainak nagyobb hatásfokú teljesítése, valamint az államháztartási érdekek hatékonyabb érvényesítése tette szükségessé.

**Felhasznált irodalom**

A lábjegyzetekben találhatók.

***Dorkó Zsolt-Bozsó Zoltán-Pándi Erik[62]: A rendőrségi ügyeleti szolgálatok***

**Absztrakt**
*A cikk bemutatja az újonnan kialakított rendőrségi ügyeleti szolgálatokat és feladataikat.*

**Abstract**
*This article presents missions and organizations of police's duty offices.*

## 1. Bevezetés

Hazánk geo- és biztonságpolitikai helyzetében közel két évtizeddel ezelőtt elkezdődött változások lényegében az elmúlt tíz esztendő során csúcsosodtak ki, amely időszakban országunk két – *a kontingens államalakulatai szempontjából meghatározó* – szövetségi rendszer tagjává vált. Az egykori fegyveres erők szerepe és dominanciája is megváltozott, így amíg az egyik részének feladatrendszere a rendészet irányába szélesedett, addig a másiké az ország fegyveres védelme, illetve a koalíciós keretek között folytatott *háborús* és *nem háborús* katonai műveletek területén bővült [1].
A rendszerek teljes kiforrottságában azonban tapasztalhatók némi hiányosságok, hiszen az a körülmény, amely szerint az EBESZ, ENSZ, EU, NATO[63] és más nemzetközi békefenntartó erőknek a válságövezetekben kifejtett tevékenysége során a katonai és rendőri működés közeledett és közeledik egymáshoz, azt a magyarországi múltban gyökerező hitet erősíti – *talán még napjainkban is* -, hogy a rend védelmében a rendőrséget hadseregként, a katonaságot pedig rendőrségként lehet működtetni [2].

## 2. Jogszabályi környezet és az ügyeleti szolgálatok felosztása

Magyarország Rendőrségének (a továbbiakban: Rendőrség) legújabb kori feladatait[64] a rendőrségről szóló 1994. évi XXXIV. törvény alapjaiban határozza meg. A jogszabály 1. § (1) bekezdése világosan megfogalmazza, hogy „*A Magyar*

[62] Heves Megyei Rendőr-főkapitányság osztályvezető, Gödöllő rendőrkapitánya, NKE HHK főiskolai tanár.
[63] EBESZ: Európai Biztonsági Szervezet; ENSZ: Egyesült Nemzetek Szervezete; EU: Európai Unió; NATO: North-Atlantic Treaty Organization, magyarul: Észak-atlanti Szerződés Szervezete.
[64] A Rendőrség feladatrendszere legutóbb 2010-ben változott meg jelentősebben.

*Köztársaság Rendőrségének […] feladata a közbiztonság és a közrend védelme, az államhatár őrzése, a határforgalom ellenőrzése, az államhatár rendjének fenntartása, a terrorizmus elleni küzdelem és az e törvényben meghatározott bűnmegelőzési, bűnfelderítési célú ellenőrzés."* [3]. A vonatkozó jogszabály alapján, a Rendőrség előzőekben részletezett tevékenységét:
- az általános rendőrségi feladatok ellátására létrehozott szerv;[65]
- a belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerv;[66]
- a terrorizmust elhárító szerv keretében látja el.[67]

A Rendőrség egyik alapvető feladata tehát a közbiztonság és a közrend (belső rend) védelme. A Rendőrség e feladatrendszerét a jelzett törvényben, valamint törvény felhatalmazása alapján más jogszabályban meghatározott bűnmegelőzési, bűnüldözési, államigazgatási és rendészeti feladatkörében látja el békeállapot, rendkívüli állapot, szükségállapot és veszélyhelyzet esetén.[68]

### 3. A Rendőrség feladatának ellátása során

- együttműködik az állami és a helyi önkormányzati szervekkel, a társadalmi és a gazdálkodó szervezetekkel, az állampolgárokkal és azok közösségeivel;
- segítséget nyújt jogszabályban meghatározott esetben az állami és a helyi önkormányzati szervek hivatalos eljárásának zavartalan lefolytatásához;
- támogatja a helyi önkormányzatoknak és az állampolgárok közösségeinek a közbiztonság megjavítására irányuló önkéntes tevékenységét.

A Rendőrség tevékenysége vezetés-irányításában az egyszemélyi parancsnoki vezetés mellett az ügyeleti szolgálatoknak is rendkívüli jelentősége van. A szolgálatok sokrétű tevékenységet végeznek a különböző jogszabályok, a közjogi szervezetszabályozó eszközök (rendelkezések, belső normák) alapján, amelyeket a mellékletben soroltam fel. Szinte valamennyi intézkedési nemhez kapcsolódik jogkövetkezményekkel járó hatás mind a Rendőrség, mind pedig az állampolgárok tekintetében.

---

[65] A Rendőrség „hagyományos" szervei, pl.: ORFK, megyei rendőr-főkapitányságok, rendőrkapitányságok, határrendészeti kirendeltségek.
[66] Nemzeti Védelmi Szolgálat (NVSZ).
[67] Terrorelhárítási Központ (TEK). Mindhárom típusú szervet a belügyminiszter irányítja.
[68] Ilyen jellegű közjogi szervezetszabályozó eszköz a Belügyminisztérium és szervei készenlétbe helyezéséről, minősített időszaki működésének szabályairól, valamint személyi állományának értesítéséről szóló 11/2011. (V. 6.) BM utasítás, valamint az általános rendőrségi feladatok ellátására létrehozott szerv készenlétbe helyezéséről, minősített időszaki működésének szabályairól, valamint személyi állományának értesítéséről szóló 12/2011. (VIII. 19.) ORFK utasítás.

Valamennyi szolgálati ágra, szakterületre vonatkozó normaismeret – *és ezt feltételező lexikális tudás* – természetszerűleg nem várható el az ügyeleti szolgálatot teljesítő rendőrtől és ilyen jellegű követelményt vele szemben támasztani nem is lehet. A rendőri szervekhez forduló, segítséget remélő személyt (állampolgárt) azonban az ügyeletes köteles a fennálló jogszabályok keretein belül felvilágosítani, részére a szükséges támogatást biztosítani. Ugyanakkor az intézkedések tekintetében is fokozott elvárás mutatkozik meg az ügyeletessel szemben, figyelemmel arra is, hogy hivatali munkaidőn túl többnyire a hatóság vezetőjének jogkörében kell eljárnia, szakszerű, másra át nem ruházható döntéseket kell hoznia [4].

E szolgálat – *működési területén* – az igényekhez igazodva irányítója, szükség szerint aktív közreműködésével részese is az emberi élet, az anyagi javak mentésének. Kiemelkedően fontos eszköze a katasztrófahelyzet, jelentős anyagi kár elhárításának, a közrend, közbiztonság fenntartásának, esetleges helyreállításának, adott esetben országunk szuverenitása védelmének is.

Általában az ügyeletek személyzete teszi meg az elsődleges intézkedéseket a bejelentések, feljelentések esetében, valamint különféle rendkívüli események bekövetkezése, szabálysértések, bűncselekmények elkövetése esetén. Az ügyeletes rendelkezik az állomány átcsoportosíthatóságának lehetőségével, kapcsolatot tart a társszervekkel, tájékoztatást ad az ügyfeleknek, külső szerveknek és jelentés tesz elöljáróinak.

Több helyi szervnél az ügyeletes egyúttal szolgálatparancsnoki feladatokat is ellát, így ő igazítja el és számoltatja be a szolgálatos állományt. Ellátja a riasztással, kiértesítésekkel kapcsolatos feladatokat és eleget tesz ellenőrzési (fogda, objektum, fegyver, stb.) kötelezettségének is. Mindezen feladatai ellátásához nélkülözhetetlen a modern híradó és informatikai (elektronikus, infokommunikációs) eszközök készségszintű ismerete is [5]. Megállapítható, hogy az ügyeleti szakterület sokrétű, a rendőri munka folyamatosságának biztosítása során valamennyi szolgálati ág tevékenységét koordinálja, ahhoz segítséget nyújt, irányítja azokat.

Az ügyeleti szolgálatok megítélése az utóbbi években felértékelődött és a Határőrség - Rendőrség integrációját követően is folyamatos átalakulás alatt áll, a folyamatok valamennyi rendőri szervnél az egységes és hatékony bevetés-irányítási ügyeletek létrehozásának irányába hatnak. A rendőri tevékenység együttműködő szervek, valamint állampolgárok részéről történő pozitív megítélésében, a szakszerű intézkedések végrehajtásában és a vezetői elvárások érvényesítésében – *feladat meghatározással, motivációval* – az ügyeleteknek vitathatatlan szerepe van, mely folyamatosan (napra készen) képzett szakembereket igényel. Ahhoz, hogy a fent vázolt célok érvényesüljenek, olyan – *valamennyi rendőri szervre egységesen*

*vonatkozó* – ajánlásokat kell megfogalmazni, amelyek – *figyelembe véve egy-egy terület specialitásait is* – kellő útmutatásokat adnak az ügyeleti szolgálatot ellátók számára [6].
Az ügyeleti szolgálatokat ellátók legfőbb feladatait a vonatkozó törvények, illetőleg jogszabályok mellett a Rendőrség ügyeleti szolgálata és a közreműködésével teljesítendő jelentési és tájékoztatási kötelezettség ideiglenes szabályozásáról szóló 41/2010. (OT 23.) ORFK utasítás szabályozza.

## 4. A Rendőrség szervezete

A bűnmegelőzési, bűnüldözési, államigazgatási, rendészeti, határrendészeti és terrorelhárítási feladatok – *az előzőekben említettek alapján* – három szerv keretében kerül végrehajtásra. Az általános célú feladatok végrehajtásának legfelsőbb (központi) szerve az Országos Rendőr-főkapitányság (ORFK). A Rendőrség területi szervei:
- az ORFK közvetlen alárendeltségében működő rendőr-főkapitányságok;
- Készenléti Rendőrség (regionális bevetési és egyéb speciális alegységeivel[69]);
- Repülőtéri Rendőr Igazgatóság;
- Bűnügyi Szakértő és Kutató Intézet;
- Oktatási Igazgatóság.

A Rendőrség helyi szervei a rendőr-főkapitányságok önálló feladatkörrel felruházott szerveként működő rendőrkapitányságok, valamint határrendészeti kirendeltségek. A rendőr-főkapitányság és a rendőrkapitányság szervezetében rendőrőrs [70] szervezhető.
A speciális célú szolgálatok, úgymint Nemzeti Védelmi Szolgálat, valamint Terrorelhárítási Központ központi és területi (alapvetően: regionális) szervekkel rendelkezik.
Az **általános célú rendőri szervek** ügyeleti szolgálatait vizsgálva kijelenthető, hogy ezek biztosítják a leginkább érdekelt intézmények, hivatalok, szervezetek munkavégzésének, akcióképességének folyamatosságát. Puszta létezésük jó hatással van a társadalom közérzetére, a köznyugalom pozitív irányú befolyásolására, mindezekkel összefüggésben különösen a bajbajutott, valamilyen kárt, támadást, zaklatást elszenvedő állampolgárok biztonságérzetére. Az ügyeleti

[69] Speciális szolgálatok, például: Állami Futárszolgálat, Légirendészeti Parancsnokság, Pénzkísérő Szolgálat, stb.
[70] Osztály, vagy alosztály jogállású.

szolgálatok végeredményben lakossági igényre jöttek létre, a lakosságot szolgálják a vezetés-irányítás folyamatosságának biztosítása révén.
Természetesen az úgynevezett ügyelet nem csupán a már vázolt területeken működhet és működik. Ahol a lakossági igény, vagy a szolgáltatás jellege megkívánja, a hivatali munkaidő-rendszeren túl is működtetnek különböző intézményeket, szolgáltatásokat. Az természetes, hogy állandó ügyelet működik különböző közszolgáltatásokat biztosító szerveknél, úgymint mentőszolgálatok, vagy tömegközlekedési szervezeteknél. Előfordulhat, hogy egyes rendkívüli események kormányzati szintű beavatkozást is igényelhetnek. A kiemelkedően súlyos, rendkívüli eseményekben a kormányzati szinten szükséges intézkedések irányítását a kormányügyeletes végzi.

## 5. Állami ügyeleti rendszer

Az állami ügyeleti rendszerről korábban kormányzati szintű határozatok rendelkeztek, amelyeket közel tíz esztendeje hatályon kívül helyezték, ezért az állami ügyeleti rendszer a vonatkozó kormányhatározat alapján lényegében megszűnt, a feladatok ellátására új intézményformákat nem hoztak létre.

### A Belügyminisztérium ügyeleti rendszere

Az ügyeleti szolgálat szervezésének célja a minisztérium, a minisztériumi szervek, valamint az önálló belügyi szervek[71] folyamatos működésének elősegítése, az együttműködő szervek, valamint az egymás közötti információs kapcsolat állandó fenntartása; a rendkívüli eseményekkel összefüggő szükséges és halaszthatatlan intézkedések megtétele; az intézkedésre jogosult és köteles szervek, személyek értesítése; a vezetők tájékoztatása.
A minisztérium ügyeleti szolgálatát a Miniszteri kabinet szervezetében működő BM Ügyelet – *Ügyeleti Osztály* – látja el. Az ügyelet munkarendje szerint a minisztériumi szervek és az önálló szervek ügyeleteitől érkező tájékoztatás alapján a rendkívüli eseményekről jelentést tesz, azokról BM Tájékoztató Jelentés címen összefoglalót készít és azokat a kabinetfőnök által jóváhagyott elosztónak megfelelően továbbítja. Az állandó ügyeleti szolgálaton túl a minisztériumban munkaszüneti és heti pihenőnapokon a miniszter által megbízott vezetők vezetői ügyeleti szolgálatot teljesítenek. Feladatuk a kiemelt rendkívüli eseményekkel kapcsolatos halaszthatatlan intézkedések megtételének elősegítése. Az ügyelet vezetője jelentéstételi kötelezettséggel tartozik

[71] A rendőri szerveken túl, például Alkotmányvédelmi Hivatal, büntetés-végrehajtás, Bevándorlási és Állampolgársági Hivatal, stb.

- a miniszternek,
- a feladatkör szerint illetékes minisztériumi felső vezetőnek,

**A Rendőrség ügyeleti rendszere**

A szolgálati feladatok maradéktalan végrehajtása érdekében állandó ügyeleti szolgálatot kell működtetni:

*a)* az Országos Rendőr-főkapitányságon (a továbbiakban: ORFK);
*b)* a Készenléti Rendőrségnél (a továbbiakban: KR);
*c)* a Repülőtéri Rendőr Igazgatóságon (a továbbiakban: RRI);
*d)* a megyei (fővárosi) rendőr-főkapitányságokon;
*e)* a rendőrkapitányságokon;
*f)* a határrendészeti kirendeltségeken;
*g)* a közös kapcsolattartási szolgálati helyeken és a rendészeti együttműködési központon;
*h)* az őrzött szállásokon;
*i)* az egyéb rendőri szerveknél, ahol azt az illetékes vezető elrendeli.

A megyei rendőr-főkapitányságok és a megyeszékhelyi rendőrkapitányságok ügyeleteit a szerv vezetője által meghatározott elhelyezéssel összevontan kell működtetni. Az összevont ügyelet, illetve az oda beosztott ügyeletesek feladatkörét a szerv vezetőjének egyértelműen meg kell határoznia. Azoknál a megyei rendőr-főkapitányságoknál, ahol az ügyeletek összevonása gazdasági, vagy más egyéb indokolt okból nem lehetséges, az összevonástól külön elbírálás alapján el lehet tekinteni. A külön elbírálás alapja az illetékes megyei rendőr-főkapitányság vezetőjének megfelelően alátámasztott kérelme az ORFK Rendészeti Főigazgatóság vezetője részére, aki arról egyéni elbírálás alapján dönt. Elbírált kérelmek esetén ismételt kérelmet nem kell benyújtani.
Az ügyeleti szolgálatot ellátó (ügyeletes) a hivatali munkaidőn kívül, külön rendelkezésben meghatározott körben, a szerv vezetőjének jogkörét gyakorolja. Az ügyeletes részére biztosítani kell azokat az eszközöket, amelyek a feladat zavartalan ellátásához és a hatáskörébe utalt intézkedések megtételéhez szükségesek. Az ügyeletest feladatának teljesítésétől elvonni, más feladatra igénybe venni nem szabad.

## 6. Az ügyeleti szolgálati formák

**Állandó ügyeletnek** minősül a rendőri munka folyamatosságát biztosító, a jelentési kötelezettség rendjét teljesítő, a rendkívüli eseményekkel összefüggésben az

elsődleges intézkedések megtétele érdekében intézkedő szolgálat. Állandó ügyeleti szolgálatot kell szervezni a fentiekben megjelölt szerveknél, amelyet a szervek vezetői a szerv állománytáblája szerint rendszeresített státusszal és a hozzá rendelt létszámmal alakítanak ki. Törekedni kell arra, hogy az ügyeleti szolgálatot ellátók csak kinevezett ügyeletesek legyenek.

**Ideiglenes ügyeletnek** minősül állandó ügyelet hiányában, időlegesen, meghatározott célra létrehozott ügyeleti forma.

**Megerősítés céljából** létrehozott ügyeletnek minősül a szükség esetén a rendőri szerv vezetője által ügyeleti szolgálatra vezényelt szolgálati személyek a helyi viszonyok, a terület közbiztonsága, valamint a mindenkori bűnügyi és határrendészeti helyzet függvényében, illetve kiemelt fontosságú eseménnyel összefüggésben az állandó ügyelet tehermentesítése, a szolgálat zavartalan ellátása érdekében.

**Vezető ügyeleti** szolgálatnak minősül a kiemelkedően súlyos rendkívüli események során a konkrét ügyekben teendő elsődleges intézkedések gyors, szakszerű és hatékony végrehajtásának érdekében létrehozott ügyeleti forma, melyet a szervek vezetői havi bontású ütemterv alapján hivatali munkaidőn túl készenléti jelleggel látnak el.

Magasabb készenlétbe helyezés és minősített időszak kihirdetése esetén a Rendőrség Összesített Készültségbe Helyezési Terve alapján, az ügyeleti szolgálatokat meg kell erősíteni, illetve az állandó ügyeleteken túl, szükség esetén ideiglenes ügyeleti szolgálatokat kell szervezni.

Az ORFK állandó ügyeleti szolgálatát (a továbbiakban: ORFK Főügyelet) az ORFK Rendészeti Főigazgatóság Ügyeleti és Védelmi Igazgatási Osztály (a továbbiakban: Ügyeleti Osztály) látja el.

## 7. Az ügyeleti szolgálati formák

**I. sz. váltásos szolgálati időrendszer**
Váltásonként 12 óra szolgálat 24 óra szabadidő, 12 óra szolgálat 48 óra szabadidő, vagy váltásonként 12 óra szolgálat, 12 óra szabadidő, 12 óra szolgálat, 48 óra szabadidő, 12 óra szolgálat, 12 óra szabadidő, 12 óra szolgálat, 72 óra szabadidő.

Azokban a folyamatos munkavégzést igénylő beosztásokban lehet alkalmazni, ahol a munkaterhelés viszonylag állandó, egyenletes.
A szolgálatteljesítési időt havi, maximum 2 havi keretben határozzák meg, melynek meg kell egyeznie az adott időszak munkanapjai számának és a napi 8 órás munkaidőnek a szorzatával. A napi szolgálatteljesítési idő a váltási rend szerint számított folyamatos 12 óra.

**II. sz. váltásos szolgálati időrendszer**
Váltásonként 24 óra szolgálat 72 óra szabadidő. A részben vagy egészben készenléti jellegű (Pl. ügyeleti, őr) szolgálatokban alkalmazható akkor, ha rendkívüli eset kivételével az állomány tagja legalább 4 órát alvással tölthet.
A szolgálatteljesítési időt havi, maximum 2 havi keretben határozzák meg, melynek meg kell egyeznie az adott időszak munkanapjai számának és a napi 8 órás munkaidőnek a szorzatával. A napi szolgálatteljesítési idő a váltási rendben meghatározott napon a szolgálatkezdéstől számított folyamatos 24 óra.
A váltásos szolgálati időrendszerekben a heti pihenőnapok a hét előre meghatározott naptári napjai, amelyeket a havi szolgálatvezénylési tervben kell meghatározni.

## 8. Az ügyeleti szolgálatok szakmai irányítása, a szolgálatok szervezési elvei

Az ORFK Főügyelet szakmai irányítása alá tartoznak:
*a)* a KR főügyelete;
*b)* az RRI ügyelete;
*c)* a megyei (fővárosi) rendőr-főkapitányságok ügyeletei.
A megyei (fővárosi) rendőr-főkapitányságok ügyeleteinek szakmai irányítása alá tartoznak az illetékességi területükön működő:
rendőrkapitányságok ügyeletei;
határrendészeti kirendeltségek ügyeletei;
őrzött szállások ügyeletei.
Az RRI ügyeletének szakmai irányítása alá tartoznak:
*a)* Őrzött Szállás és Objektumbiztonsági Szolgálat ügyelete;
*b)* Közrendvédelmi és Határellenőrzési Osztály Ferihegy I. szolgálatirányító parancsnok;
*c)* Közrendvédelmi és Határellenőrzési Osztály Ferihegy II. szolgálatirányító parancsnok;
*d)* bűnügyi nyomozó;

*e)* CCTV és Készenléti Alosztály kiemelt főelőadó, előadó, vizsgáló, monitorkezelő;
*f)* Sólyom Bevetési Alosztály bevetési járőr.

A KR főügyeletének szakmai irányítása alá tartoznak a KR-nél működtetett ügyeleti, szolgálatok:

*a)* a KR Rendészeti Igazgatóság híradó ügyelete;
*b)* a KR Különleges Szolgálatok Igazgatósága (a továbbiakban: KSZI) Állami Futárszolgálat ügyelete;
*c)* a KR KSZI Tűzszerész Szolgálat ügyelete;
*d)* a KR KSZI Pénzkísérő Szolgálat ügyelete.

A rendőrkapitányság ügyeletének alárendeltségébe tartoznak az illetékességi területén létrehozott és működő rendőrőrsök ügyeletei.

A határrendészeti kirendeltségek és határellenőrzési osztályok ügyeleteinek alárendeltségébe tartoznak az illetékességi területén működő határátkelőhelyek és a kihelyezett szolgálati helyek ügyeletei, valamint az ideiglenes határátkelőhelyek.

Az ügyeletek az állománytáblában meghatározott közvetlen vezető alárendeltségében végzik a belső rendelkezésekben meghatározott tevékenységüket. Az ügyeletes a rendőri szerv vezetőjének távollétében, illetve hivatali munkaidőn kívül, annak átruházott jogkörében (nevében) jár el.

Az ügyeleti szolgálatot teljesítők szolgálati időrendszerbe sorolását a hatályos belső rendelkezésekre figyelemmel a rendőri szerv vezetője határozza meg.

A rendőri szerv ügyeletére érkező hívásokat (segélyhívások, városi hívások) a hívó fél előzetes tájékoztatását követően lehet rögzíteni. A hangrögzítés tényéről szóló tájékoztatást gépi hangbemondással kell biztosítani. Azokon az ügyeleteken, ahol az automatikus tájékoztatás technikailag nem megoldott, illetve technikai hiba lépett fel, ott a bejelentés megtétele előtt – *amennyiben a késedelem veszéllyel nem jár, illetve nem késlelteti az egyébként megteendő sürgős intézkedést* – a bejelentő részére szóban kell megadni a szükséges felvilágosítást.

Az ügyeletekre így beérkező hívásokat csak olyan rendőrségi mellékre, illetve munkaállomásra lehet továbbkapcsolni, amelyen a hangrögzítés megoldott és a beszélgetést rögzítik. Az előzetes felvilágosítás során tájékoztatni kell a bejelentőt, hogy – *amennyiben kifogásolja a hangrögzítés tényét* – bejelentését bármely ügyeleten személyesen is megteheti. A közvetlen vezetőnek az ügyeletesi állomány részére a feladat végrehajtásával kapcsolatosan felkészítést, illetve eligazítást kell tartani.

A közös elhelyezésből adódóan a Budapesti Rendőr-főkapitányság Központi Ügyeleti Főosztály ügyeletvezetőjének az ORFK Főügyelet felé történő szóbeli

jelentéseit az időpont pontos dokumentálása és a szóbeli jelentés hanganyagának visszakereshetősége érdekében telefonon is meg kell tennie.
A szolgálat átadás-átvétel során a szolgálatot kezdő ügyeletes a rendelkezésre álló információk alapján köteles megismerni az elmúlt 48 órában történt és a „kiemelt rendkívüli" kategóriába tartozó események anyagait is.

**9. A jelentési, tájékoztatási kötelezettség rendje**

A rendőri szervek vezetői az illetékességi területükön történt eseményekről, a tett intézkedésekről ügyeleteik útján az alábbiak szerint kötelesek jelentést tenni az ORFK Főügyeletnek abban az esetben is, ha ezt előzetesen szóban a szerv részéről valaki már jelentette az ORFK illetékes vezetőjének:
*a)* a „*kiemeltnek*" („*K*" jelölésű) minősített kiemelt rendkívüli eseményekkel kapcsolatos:
aa) elsődleges adatokat az előzetes ellenőrzés után távbeszélőn azonnal,
ab) az élet- és anyagi javak mentése, a veszélyhelyzet elhárítása érdekében tett további intézkedéseket távbeszélőn folyamatosan,
ac) a mentési és kárelhárítási munka befejezése, a helyszíni szemle megtartása után az eseményt, az előidéző okokat, következményeket, a tett intézkedések addigi eredményét írásban haladéktalanul;
*b)* a „*nem kiemeltnek*" („*R*" jelölésű) minősített rendkívüli eseményeket a tények és adatok, azok megállapítása és ellenőrzése, valamint a szükséges intézkedések megtétele után a nap bármely szakában, írásban (fax, e-mail) a legrövidebb időn belül;
*c)* az egyéb felsorolt eseményeket minősített időszakban soron kívül, illetve folyamatosan;
*d)* a MONITORING valamely fokozatának elrendelése esetén az elrendelő által meghatározott információkat, figyelemmel a kért tartalomra, a jelentés módjára és formájára, valamint idejére.
A vezetői hírigény kielégítése céljából a kiemelt rendkívüli eseményekről a számítógépes jelentőszolgálati rendszeren megküldött jelentésekben foglaltakhoz képest további információkat is szükséges az ORFK Főügyeletre továbbítani. A jelentőszolgálati rendszeren megküldött jelentéssel párhuzamosan, vagy akár azt megelőzően is az illetékes ügyelet rendelkezésére álló írásos, az eseménnyel kapcsolatos lényeges adatokat, körülményeket tartalmazó háttéranyagok (jelentések, jegyzőkönyvek, feljegyzések stb.) közül az ORFK Főügyeletnek csak azokat kell e-mailben, vagy faxon megküldeni, amelyek nem lettek a Robotzsaru rendszerben előzőleg rögzítve (pl.: egyes demonstrációk bejelentésével kapcsolatos

írásos anyagok). Azokat a háttéranyagokat, amelyeket a Robotzsaru rendszerben már rögzítettek, e-mailben vagy faxon az ORFK Főügyelet részére továbbítani nem kell, az ORFK Főügyelet azokat a Robotzsaru rendszerből válogatja le. Kerülni kell a terjengős, nehezen áttekinthető és a lényeges információkat nélkülöző írásos anyagok megküldését.

Az ügyeletek által hiányosan, pontatlanul készített és a jelentőszolgálati rendszeren megküldött jelentéseket ki kell egészíttetni. A lényegesnek ítélt nyitott kérdéseket (pl. őrizetbe vétel foganatosításával vagy annak elmaradásával, fegyverhasználattal, személyi állománnyal kapcsolatos események stb. körülményeit) minden esetben tisztázni kell. Erről az ügyeletes újabb adatok soron kívüli bekérésével gondoskodik.

A jelentő ügyelet által szóban ismertetett kiemelt rendkívüli eseményekről a jelentést fogadó ügyelet vezetőjének legkésőbb egy óra elteltével kiegészítő információt kell kérnie. Az írásos jelentés megérkezéséig – *amennyiben szükséges, azt követően is* – folyamatosan figyelemmel kell kísérnie az esemény alakulását.

A alapján késedelmesen küldött jelentésekre az ügyeletesnek minden esetben rá kell vezetnie az elsődlegesen szóban, majd az írásban történő jelentés pontos időpontját, a jelentést küldő és az azt fogadó ügyeletes nevét. A késedelmesen vagy kifogásolható tartalommal küldött anyagokat vezetői beszámoltatáskor – *kivizsgálás céljából* – át kell adni a közvetlen vezetőnek.

A rendőri szervek vezetői kötelesek az illetékességi területükön történt, a közvéleményt foglalkoztató bűnügyi vagy közbiztonsági szempontból lényeges eseményeket figyelemmel kísérni és értékelni. Amennyiben azokról az illetékes szervek tájékoztatása szükséges, úgy az ORFK Főügyeletet haladéktalanul értesítik.

Az ORFK azon szervezeti egységeinél vagy szervezeti elemeinél (a továbbiakban együtt: szervezeti egység), ahol ügyelet nincs, vagy nem állandó jelleggel működik, a szerv vezetője köteles gondoskodni arról, hogy a szervnél történt és az utasítás mellékleteiben felsorolt rendkívüli eseményekről az ORFK Főügyeletet haladéktalanul tájékoztassák.

Az ORFK szervezeti egységeinél, valamint a KŐ-nél, az NNI-nél, a KR-nél és az RRI-nél történt, vagy az ott szolgálati beosztást betöltő rendőrt érintő, rendkívüli, illetve kiemelt rendkívüli esemény bekövetkezése esetén az adott szerv szervezeti egységének vezetője köteles gondoskodni az ORFK Főügyelet haladéktalan tájékoztatásáról.

Az ORFK Főügyelet azonnal jelenti:

*a)* a rendkívüli eseményeket az országos rendőrfőkapitánynak, a bűnügyi vagy a rendészeti főigazgatónak, illetve az általuk meghatározott szervnek, személynek, valamint az illetékes vezetőknek és az Ügyeleti Osztály vezetőjének;

*b)* a közérdeklődésre számot tartó eseményeket munkaidőben az ORFK Szóvivői Iroda vezetőjének, munkaidőn túl az ORFK Szóvivői Iroda ügyeletesének;
*c)* a kiemelt rendkívüli eseményeket a hatáskörrel rendelkező főosztályvezetőnek, illetve az Ügyeleti Osztály vezetőjének.

Az ORFK Főügyelet magasabb készenlétbe helyezése esetén és minősített időszakban a bekövetkező eseményeket soron kívül szóban, külön utasításra írásban jelenti:
*a)* az országos rendőrfőkapitánynak és a bűnügyi főigazgatónak (a bűnügyi főigazgató akadályoztatása esetén a helyettesítésre kijelölt személynek),
*b)* az Ügyeleti Osztály vezetőjének,
*c)* az *a)-b)* pontokban megjelölt vezetők által meghatározott személyeknek, szerveknek.
Az ORFK Főügyelete közvetlenül, a KR, a KŐ és az NNI főügyelete pedig az ORFK Főügyeletén keresztül a BM ügyeletét és a Rendvédelmi Szervek Védelmi Szolgálata (a továbbiakban: RSZVSZ) területileg illetékes vezetőjét, illetve beosztottját, a megyei (fővárosi) rendőr-főkapitányság és az RRI ügyelete pedig az RSZVSZ helyi munkatársát szóban, azonnal tájékoztatja az utasításban meghatározott eseményekről.
A megyei (fővárosi) rendőr-főkapitányságok ügyeleteinek, a KR, az RRI, a KŐ és az NNI ügyeleteinek magasabb készenlétbe helyezése esetén és minősített időszakban 20.00 órai eseményzárással 22.00 óráig kötelesek ügyeleteik útján összefoglaló jelentést tenni az ORFK Főügyelet részére. Az ORFK Főügyelet magasabb készenlétbe helyezése esetén és minősített időszakban 20.00 órai eseményzárással naponta 23.00 óráig – *a békeidőszaki jelentési kötelezettségen túl* – köteles összefoglaló jelentést készíteni és azt a BM ügyeletének felterjeszteni.
A szerv vezetője, ha az katonai légi járművet érintő esemény következik be 5 munkanapon belül köteles értékelő jelentést az eseménnyel kapcsolatosan, állásfoglalás céljából az illetékes megyei közrendvédelmi, közlekedésrendészeti vagy határrendészeti osztály vezetőjének, Budapesten a budapesti rendőrfőkapitány illetékes szakmai helyettesének, illetve a KR parancsnoka szakmai helyettesének, az NNI igazgató-helyettesének és a KÖ hivatalvezetőjének felterjeszteni. Az állásfoglalással kiegészített jelentést további 3 munkanapon belül az ORFK Rendészeti Főigazgatóság Közrendvédelmi Főosztálya vezetőjének, az ORFK Rendészeti Főigazgatóság Közlekedésrendészeti Főosztálya vezetőjének, az ORFK Rendészeti Főigazgatóság Határrendészeti Főosztálya vezetőjének kell megküldeni, akik szakmai revízió keretében azt megvizsgálják, értékelik, szükség esetén azzal kapcsolatosan intézkedést kezdeményeznek.

A megtévesztéssel, a sértett figyelmének elterelésével gépjárműben elhelyezett, vagy ott lévő tárgy, értéktárgy vagy pénz eltulajdonításának célzatával elkövetett lopásról (ún. trükkös lopás) az általános jelentéskötelezettségen felül e-mailben (az ügyeleti szervek ún. funkcionális elektronikus e-mail címére továbbított levélben megjelenítve a bűncselekmény kapcsán keletkezett összes adatot), a Rendőrség által alkalmazott GroupWise levelezőrendszer használatával az alábbiak szerint kell a tájékoztatási kötelezettséget teljesíteni:

*a)* az elkövetés helye szerinti szerv (rendőrkapitányság) ügyelete a megyei (fővárosi) rendőr-főkapitányság ügyeletét és a megye (főváros) területén lévő rendőrkapitányságok, határrendészeti kirendeltségek, illetve a feltételezett menekülési útvonallal érintett megyei (fővárosi) rendőr-főkapitányságok, rendőrkapitányságok, határrendészeti kirendeltségek ügyeleteit;

*b)* a bejelentés helye szerinti szerv (rendőrkapitányság) ügyelete az elkövetés helye szerinti megyei (fővárosi) rendőr-főkapitányság és a feltételezett menekülési útvonallal érintett megyei (fővárosi) rendőr-főkapitányságok ügyeleteit;

*c)* az *a)* és *b)* alpontban az elkövetés helye szerinti megyei (fővárosi) rendőr-főkapitányság ügyelete az ORFK Főügyeletét.

Az állam elleni bűncselekmény, állami vezetők elleni támadás, terrortámadás, katasztrófahelyzet, légi jármű hatalomba kerítése, halálos tömegszerencsétlenség, veszélyes bűnöző vagy fogvatartott menekülése, szökése, intézkedő rendőr elleni súlyos támadás, rendőr lőfegyverhasználata esetén az illetékes rendőrkapitányság vagy határrendészeti kirendeltség ügyelete a GroupWise levelezőrendszer alkalmazásával e-mailben tájékoztatja a megyei (fővárosi) rendőr-főkapitányság, a megye (főváros) területén lévő rendőrkapitányságok és határrendészeti kirendeltségek ügyeleteit.

A veszélyes bűnöző vagy fogvatartott menekülése, szökése esetén a szomszédos, illetve a menekülés útvonalával érintett megyei (fővárosi) rendőr-főkapitányságok, rendőrkapitányságok és határrendészeti kirendeltségek ügyeletei az egyéb hírforgalmi eszközök igénybevételén túl e-mailben kölcsönösen és folyamatosan tájékoztatják egymást, koordinálják az intézkedéseket. Az e-mailben küldött információk késedelem nélküli fogadása érdekében a levelezőrendszer riasztási paramétereit úgy kell beállítani, hogy az ügyeletek által küldött üzenet megérkezésekor figyelmeztető jelzés jelenjen meg az e-mailt fogadó számítógépen. Ennek beállításáról minden szerv rendszergazdája késedelem nélkül köteles intézkedni.

**Összegzés**

Jelen cikkünk bemutatta a rendőri szervek korszerűsített ügyeleti szolgálati rendszerét.

**Felhasznált irodalom**

[1] Pándi Balázs: A tábori hírrendszer vizsgálata a hatékonyság növelésének érdekében, PhD értekezés, 41. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2009.
[2] Dr. Finszter Géza: A rendészeti rendszer alkotmányos és közjogi alapjai (2. számú előtanulmány az átfogó rendészeti stratégia társadalmi vitájához), 16-17. oldal, Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Budapest, 2008.;
[3] A Rendőrségről szóló 1994. évi XXXIV. törvény, Complex Jogtár, ISSN 1788-5027, Budapest, 2011. július 31.;
[4] Horpácsi Ferenc: A határőrség minősített időszaki feladatai, különös tekintettel a bevetési szervek alkalmazására, PhD értekezés, 49-51. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2005.
[5] Németh Gyula: A rendőrség logisztikai támogatásának átalakítása, PhD értekezés, 60-61. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2011.
[6] Zimán Ferenc: A megyei csapaterő századok helye és szerepe a rendkívüli események kezelésében, az együttműködés lehetősége a Készenléti Rendőrséggel, Belügyi Szemle, 52. évfolyam, 4. szám, 3-18. oldal, ISSN 1218-8956, Budapest, 2004.

**Jelen számunk szerzői**

| | |
|---|---|
| **Dr. Bleier Attila** | Ericsson fejlesztőmérnök |
| **Dr. Bozsó Zoltán** | Gödöllői rendőrkapitány |
| **Dorkó Zsolt** | NKE PhD hallgató |
| **Fábián Éva** | NKE PhD hallgató |
| **Horváth Tamás** | MVM fejlesztőmérnök |
| **Dr. Kerti András** | NKE HHK adjunktus |
| **Dr. Kovács Tibor** | OE egyetemi docens |
| **Dr. Pándi Erik** | NKE HHK főiskolai tanár |
| **Prisznyák Szabolcs** | NKE PhD hallgató |
| **Puskás Béla** | OE PhD hallgató |
| **Román Zsolt** | OE PhD hallgató |
| **Dr. Rajnai Zoltán** | OE egyetemi tanár |
| **Szabó Anna Barbara** | OE PhD hallgató |
| **Szente András** | OE PhD hallgató |
| **Vanderer Gábor** | OE PhD hallgató |

**Szerzőink figyelmébe**

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás nélkül* - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Felelős kiadó: Dr. Fekete Károly mk. alezredes
Megjelent az NKE HHK Híradó Tanszék gondozásában, 10 példányban, illetve elektronikusan:

www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK Híradó Tanszék
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-358 mellék)
hhk_hirado_szakcsoport@uni-nke.hu