# HADMÉRNÖK

A ZMNE Bolyai János Katonai Mûszaki Kar
és a Katonai Mûszaki Doktori Iskola
on-line tudományos kiadványa

**III. Évfolyam 3. szám 2008. szeptember**

**ZMNE**
**BUDAPEST**

*A szerkesztőség elérhetősége:*
Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
*Postacím:* 1581. Budapest Pf.:15.
*Telefon:* +36-1-432-9048
*Fax:* +36-1-432-9208
*HM:* 29-734
*e-mail:* hadmernok@zmne.hu

**Kiadó:** Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
**Kiadásért felelős:** Prof. Dr. Szabó János, a ZMNE rektora
**ISSN 1788-1919**

**Jelen számban megjelent írások szerzői:**

**Apostol Attila** – ZMNE BJKMK
**Bakosné Diószegi Mónika** – Budapesti Műszaki Főiskola
**Csuka Antal** – Gábor Dénes Főiskola, ZMNE KMDI, doktorandusz hallgató
**Dr. habil Cziva Oszkár** tü. ezredes – Fővárosi Tűzoltóparancsnokság
**Előházi János** – ZMNE KMDI, doktorandusz hallgató
**Farkas Imre** – ZMNE KMDI, doktorandusz hallgató
**Dr. Földi László** mk. őrnagy – ZMNE BJKMK, egyetemi docens
**Prof. Dr. Halász László** – ZMNE BJKMK, egyetemi tanár
**Hanka László** – ZMNE BJKMK, egyetemi adjunktus
**Horváth Csaba** – ZMNE BJKMK, egyetemi hallgató
**Horváth Zita** – ZMNE BJKMK, egyetemi hallgató
**Kanyó Ferenc** – Fővárosi Tűzoltóparancsnokság
**Körmendi Krisztina** – PROTAN Zrt.
**Prof. Dr. Munk Sándor** – ZMNE BJKMK, egyetemi tanár
**Dr. Négyesi Imre** mk. alezredes – ZMNE BJKMK, egyetemi docens
**Dr. Pándi Erik** r. alezredes – ZMNE BJKMK, egyetemi docens
**Pántya Péter** – ZMNE BJKMK, egyetemi hallgató
**Dr. Sipos Jenő** mk. ezredes – ZMNE BJKMK, dékán
**Prof. Dr. Solymosi József** – ZMNE BJKMK, egyetemi tanár
**Szombati Zoltán** mk. ezredes – MH 93. Petőfi Sándor Vegyivédelmi Zászlóalj
**Dr. habil Vincze Árpád** – Országos Atomenergia Hivatal

HADMÉRNÖK

**III. Évfolyam 3. szám - 2008. szeptember**

**Cziva Oszkár**
Headquarters of the Fire Department of Budapest
(Fővárosi Tűzoltóparancsnokság)
drczivao@tuzoltosagbp.hu

**Kanyó Ferenc**
Headquarters of the Fire Department of Budapest
(Fővárosi Tűzoltóparancsnokság)
kanyof@tuzoltosagbp.hu

# DIFFERENT INTERNATIONAL METHODS FOR TESTING THE ABILITY OF FIREFIGHTERS

***Abstract/Absztrakt***

*The current physical test has become some sort of "necessary evil" among firefighters, and most of them are opposed to it even more strongly than members of the military, the police or the border guards. This rejection can be traced back to the general opinion that the exercises during these tests (2000-meter running, 4x10-meter "pendulum running", etc.) are regarded unnecessary for the firefighting profession. The question often arises:" When do we have to run 2000 meters while putting out a fire?" This negative attitude towards regular exercise and healthy lifestyle causes a lack of information, deeply affects the level of physical fitness, and it is also responsible for thoughts like "We've got to get over with this somehow!" Based on the feedback received from the staff, our firefighters would rather be tested on performing professional tasks that would clearly show their physical fitness for the job.*

*A jelenlegi fizikai tesztekre, mint szükséges rosszra tekintenek a tűzoltók, és közülük számosan nagyobb ellenszenvvel viseltetnek iránt uk, mint a katonák, rendőrök, vagy határőrök. Ez az ellenérzés arra az általános véleményre vezethető vissza, amely szerint a tűzoltói gyakorlatban feleslegesek a teszt során végrehajtandó feladatok (2000 m-es futás, 4x10 méteres ingafutás, stb.). Gyakran felmerülő kérdés: „Mikor kell nekünk 2000 métert futnunk, amikor tüzet oltunk?". Ez a negatív hozzáállás a rendszeres mozgáshoz és az egészséges életmódhoz információhiányt okoz, nagyban befolyásolja a fizikai állapotot, és „valahogy csak túl leszünk ezen és megcsináljuk" álláspontot erősíti. A vezetéstől kapott visszajelzések alapján, a tűzoltók felmérése inkább szakmai feladatok alapján kell,*

*hogy történjen, amelyek világosan megmutatják fizikai állóképességüket a munkájuk során.*

***Keywords/kucsszavak:*** *ability tests, Fire Service, Candidate Physical Ability Test, Fire-simulation containers ~ képesség tesztek, tűzoltóság, fizikai felvételi teszt, tűz-szimulációs konténerek*

There are different ways of testing firefighter candidates all around the globe. The main purpose of the tests is to measure if the applicant is physically and psychologically fit for the job. Later, when a person becomes a firefighter, his fitness continues to be monitored and evaluation of their performance is conducted on a regular basis.

We have collected material from many different countries and began to select the best possible methods applied around the world. Learning about experiences in other countries proved to be extremely useful in the process of creating a new system for Hungary.

The profession of firefighters is considered to be one of the most honorable occupations in the world that requires outstanding psychological and physical conditioning from each fireman to perform well on duty.

Examining, testing, and analyzing the physical fitness of firefighters as well as discovering new methods to improve their skills based on the results of these tests have been common practice in Hungary for almost ten years. The main purpose of examining the physical fitness of firefighters is to determine their permissible load.

Below are some examples of fitness tests performed around the world from different departments.

### Nova Scotia, Canada

A wild-land firefighter's standardized fitness test comes into effect in 2008. The test will include a 4.8-kilometre walk while weighed down by 20-kilogram vest. They will have 45 minutes to finish the course. There will be other tests too.

### Somerset Fire and Rescue Service, UK

Specific job related tests are given such as written and aptitude tests, and physical and fitness tests which must be passed before proceeding to interview. The fitness tests that are conducted are very specific to the job required, and include the following:

- Multistage Fitness Test/ bleep test - a pass mark of level 8, shuttle 4
- Hose Running - a test of dexterity, stamina and coordination. This test will involve 25 m lengths of 70 mm hose to be rolled out and returned in a set time.
- Ladder Climb Test - a test for compatibility with working at heights, and will involve locking the legs allowing both arms to be free.
- Ladder Extend Test - a test of arm and grip strength. The test simulates extending the 13.5m ladder that is used extensively within the service.
- Dead lift simulator - device which tests lower back and leg strength and is set at 50 kg.

- Enclosed Space Test - a test of confidence, agility and will identify claustrophobic tendencies. The candidate dons breathing apparatus (BA), facemask and negotiates a crawl and walkway with vision obscured.

Two tests are now not included, the Back and leg pull test using a Dynamometer (due to possible risks through poor technique) and the Hand Grip Test (as grip strength is taken into account during the ladder extension)

### UK Fire Service

You will have to undertake a series of tests such as:

- Lung Capacity
- Chester Step Test
- Height
- Weight
- Strength Tests
- Eye Tests
- Urine Sample
- Blood Test
- A visit to the onsite Doctor

### Surrey County Fire Fighters, UK

Applicants must complete a practical and physical assessment.

**Practical:** Applicants will be tested in the five different areas listed below. In order to reach the standard, applicants must be successful in all five tests. All five of the practical tests will be conducted in the full fire kit.

- Dead lift
- Ladder extension
- Ladder ascent and descent
- Enclosed space (Breathing Apparatus)
- Hose running

**Physical:** Applicants will be tested in the three different areas listed below.

- Grip strength test
- Isometric back strength test
- Aerobic capacity test (Chester Step Test)

### Saskatchewan Environment forest firefighters (Canada)

The annual testing protocol includes the following tests (plus several others):

- a fitness walk with weight packs. Carrying 20.25 kilograms for 4.8 kilometers in less than 45 minutes.
- hose carry and hose dragging

### Fire Departments, US

The International Association of Fire Fighters (IAFF) unveiled several years ago the new Joint Fire Service Candidate Physical Ability Test (CPAT). This unprecedented, innovative and equitable physical ability test for fire fighter candidates is designed to help fire departments measure the physical ability of candidates to perform routine fire fighting tasks. It consists of eight events:

- a stair climb
- hose drag
- equipment carry
- ladder raise and extension
- forcible entry
- search maze
- rescue simulation
- ceiling breach and pull.

It is a pass-fail test that is content-valid based on fire fighter job tasks, but avoids the pitfalls of testing candidates on specific fire fighting skills that require academy training.

The test was designed to be both reliable and valid, meaning the test will produce consistent results and will measure an applicant's ability to display job-relevant characteristics and skills. It has been through an extensive validation process, including scientific, legal, and fire service review.

### Fire Rescue, Largo

They have a voluntary fitness program, where members have to meet certain minimum fitness standards for the following tests (the links are to general descriptions of these tests, and may not be the specific procedures used by this department):

- 1-1/2 mile run
- push-ups
- sit-ups
- sit & reach
- chin-ups

### Houston Fire Department

The Houston Fire Department uses a job-related physical ability test designed to test determine if an applicant has the strength and endurance needed to perform the job duties of a Firefighter. These job duties require balance, coordination, strength, endurance, and cardiovascular fitness. Applicants will be tested over seven (7) timed, pass/fail events while wearing gloves and an air pack.

- Balance Beam Walk
- Ladder Extension
- Stair Climb
- Equipment Hoist
- Portable Equipment Carry
- Rescue Attempt

- 1.5 Mile Run

### NSW Fire Brigade, Australia

During the Firefighting Task Course you will be required to complete the tasks (listed below) in succession, walking from one task to the next. You will be required to wear structural Personal Protective Equipment (PPE) including coat, over-trousers, lightweight helmet, general purpose gloves and non-operational Self-Contained Breathing Apparatus (without face mask).

- Ladder climb
- Hose coupling
- Ladder raise and lower
- Tunnel crawl
- Beam walk
- Chain cutting
- Hose reel drag
- Hose drag and hold
- Tower climb and container haul
- Tower climb and visual recognition

### Rochester Fire Department, US

Candidates must pass the physical agility test twice — first to get into the training academy, then after passing a written exam they must do it all again to get out of the academy and join the department. Fail to complete any one of a total eight stations, and they are out.

The testing involves various job specific tasks, including hauling a fire hose, dragging a 165-pound dummy, swinging a sledgehammer, and raising a ladder. The toughest test is three minutes on the stair machine saddled with 75 pounds in weights to simulate equipment.

### Scotland Fire Fighters

Although there are no ongoing mandatory fitness tests for Scottish firefighters, six of the eight forces have established their own monitoring regime. Strathclyde Fire and Rescue, has yet to introduce any test, while Fire's service only assesses new recruits. They are both reviewing their procedures with a view to introducing fitness tests for employees every three years. Of those that do regular testing, the demands and frequency of the tests vary widely.

Firefighters in both Dumfries and Galloway and Lothian and Borders take a mandatory fitness test every three years, using an exercise bike. An occupational health therapist monitors their heart rate, blood pressure and body fat.

Central Scotland's service uses the Chester Step Test, as does Tayside carried out every year on uniformed staff. Grampian has used the Chester step test for more than 15 years, with all uniformed staff under the age of 40 being tested every two years and annual tests for those over 40 years of age. Highlands and Islands Fire and Rescue operate a fitness test every three years.

A Scottish Executive spokesman said there were no plans to introduce a national standard fitness test across all the emergency services.

## The occupation specific physical fitness evaluation [2]

### 1. Aerobic fitness

Aerobic fitness will is measured directly using expired air analysis while running on a treadmill. The speed and incline are gradually increased until the candidate reaches his/her maximum intensity. This test is designed to measure endurance or "work capacity".

Participation in moderate to high intensity aerobic workouts (30 - 45 minutes per workout, 4 - 5 times per week) including such activities as jogging, cycling, swimming and rowing, can help you prepare for the aerobic fitness assessment. Consult your physician and/or a qualified fitness instructor before starting any exercise program.

### 2. Job-related performance evaluation

There are eight job-related performance tests. The tests are designed to simulate the physical demands of a firefighter's job which requires both muscular strength and endurance.

To prepare for these tests, you may wish to participate in supervised weight training, stretching and an aerobic exercise program to increase strength, improve flexibility and enhance aerobic fitness. Consult your physician and/or a qualified fitness instructor before starting any exercise program.

### 1. Ladder climb

Wearing a 9.1 kilogram cylinder from an S.C.B.A. (self-contained breathing apparatus), you will climb a 12.2 metre extension ladder, uncouple and re-couple a wall-mounted hose connection, then climb down the ladder. This test assesses fear of heights (acrophobia) and manual dexterity.

### 2. Search enclosed area (revised)

Wearing a blacked-out face piece, you will be locked in a confined area for a time to be determined by the tester. While you are confined, you will be instructed by the tester to reach up to the top, left front corner and count the number of washers on a bolt sticking out of the wall. You must then call out the correct number to the tester. This test detects fear of confined areas. It is scored on a pass/fail basis - it is not timed

**Note:** During the remaining tests you will be wearing a 13.5 kilogram vest plus 2.3 kilogram weights on each ankle. These weights approximate the heaviness of the protective clothing and SCBA worn by firefighters. You will be timed when you perform all tests except the Ladder Lift Test.

### 3. Hose carry/climb

You will lift and carry over your shoulder a 38.5 kilogram bundle of hose up and down five flights of stairs. This test simulates carrying equipment to the staging areas of a high-rise fire. It assesses dynamic balance, muscular strength of the upper body and back, plus muscular endurance and power of the legs.

### 4. Rope pull

Using a rope, you will hoist and lower in a hand-over-hand manner a 22.5 kilogram weight a height of 20 metres. This test simulates hoisting fire fighting equipment to and from

windows or roofs. It assesses manual dexterity plus the muscular strength and endurance of the upper body and back.

### 5. Hose advance/drag

You will pull a 70 kilogram load which simulates a charged hose line (a hose line that is ready to discharge water), a distance of 15 metres. This test assesses leg power and muscular strength of the upper body.

### 6. Ladder lift

You will remove and replace a 25.5 kilogram ladder from brackets mounted 1.93 metres above the floor. This test simulates the demands involved in numerous fire fighting activities (ie. pike poling, removing ladders from aerial beds, etc.) which require working at or above chest/shoulder height. It assesses muscular strength and endurance of the upper body and back.

### 7. Victim drag

You will drag a 91 kilogram "victim" a distance of 15 metres while weaving in and out of traffic cones placed every 3 metres. This simulates rescuing a downed firefighter wearing full turn-out gear. It assesses upper body, back, plus lowers body muscular strength, agility and dynamic balance.

### 8. Forced Entry (new)

In this test you are required to move a heavily weighted tire a distance of 12 inches (30.5 cm), until the tire contacts the wall, by hitting the tire repeatedly with a 10 lb (4.5 kg) sledge hammer.

This task simulates a forced entry through a door or wall and requires upper body strength, upper body endurance and motor ability. The height of the table is the height of a door handle and also the height at which a sledge hammers or axe is normally swung during a forced entry.

Moving a tire of this weight a distance of 12 inches has been documented to require the same amount of sledge hammer work as breaking through a door or wall.

The tester will record the number of hits and the total time taken to complete the task. Timing begins when you first draw the sledge hammer back from the tire and ends when the tire first contacts the wall.

Please be aware that the hammer will rebound, so hold onto the hammer tightly during both the hit and rebound.

### Budapest Fire Brigade

The current physical test (2000 m, 4X10 m “pendulum running”, sit-ups, push-ups) is regulated by a decree and firefighters have a strong dislike for, because it is not specifically made up of profession-related exercises and does not reflect reality.

In the world of professional sport, it has been standard practice to model sports events and measure the performance of the athletes. Based on similar experiences, it is clear that performance can only be measured in its entirety and not by examining certain selected skills. Experiments with professional athletes prove that even our Olympic and world champions lack certain skills in areas like fitness, coordination, or mental abilities, but they are still world-best in their own event.

Annual physical testing of the staff has been compulsory since 1997. The decree gave all units and the entire staff five years of grace period to prepare for regularly meeting the new requirements. Passing the yearly physical tests and having medical and psychological check-ups have become compulsory for everyone on the job.

However, the current physical test has become some sort of “necessary evil” among firefighters, and most of them are opposed to it even more strongly than members of the military, the police or the border guards.

This rejection can be traced back to the general opinion that the exercises during these tests (2000-meter running, 4x10-meter “pendulum running”, etc.) are regarded unnecessary for the firefighting profession. The question often arises: ”When do we have to run 2000 meters while putting out a fire?” This negative attitude towards regular exercise and healthy lifestyle causes a lack of information, deeply affects the level of physical fitness, and it is also responsible for thoughts like ”We’ve got to get over with this somehow!”

Based on the feedback received from the staff, our firefighters would rather be tested on performing professional tasks that would clearly show their physical fitness for the job.

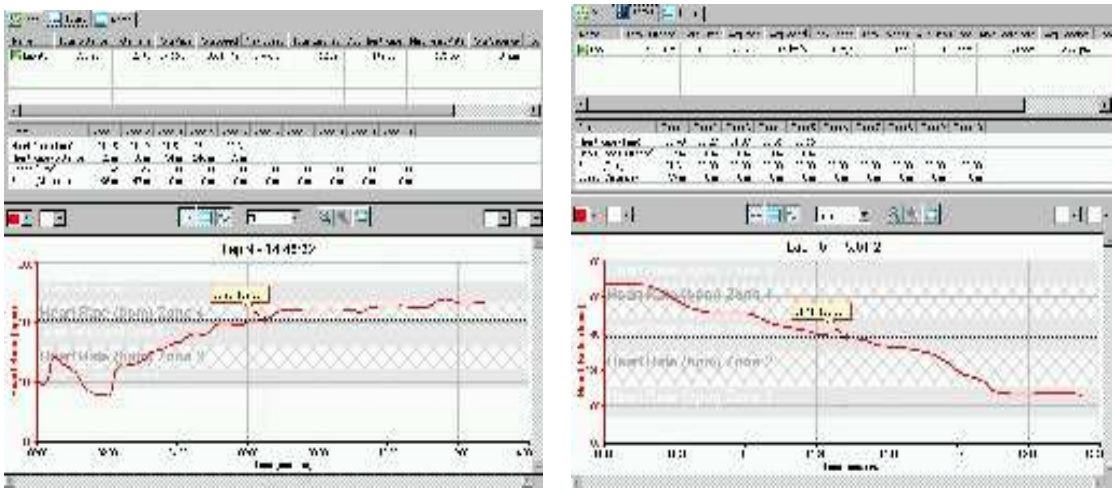
Fire-simulation containers can perfectly model interior fires to be extinguished in lifelike circumstances. During these practices, firefighters are under close observation and they can gain true-to-life experience regarding some unpredictable happenings and difficulties similar to the ones they might encounter while putting out a fire in an apartment or a basement. They can also experience some of the physical and psychological effects a fire might have on their body, and also they can learn how to put out the fire effectively and as quickly as possible. (photos: 1, 2, 3, 4)

Monitoring the physiological parameters of firefighters in action and analyzing and comparing the test results to each other make it possible to assess their physical fitness and determine the optimal duration of labor with their breathing apparatus on.

In order to assess their abilities, we used a FIRE DRAGON III container to make it possible for the firefighters to work in pairs wearing protective equipment such as protective clothing (Bristol), and self-contained breathing apparatus (6-liter Draeger PSS cylinders filled with compressed air at a pressure of 300 bars, weighing 10.6 kilos) providing air supply for about 10-12 minutes to carry out the tasks.

Firefighters tested, had been fitted with heart monitors (Garmin Forerunner 301 and 305) that send heart-rate signals through a device to analyzing software that helped us watch the changes in their heart rate in relation to their work load during the entire test.

The following diagrams show heart rate and antropometric values determining the zones of work load classified by age, the time scale for each zone, and values compared to the maximum determined heart rate based on these pieces of data.



Based on the amount of consumed air we can measure the amount of oxygen used each minute of the test ($VO_2$) and proportionately calculate the intensity of work from how much the firefighters weigh in order to find out precisely how fit each of them is. Three minutes after the end of the test, capillary blood samples were taken, lactic acid levels and blood pressures were checked.

To judge the level of physical fitness just by monitoring the changes of heart rate during the test is not enough, as it only shows the momentary condition of the person. That is why simultaneous monitoring of performance, inhalation of oxygen, and the amount of lactic acid produced by the muscles is all necessary to determine the stamina.

The subjects were allowed to discover the „plain” area and familiarize themselves with the tasks. Following that, each couple of firefighters put on their protective clothing, and before they could climb up to the entrance on the top of the container, the pressure of compressed air in each cylinder was checked. Then the firefighters tested the nozzles by making different patterns of water stream, and after connecting the regulators to the facepieces, the test began.

Describing our experiment we outlined a modern procedure used to test the physical fitness of firefighters that is suitable to monitor them in extreme circumstances that they often have to face on duty.

## References:

[1] Dr. Malomsoki, Dr. Martos, 15. Methodology Letter, OSEI, Budapest 1994, HU ISSN 1215-2234

[2] http://www.topendsports.com/testing/tests (2008. 03. 28.)

HADMÉRNÖK

III. Évfolyam 3. szám - 2008. szeptember

**Bakosné Diószegi Mónika**
Budapesti Műszaki Főiskola

**Solymosi József**
Zrínyi Miklós Nemzetvédelmi Egyetem
solymosi.jozsef@zmne.hu

# LÁGYSZÁRÚ MEZŐGAZDASÁGI NÖVÉNYEKBŐL ELŐÁLLÍTOTT PELLET VIZSGÁLATA, AZ ENERGIABIZTONSÁG NÖVELÉSÉT SZOLGÁLÓ LEHETŐSÉG SZEMSZÖGÉBŐL

***Absztrakt***

*Az emberiség növekvő energiaigénye, a kifogyóban levő földgáz és kőolaj forrás felgyorsítja az újabb energia előállítására irányuló kutatásokat. Fő szempont bolygónk biológiai egyensúlyának fenntartása, egyben a Kiotói világkonferencia megállapodásainak figyelembe vétele. További sürgető kötelezettség hazánknak e területen előírt szigorú Európai Uniós elvárások kielégítése. Melyben célkitűzésként szerepel az egyes tagországok megújuló energiaforrás százalékos növelése a hagyományos energiaforrásokhoz képest. A nap, szél és a geotermikus energiaforrások, valamint a biomassza kifogyhatatlan forrásként vesznek körül bennünket. Magyarország kitűnő természeti adottságának és több évszázados állattenyésztési múltjának köszönhetően- rendkívül jó eséllyel nyithat a biomasszából előállítható energia felé. Ebben a közleményben rövid áttekintést adunk a hazánkban képződő nagy mennyiségű mezőgazdasági hulladék energetikai hasznosíthatóságának lehetőségeiről.*

*Human's increasing demand of energy use, the ending resources of natural gas and fuel accelerates researches on development of 'newer' energy production. The main criteria is to preserve our planet's biological balance considering also the agreements of the World Conference on environmental protection of Kyoto. Furthermore our country's urging obligation is to fulfill the strict European Union requirements in this domain. In which the goal is to increase the percentage of renewable energy resources contra our traditional energy sources. Solar, wind, geothermal power and biomass surround us with unlimited sources. Hungary - with its excellent natural features and centuries long agricultural and animal husbandry tradition - has an extremely promising base to open towards the energy*

*processed from biomass. This publication gives a brief overview on the possibility of energy recycling of Hungary's significant amount of agricultural waste.*

***Kulcsszavak:*** *biomassza, energia egyensúly, mezőgazdasági hulladék hőenergia, energia ellátottság, környezetvédelem ~ biomass, energy balance, agricultural waste heat energy, energy supply provision, environmental protection.*

## MAGYARORSZÁGI ENERGIATERMELÉS

A hazánkban előállított energia az ország éves energia igényének mindösszesen az egyharmadát fedezi. Kézenfekvő elgondolkodni azon, hogy ennek az aránynak a javítását milyen eszközökkel lehet elérni. Fejlett, komoly hagyományokon alapuló mezőgazdaságunk nagy mennyiségű szerves hulladékot hagy maga után évente. Ennek hasznosíthatósága vezet az elégetéséből nyerhető energia vizsgálata felé. Rövid közleményünk fókuszában az eljárás műszaki és gazdasági vizsgálata áll, aminek célja az energiamérleg elkészítése és értékelése.

Magyarország elektromos energiatermelésében a megújuló energiák részaránya 2003-ban 0,5 százalék volt [1]. Az EU csatlakozási tárgyalásokon hazánk képviselői elérték, hogy a megújuló energiák részaránya 2010-re messze a többi tagállam vállalt értéke alatt, mindössze 3,6 százalék (38 PJ/év) legyen. (Ebből kb. 2,8 százalék a biomassza, főleg tűzifa.) Ugyanakkor 2015-ig a megújuló energiák részarányát Magyarországon is 12 százalékra kell növelni.

A megújuló energiatermelés hazai szempontjainak megfogalmazásakor az EU-s elvárásokon és vállalásainkon túl azt is figyelembe kell venni, hogy Magyarország fosszilis energia tartalékai végesek. Valószínűsíthető a gázárak további gyors növekedése is, ami az energiafelhasználás struktúráját át fogja rendezni. A jelenlegi energiatermelés meglehetősen környezetszennyező, emiatt szigorúbb környezetvédelmi szabályozás várható.

Magyarország energiatermelése a Központi Energia Hivatal adatai [1] alapján 2007-ben energiahordozók szerint:

**1. táblázat**

| **Energiaforrás** | **Energia** | **Részarány** |
|---|---|---|
| | [PJ] | [%] |
| Szén | 74,1 | 17,4 |
| Kőolaj | 35,1 | 8,6 |
| Földgáz | 83,1 | 19,8 |
| Gazolin | 6,8 | 1,7 |
| Propán-bután gáz | 7,4 | 1,9 |
| Tűzifa | 25,2 | 6,1 |
| Nukleáris energia | 160 | 38,2 |
| Vízierőművek | 0,8 | 0,2 |
| Egyéb | 25,5 | 6,1 |
| **ÖSSZESEN** | **418** | **100** |

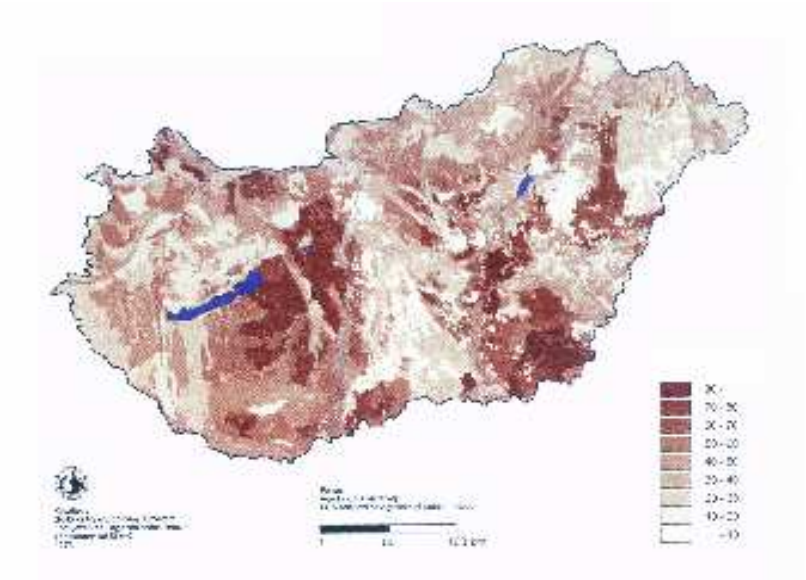
A 418 PJ mellett, a még szükséges energia behozatal értéke: 849 PJ!

Magyarországon közel 1 millió hektárnyi gyenge minőségű szántóterület van, melyen az Európai Unió által előírt minőségű gazdaságos növénytermesztés megvalósíthatatlan. E területek egy része energetikai növénytermesztésre hasznosítható. Energetikai növénytermesztés az 1,79 millió ha 17 AK alatti – rossz minőségű –, talajokon is megvalósítható. Országos szinten is fontos feladat meghatározni azt az energia mennyiséget, amely a hagyományos mezőgazdasági termelésből kieső területeken energetikai növényekből előállítható.

Magyarország területének felosztása mezőgazdasági szempontból, a Központi Statisztikai Hivatal [2] által közzétett mezőgazdasági termelés 2003:

| | |
|---|---|
| vegetáció: | 7 596 000 ha, |
| erdő: | 1 760 000 ha, |
| megművelt terület: | 5 744 000 ha, |
| szántó terület: | 4 500 000 ha, |
| az EU által támogatott terület: | 3 488 000 ha, |
| 17 AK alatti terület: | 1 790 000 ha. |

Hazánk talajminőségének megoszlása jól érzékelhető az MTA Talajtani és Agrokémiai Kutatóintézetében 1997-ben készült agrotopográfiai térképen [3]:



1. ábra

Magyarország biomassza potenciálja kb. 350-360 millió tonna, ebből évente 105-110 millió tonna regenerálódik. Az évente megújuló növényzet energiapotenciálja: 1185 PJ. Ez több mint az ország energiaszükséglete, mely 2007-ben 1040 PJ/év (ennek 57-58 százaléka, 583 PJ import volt).

Magyarországon évente 15-20 millió tonna biomassza keletkezik, melyből kb. 9 milliót az energiaerdő, a többit a lágyszárú növények tesznek ki. (Az összes erdő mennyisége mintegy 250 millió tonna.)

A mezőgazdasági melléktermékként jelentkező biomassza jelentős mértékű. A betakarított hasznosításra kerülő növények csupán egy része kerül feldolgozásra fogyasztás céljából. A többi része mezőgazdasági hulladékká válik az aratás után. Emellett Magyarországon is egyre nagyobb szerepet kapnak a kifejezetten energianyerés céljából termesztett energianövények.

Ezek a fűz (salix), a nyár (poplar), az akác (robinia), a bálványfa, a különböző energiafüvek, az energianád (miscanthus), a repce, a kender és a tritikale.

## A HAZAI KUKORICASZÁR,-CSUTKA ÉS –CSUHÉ ALAPÚ BIOMASSZA KÉSZLET

Az alábbiakban látható a kukoricaszár, -csutka és -csuhé alapú biomassza hasznosítása területén tudomásomra jutott legújabb ismeretek.

A Magyarországon országos átlagként figyelembe vehető hektáronként 6 tonna betakarított kukorica-szemtermés esetén, a visszamaradó növényi részek szárazanyagban kifejezett mennyisége és aránya tetemes [4]:

**2. táblázat**

| **Megnevezés** | **1 ha-on maradó szárazanyag** | **1 ha-on maradó szárazanyag** | **1 ha-on maradó energia** |
|---|---|---|---|
| | [kg] | [%] | [MJ] |
| Szár+ címer | 1965 | 33 | 8057 |
| Levél | 1867 | 31 | 9690 |
| Csuhé | 862 | 14 | 4396 |
| Csutka | 1003 | 17 | 4403 |
| Szem | 261 | 5 | 2490 |
| **Összesen** | **5958** | **100** | **29036** |

A különböző időpontokban vett tárolt kukoricaszár-minták szárazanyag tartalma:

**3. táblázat**

| **Mintavétel időpontja** | **Szárazanyag-tartalom** |
|---|---|
| | [%] |
| Október | 43 |
| November | 53 |
| December | 57 |
| Január és február | 71 |

Az adatokból megállapítható, hogy a kukoricaszár megfelelő tárolás mellett történő természetes száradása igen jelentős.

## BIOAMASSZÁBÓL NYERHETŐ HŐENERGIA ELŐÁLLÍTÁSÁNAK MŰSZAKI VIZSGÁLATA

A biomassza közvetlen elégetése történhet :

- a biomassza közvetlen tűztérbe juttatásával,
- tömörítést követő égetéssel (bála-, apríték -, biobrikett- vagy pellettüzeléssel),
- illetve termikus elgázosítással.

*A biomassza közvetlen tűztérbe juttatása:*

Az energetikai hasznosítás legegyszerűbb és az energiamérleg szempontjából is a legkedvezőbb változata az eredeti, vagy az eredetihez közeli állapotban történő energetikai

felhasználás. A biomassza ily módon való eltüzelése a magas szállítási és tárolási költségek miatt gazdaságtalan annak ellenére, hogy előkészítési munkát – az esetleges szárításon kívül – , nem igényel.

*Tömörítéssel történő előkészítés:*
Célja a térfogati sűrűség növelése, ami kedvezően befolyásolja a tárolás helyigényét, a rakodás és a szállítás feltételeit és a tüzelés szabályozását. A tömörítés történhet bálázással, brikettálással vagy pelletálással. A biomasszát eredeti vagy aprítást és homogenizálást követő állapotban lehet tömöríteni.

*Termikus elgázosítás:*
A biomassza közvetlen égetésének harmadik módja a termikus elgázosítás. A biomassza égése közben keletkező hő hatására bomlás megy végbe, a kigázosodás során pirolízisgázok keletkeznek. .A pirolízis gázait egy másik tűztérben égetik el további levegő beadagolásával, ahol az égés magas hőmérsékleten (1100–1250 $^{o}$C) fejeződik be.
Ennek alapján meg kell vizsgálni a mezőgazdasági hulladék hasznosíthatóságának állomásait a betakarítástól a raktározásig.

**Betakarítás**

A mezőgazdasági növényi maradványokat – így a kukorica szárát, csutkáját és csuhéját, valamint a gabonaszalmát is –, a főtermék betakarításával egy időben, vagy közvetlen azt követően kell begyűjteni, és a feldolgozás helyére szállítani. A szalma – a főtermék betakarítása után –, szálasan, kazlazva vagy bálázott formában takarítható be. A teljes betakarított szalmamennyiség mintegy 90 százaléka bálázva (kisbála, hengerbála, szögletes bála) kerül le a táblákról. A betakarításkor általánosan 15 – 20 százalék nedvességtartalmú gabonaszalma bálakazlakban jól tárolható. A tárolás során különös figyelmet kell arra fordítani, hogy csapadék a kazlakat ne érje, mivel a nedves szalma feldolgozása (brikettálása, pelletálása, égetése) költségtöbblettel jár.

A kukoricaszár gazdaságos felhasználása abban az esetben valósítható meg, ha a betakarításkori nedvességtartalma a 30 százalékot nem sokkal haladja meg. A kukoricacsutka nedvességtartalma alacsonyabb. Nedvességtartalom szempontjából nem eléggé homogén alapanyagból nem lehet egyenletes minőségű brikettet, pelletet gyártani.

**4. táblázat** A gabonaszalma és a kukoricaszár hozama, fűtőértéke és energiahozama (Kocsis Károly, 1992 [5])

| **Biomassza** | **Nedvességtartalom [%]** | **Biomassza-hozam [t/ha]** | **Fűtőérték [MJ/kg]** | **Nettó hőérték [kgOE/kg*]** | **Nettó energiahozam [kgOE/ha*]** |
|---|---|---|---|---|---|
| Gabonaszalma | 10–15 | 1,5–3,5 | 15,3–16,2 | 0,29–0,31 | 435–1085 |
| Kukoricaszár | 30–40 | 3,5–5,5 | 10,2–12,4 | 0,19–0,24 | 665–1320 |

*80% hatásfok mellett

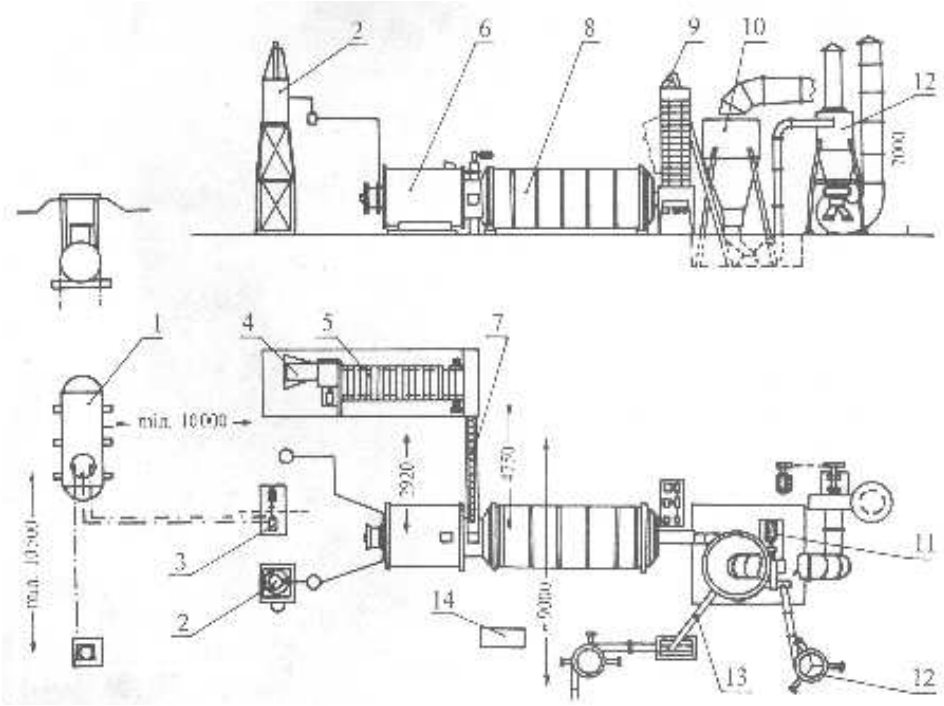
Meg kell jegyezni, hogy a kukoricaszár nedvességtartalma elérheti az 53 % is.

**Szárítás**

A brikettáláshoz, pelletáláshoz vagy a közvetlen hőenergetikai felhasználáshoz, tüzeléshez előírt nedvességtartalom beállítása szárító üzemekben történik. Erre leginkább alkalmas berendezések a zöldtakarmány-szárítók.

A forgódobos zöldtakarmány-szárítók a legkedvezőbb fajlagos hőfelhasználással rendelkeznek. Előnyük, hogy a mezőgazdasági üzemekben egyéb szárítási célokat is szolgálnak, tehát a beruházási költségük több termékre megoszlik. Járulékos beruházási igényük (tűzivíztároló, épületek, útburkolatok stb.) alacsony, hiszen szabadban telepíthetők. Gépi segédberendezései (ventilátor, ciklon, kalapácsos daráló) felhasználhatók a présgépek kiszolgálásához szükséges technológiai gépláncban. Előny, hogy az üzemet kiszolgáló személyzet szakképzettsége is közel áll a biomasszát feldolgozó üzem személyzetének szakképzettségéhez.

A következő ábra egy forgódobos zöldtakarmány-szárító üzem technológiai folyamatábráját mutatja:




2. ábra Forgódobos zöldtakarmány-szárító üzem
1 – olajállomás, 2 – tüzelőberendezés, 3 – szivattyúház, 4 – szecskavágó, 5 – behordó, 6 – kemence,
7 – ferde felhordó, 8 – szárítódob, 9 – hűtőtorony és hűtőciklon, 10 – szecskaciklon, 11 – daráló,
12 – lisztciklon, 13 – szemestermény-szárító, 14 – vezérlőszekrény

A bálázott növényi szárrészek a környezeti levegővel is száríthatók. Itt igen lényeges a bálák tömörsége, általában 100 kg/m$^3$ térfogattömeg a kedvező. A szalmabálák nedvességtartalma nem lehet magasabb, mint 30 százalék. A környezeti levegővel való szárításhoz 70 százalék relatív páratartalom alatti levegő szükséges, ekkor a szárítással kinyerhető víz 1–2 g/m$^3$, a levegő kezdeti relatív páratartalmának függvényében. A szárítási idő hosszú, 30 százalékos kezdeti nedvességtartalomnál meghaladja a 240 órát. E szárítási

mód előnye az olcsósága és egyszerűsége. Hátránya az egyenetlen száradás, a hosszú száradási idő, szakaszos jellege, bizonyos időszakokban (amikor a levegő relatív páratartalma 70–75 százalék körül van, tehát kora tavasszal és késő ősszel) használhatatlan, a szellőztető szintekre való be–, és kitárolás költséges, s kazalszárításnál fóliatakarás, szellőztető kazal alkalmazása szükséges.

A mesterséges szárítókban az alapanyag nedvességtartalmát folyamatosan mérni kell, hogy a homogenizálást és a szárítást szabályozni lehessen. A túlszárítás energiatöbbletet igényel, és ez növeli a költségeket, rontja a gyártás eredményességét. Éppen ezért ajánlatos a technológiai folyamatba már légszáraz anyagot bevinni, mely előzőleg fedett, de levegő járta helyen pihent. A mesterséges szárítók akkor gazdaságosak, ha hulladékhővel működtethetők, vagy fűtésük a szárított mezőgazdasági melléktermék felhasználásával történik.

Egy tonna nedves szalma nedvességtartalmának 20 százalékkal való csökkentése a gyakorlatban 900–1000 MJ, azaz 250–280 kWh energiát igényel. Ugyanekkora mennyiségű nedves kukoricaszár nedvességtartalma kétszer akkora, mint a szalmáé, ezért nedvességtartalmának 40 százalékkal való csökkentésére 1800–2000 MJ, azaz 500–560 kWh energiára van szükség.

A gazdaságos szárítás és tömöríthetőség érdekében célszerű az alapanyagot a szárítás előtt megőrölni, mechanikailag feltárni. Különösen szükséges ez a kukoricaszár feldolgozása esetében, mert a szár felületét fényes, vízzáró réteg vonja be, mely jelentős mértékben akadályozza a száradást. A szálas, ömlesztett és bálázott melléktermékek aprítására azok a bálabontók (pl. az ún. univerzális dézsás őrlők) alkalmasak, melyek rostával ellátott kalapácsos forgórésszel rendelkeznek.

A szalma és a kukoricaszár, -csutka, -csuhé további feldolgozásához, préseléséhez szükséges, hogy az alapanyagok ne tartalmazzanak szilárd idegen anyagokat, pl. fémet, követ. Az idegen anyagok eltávolítására rostákat és mágneses fémleválasztót kell alkalmazni.

## Préselés

A tömörítés présgépekben történik. A biobrikett előállításához kötőanyagot nem használnak, a szemcséket hideg tömörítés esetén a súrlódásos kapcsolatok tartják össze, a meleg eljárás során ezen túl az alapanyagban végbemenő kémiai elváltozások is szerephez jutnak.


3. ábra

A pellet a brikettnek egy speciális változata, előállításának technológiáját eredetileg takarmány készítésére fejlesztették ki. A pellet igen jó tulajdonságokkal rendelkező energiahordozó. Alacsony nedvességtartalmú növényi eredetű hulladék, amit darálás után nagy nyomáson és magas hőmérsékleten átsajtolnak egy 6-8 mm átmérőjű nyíláson. Az így kapott rudacskákat nevezzük pelletnek.

A gabonaszalma, kukoricaszár, -csuhé és -csutka más mezőgazdasági melléktermékkel, biomasszával együtt történő pelletálásának elvileg és a gyakorlatban nincs akadálya. Ebben az esetben külön technológiai lépésként jelentkezik a komponensek összekeverése, mely azonban nem jár jelentős költségnövekedéssel. Ha a keverés a pelletálás technológiai paramétereire kedvező hatással van, könnyen előfordulhat, hogy gazdaságos alkalmazni. Erre nézve a gyártók nem adnak tájékoztatást, mivel a technológiai paraméterek üzemi titkot képeznek.

A biomassza tömörítésének – brikettálásának vagy pelletálásának –, legfontosabb fázisa a préselés. A présgépek számos változata alakult ki, ezek általában egy-egy biomassza speciális tulajdonságaihoz igazodnak. Közös jellemzőjüket meghatározza az a tény, hogy a présgépekben a 800 bar feletti nyomáson, és az ekkora nyomáson létrejövő 80–150$^{o}$C hőmérsékleten az anyagrészecskék idegen kötőanyag nélkül is egymáshoz kötődnek. A gépből kijövő, 60–80$^{o}$C hőmérsékletű anyagot le kell hűteni.

A felhasznált biomasszák eltérő fizikai jellemzőik (sűrűség, térfogattömeg stb.) és összetételük miatt nem egyformán préselhetők. Az egyes préstípusok alapanyagokkal szemben támasztott követelményei különbözőek lehetnek. A legtöbb géptípusnál a feldolgozandó biomassza nedvességtartalmának maximuma 10–14 százalék között van.

A présgépek főbb részei: a présfej, a tömörítő szerkezet (dugattyú, csiga, görgő) és a préshüvely. A présfej hűtése vagy fűtése, valamint a préshüvely kiképzése döntő az optimális hőmérséklet és préselési nyomás kialakítása szempontjából. A présgépek villamosenergia felhasználása meglehetősen nagy, a présgépek motorteljesítménye 30–180kW, fajlagos villamosenergia felhasználásuk 50–150kWh/t.

A dugattyús és csigás présgépek elvi megoldásukat tekintve annyiban különböznek egymástól, hogy a biomassza szállítását és tömörítését egyikben dugattyú, másikban csiga végzi. Mindkét présfajta ikresített változatban is üzemeltethető.

Préselés után a termékek fizikai jellemzői különbözőek lehetnek, a biobrikett összetétele egy kutatási eredmény szerint az alábbi:

**5. táblázat** A biobrikettek főbb fizikai és tüzeléstechnikai jellemzői ([6]Janzsó, 1989)

| **Alapanyag** | **Sűrűség [kg/m$^3$]** | **Nedvesség-tartalom [%]** | **Fűtőérték [MJ/kg]** | **Hamu-tartalom [%]** |
|---|---|---|---|---|
| Gabonaszalma | 1130–1370 | 6,3 | 15,42 | 8 |
| Kukoricaszár | 1290–1310 | 6,2 | 15,49 | 6 |

A brikett (pellet) gyártásához szükséges gépek, berendezések terén a hazai ipar jelentős fejlesztéseket végzett az elmúlt két évtizedben. Ugyanakkor a pelletáló berendezések fejlesztése és hazai gyártása nem hozott látványos eredményt, a hazai pelletáló üzemek import présgépekkel működnek.

**Csomagolás, tárolás**

A biobrikett és pellet nedvszívó tulajdonságából következik, hogy tárolásuk és a csomagolásuk fokozott figyelmet igényel. Amennyiben lakossági igények kiszolgálása a cél, akkor 25-50 kg-os egységcsomagolás (zsák, papírdoboz stb.) alakítható ki. Nagyüzemi felhasználásnál konténerekben történik a szállítás.

Csomagolóanyagként célszerű természetes anyagokat, papírzsákokat használni, tekintettel arra a tényre, hogy a csomagolóanyagokat általában elégetik. A műanyag alapú csomagolóanyag égetésével a környezet súlyosan szennyeződik.

# ENERGIAMÉRLEG ELKÉSZÍTÉSE A FENT LEÍRTAK FIGYELEMBE VÉTELÉVEL

A kukoricacsutka és -csuhé, valamint gabonaszalma alapú biomasszák energetikai célból történő felhasználása rendkívül időszerű feladat. E téren az elmúlt évtizedekben jelentős kutatások, fejlesztések történtek, ugyanakkor számos kérdés még megoldásra vár.

Jelen energetikai elemzésben külön kell választani a biomassza elégetésének közvetlen módját a préselés utáni elégetéstől.

Közvetlen eltüzelés esetén magasak a szállítási és tárolási költségek, és a tüzelés hatásfoka az alacsony égési hőmérséklet miatt rossz. A szálas anyag aprításához és szárításához energiára van szükség.

Préselés utáni elégetés esetén ugyan alacsonyabbak a szállítási és tárolási költségek, de a szálas termék aprításához és szárításához itt is jelentkező energiaigényen túl, jelentős mennyiségű energiát igényel a brikettálás, vagy még inkább a pelletálás.

Az alábbiakban összefoglalom a pelletek felhasználásának energiamérlegét, figyelembe véve a pellet előállításának energiaigényét, és a pellet energiatartalmát. Az energiamérleget elkészítettem pellet felhasználása és közvetlen tüzelés mellett.

Számításaim során a következő átlagos adatokból indultam ki:
A melléktermékként keletkező (bálázott) szalma piaci ára **3000 Ft/tonna**,
a melléktermékként keletkező (bálázott) kukoricaszár ára **4000 Ft/tonna**,
a házak fűtésére szolgáló energia ára **3,1 Ft/MJ** (240.000 Ft/év per 80.000 MJ/év),
a földgáz ára (2008. január 1-jétől hatályos GKM rendelet) **2,7 Ft/MJ**,
a villamos energia ára (ELMŰ, 2008. január) 43,2 Ft/kWh, azaz **12 Ft/MJ**.

A nyersanyag árának energia-egyenértékké történő átszámításakor, valamint a tüzelőanyag fűtőértékének ár-egyenértékké történő átszámításakor a házak fűtésére szolgáló energia árával számoltam.

A szárítás hőigényének ár-egyenértékké történő átszámításakor figyelembe vettem, hogy a szárítás közvetlen hőfelhasználással történik, ezért – földgáztüzelésű szárítót feltételezve –, a földgázból nyerhető energia árával számoltam.

A pelletálás energiaigényének ár-egyenértékké történő átszámításakor figyelembe vettem, hogy a pelletálás közvetlen villamos energia felhasználással történik, ezért a villamos energia árával számoltam.

Az alábbi táblázatban összefoglalom a pellet tüzelés gazdaságossági számításainak eredményét, mely a fentiekben ismertetett kiindulási adatokra és meggondolásokra épült. A táblázat első fele energetikai adatokat, a második fele áradatokat tartalmaz [7].

**6. táblázat**

| | | Gabonaszalma | | Kukoricaszár | | Kukoricacsutka | |
|---|---|---|---|---|---|---|---|
| | | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. |
| | | 15% | 20% | 52% | 65% | 35% | 40% |
| Nyersanyag ára | MJ/kg | 1,3 | 1,4 | 1,7 | 2,3 | 1,5 | 1,6 |
| Szárítás 10%-ig | MJ/kg | 0,3 | 1,3 | 3,6 | 6,1 | 1,7 | 3,3 |
| Pelletálás | MJ/kg | 1,4 | 1,4 | 1,6 | 1,6 | 1,6 | 1,6 |
| *Összesen* | *MJ/kg* | *3,0* | *4,1* | *6,9* | *10,0* | *4,8* | *6,5* |
| Fűtőérték | MJ/kg | 13,5 | 13,5 | 13,0 | 13,0 | 13,5 | 13,5 |
| Költséghányad | % | 22 | 30 | 53 | 77 | 36 | 48 |
| | | | | | | | |
| Nyersanyag | Ft/kg | 3,0 | 3,2 | 4,0 | 5,5 | 4,0 | 4,3 |
| Szárítás 10%-ig | Ft/kg | 0,81 | 3,51 | 9,72 | 16,47 | 4,42 | 5,28 |
| Pelletálás | Ft/kg | 16,8 | 16,8 | 19,2 | 19,2 | 19,2 | 19,2 |
| *Összesen* | *Ft/kg* | *20,61* | *23,51* | *32,92* | *41,17* | *27,62* | *28,78* |
| Fűtőérték | Ft/kg | 41,85 | 41,85 | 40,3 | 40,3 | 41,85 | 41,85 |
| Költséghányad | % | 49 | 56 | 81 | -2 | 65 | 68 |

A biomassza hőenergiájának hasznosítására lehetőség kínálkozik olyan módon is, hogy a biomasszát közvetlenül, pelletálás nélkül vezessük a tűztérbe. Ebben az esetben a pelletáláshoz szükséges energia illetve költség nem terheli a folyamatot, ugyanakkor a technológia más területen (pl. szállítás, tárolás) bonyolódik.

Az alábbi táblázatban összefoglalom a közvetlen (pelletálás nélküli) tüzelés gazdaságossági számításainak eredményét, mely ugyancsak a korábbiakban ismertetett kiindulási adatokra és meggondolásokra épült. A táblázat első fele energetikai adatokat, a második fele áradatokat tartalmaz.

**7. táblázat**

| | | Gabonaszalma | | Kukoricaszár | | Kukoricacsutka | |
|---|---|---|---|---|---|---|---|
| | | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. | Átlagos betakarítási nedv.tart. | Legnagyobb betakarítási nedv.tart. |
| | | 15% | 20% | 52% | 65% | 35% | 40% |
| Nyersanyag | MJ/kg | 1,3 | 1,4 | 1,7 | 2,3 | 1,5 | 1,6 |
| Szárítás 10%-ig | MJ/kg | 0,3 | 1,3 | 3,6 | 6,1 | 1,7 | 3,3 |
| *Összesen* | *MJ/kg* | *1,6* | *2,7* | *5,3* | *8,4* | *3,2* | *4,9* |
| Fűtőérték | MJ/kg | 13,5 | 13,5 | 13,0 | 13,0 | 13,5 | 13,5 |
| Költséghányad | % | 12 | 20 | 41 | 65 | 24 | 36 |
| | | | | | | | |
| Nyersanyag | Ft/kg | 3,0 | 3,2 | 4,0 | 5,5 | 4,0 | 4,3 |
| Szárítás 10%-ig | Ft/kg | 0,81 | 3,51 | 9,72 | 16,47 | 4,42 | 5,28 |
| *Összesen* | *Ft/kg* | *3,81* | *6,71* | *13,72* | *21,97* | *8,42* | *9,78* |
| Fűtőérték | Ft/kg | 41,85 | 41,85 | 40,3 | 40,3 | 41,85 | 41,85 |
| Költséghányad | % | 10 | 16 | 34 | 54 | 20 | 23 |

Minden esetben megállapítható, hogy a kukorica alapú technológiáknál célszerű a nyersanyag természetes szárítását alkalmazni. Ha ez nem lehetséges, akkor könnyű belátni, hogy e biomasszák energetikai hasznosítása csak akkor versenyképes a jelenlegi energiahordozókkal, ha a szárítás hőenergia igényét valamilyen ún. „hulladékhővel” tudjuk

biztosítani, illetve célszerű a kukorica alapú technológiáknál a nyersanyag természetes szárítását alkalmazni.

## A LÁGYSZÁRU MEZŐGAZDASÁGI TERMÉKEK ENERGIAHASZNOSÍTÁSÁNAK GLOBÁLIS ÉRTÉKELÉSE

A biomassza energetikai hasznosításának gazdasági értékelésekor sokszor csak a hagyományos „költség – jövedelem – beruházás" jellegű módszert alkalmazzák. Eszerint minél kisebb költséggel és eszközfelhasználással minél nagyobb profitot érünk el, annál kedvezőbb lesz a befektetés. Ez tény, mégis célszerű foglalkozni a biomassza-energetikai vertikum érdekérvényesítésével, mert a jelenlegi energiaforrások készlete véges, s apadásuk a jövőbeni energiaárak további jelentős emelkedését fogja eredményezni. A magasabb energiaárak tükrében, a ma még gazdaságtalannak tűnő energiaforrások kihasználása hamar gazdaságossá fog válni, és akkor az lesz lépéselőnyben, aki már ma ebben az irányban halad.

Kukoricacsutka és -csuhé, valamint gabonaszalma hasznosításának számos gazdasági indoka van, melyek pénzértéke azonban nehezen becsülhető. Vegyük például a mezőgazdasági területek versenyképességét, új munkahelyek keletkezését vagy az ezekkel együtt járó helyi infrastruktúra és életszínvonal fejlődését. Szintén nem pénzesíthető a környezetkímélőbb tüzelés során a levegőbe jutott jóval kevesebb kén-dioxid és nitrogén-oxidok mértéke, a foszilis tüzelőanyagokéhoz képest. Továbbá nem szabad elfelejteni azt az ésszerű és megkérdőjelezhetetlen törekvés szükségszerűségét, ami a hazai energiaellátás kiszolgáltatottságának csökkentésére irányul.

Általánosan megállapítható, hogy a biomassza-energiaforrások előnyei a makrogazdaságban – környezetvédelemben, vidékfejlesztésben, energiapolitikában, hulladékgazdálkodásban –, jelentkeznek. Jelentős elterjedésük kizárólag az energiatermelők, az energiafogyasztók és az állami érdekek harmonizálásával képzelhető el.

### Irodalomjegyzék


[1] Központi Energia Hivatal 2007, http://www. eh.gov.hu

[2] Mezőgazdasági termelés 2003. Központi Statisztikai Hivatal, Budapest, 2004.

[3] MTA Talajtani és Agrokémiai Kutatóintézet 1997, http://www. taki.iif.hu

[4] dr.Horváth S., dr. Legeza L., dr. Goda T., Baranyi I., Bakosné D.M.: Kukoricacsutka és csuhé, valamint gabonaszalma, mint mezőgazdasági melléktermékek hasznosítása , Kutatási jelentés, 2005., pp:23.

[5] Kocsis Károly: A biomassza energetikai hasznosítása az agrárgazdaságban. I. Országos Agrár-környezetvédelmi Konferencia, Budapest, 1992. nov. 26–27.

[6] Janzsó J.: Mezőgazdasági és erdészeti melléktermékek hasznosítása. BIO-INNOCOR D. Budaörs, 1989.

[7] Bakosné Diószegi Mónika: Biomassza tüzelésű kazánház tervezése Diplomamunka, BME Gépészmérnöki Kar, 2006., pp:100

HADMÉRNÖK

III. Évfolyam 3. szám - 2008. szeptember

**Halász László**
Zrínyi Miklós Nemzetvédelmi Egyetem
halasz.laszlo@zmne.hu

**Hanka László**
Zrínyi Miklós Nemzetvédelmi Egyetem
hanka.laszlo@zmne.hu

**Vincze Árpád**
Országos Atomenergia Hivatal
vincze@haea.gov.hu

# A NUKLEÁRIS ERŐMŰVEK NEGYEDIK GENERÁCIÓJÁNAK ÉS EGY KORSZERŰBB REPROCESSZÁLÁSI ELJÁRÁS JÖVŐBELI ALKALMAZÁSÁNAK LEHETŐSÉGE A NUKLEÁRIS HULLADÉKOK NÖVEKVŐ MENNYISÉGÉNEK ÉS ELHELYEZÉSI PROBLÉMÁJÁNAK TÜKRÉBEN

***Absztrakt***

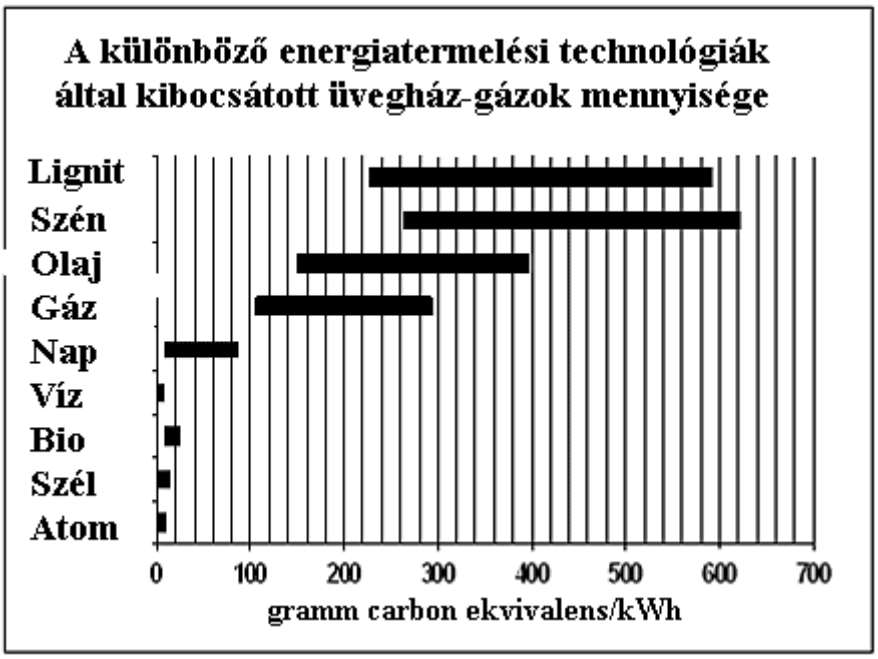
*A nukleáris energetika hosszú távon csak az erőművek új generációjának kifejlesztésével tartható fenn. Az fémolvadékkal hűtött gyorsreaktorokban – ellentétben a hagyományos termikus reaktorokkal –, gyorsneutronokkal tartják fenn a láncreakciót. Ennek köszönhetően az uránium és a nagyobb rendszámú elemek atommagjai lényegesen nagyobb százalékban hasadnak, így az urán fűtőanyag energiájának sokkal nagyobb részét lehet kinyerni. Ez a technológia felkínálja egy alternatív reprocesszálási eljárás alkalmazásának lehetőségét, melynek során a tiszta plutónium előállítása nem kerül szóba. A pyrometallurgiai eljárás során elkülöníthetőek a transzuránok, melynek köszönhetően a transzurán összetevőknek csak elenyésző mennyisége kerül a hulladéktárolókba, drasztikusan lecsökkentve ezáltal a tárolás időtartamát. Minden erőművi reaktor működése során évente több tonna hulladék keletkezik melynek tárolásáról gondoskodni kell. A jövő reaktorai újra tudják majd hasznosítani a kiégett fűtőanyagot, csökkentve ezáltal a felhalmozódott mennyiséget, de a nukleáris hulladék mennyisége az elkövetkező évtizedekben akkor is növekszik majd, ha egyetlen új termikus reaktort sem helyeznek üzembe. Már napjainkban is több nukleáris hulladék van a Földön, mint amennyit az erre kijelölt tározókban el lehet helyezni. Az Egyesül Államok kormánya ezért 1987-ben úgy döntött, hogy épít egy geológiai megőrzőhelyet a Nevada állambeli Yucca-hegy gyomrában, nagy aktivitású nukleáris hulladékok számára. Ez a létesítmény azonban biztosan nem nyílik meg 2017 előtt. Azon reaktorok lebontása, amelyek működési idejük végére értek, egyrészt új kihívást másrészt összetett feladatot jelentenek, de jelentős mértékben hozzájárulnak a nukleáris hulladékok tárolásával kapcsolatos problémákhoz.*

*A safer, more sustainable nuclear power cycle could be based on the new generation of reactors. An ALMR reactor system – in contrast with current thermal reactors –, would use fast-moving neutrons. This process permits all the uranium and heavier atoms to be consumed, thereby allowing vastly more of the fuel's energy to be captured. This technology permits an alternative recycling strategy – called pyrometallurgical process –, that doesn't involve pure plutonium at any stage. Pyroprocess collects virtually all the transuranic elements, only a very small portion of the transuranic component ends up in the final waste, which reduces the needed isolation time drastically. Each of the power generating reactors annually produces tones of debris that must be stored. Future reactors may recycle spent fuel and reduce waste, but the amount of spent fuel will rise in coming decades even if no new thermal reactors are built. There is already more nuclear waste than the currently operating repository facilities can hold. In 1987 US government decided to build a new geological repository at Yucca Mountain in Nevada for high level waste, but it won't open before 2017. Dismantling a nuclear power plant that has reached the end of its life is a new callenge and a complicated task, which operation contributes to the problem of storing nuclear waste.*

***Kulcsszavak**: Nukleáris erőmű, kiégett fűtőelemek, nukleáris hulladék, reprocesszálás, pyrometallurgiai eljárás, termikus reaktor, gyors reaktor, ALMR reaktor, plutónium és transzuránok, nukleáris hulladékok tárolása, Yucca-hegy, reaktorok lebontása ~ Nuclear power plant, spent nuclear fuel, nuclear waste, reprocessing, pyrometallurgical process, thermal reactor, fast reactor, advanced liquid metal reactor, plutonium and transuranics, repository of nuclear waste, Yucca Mountain, dismantling reactors.*

## A NUKLEÁRIS ENERGIA JELENLEGI SZEREPE A FÖLD ORSZÁGAIBAN

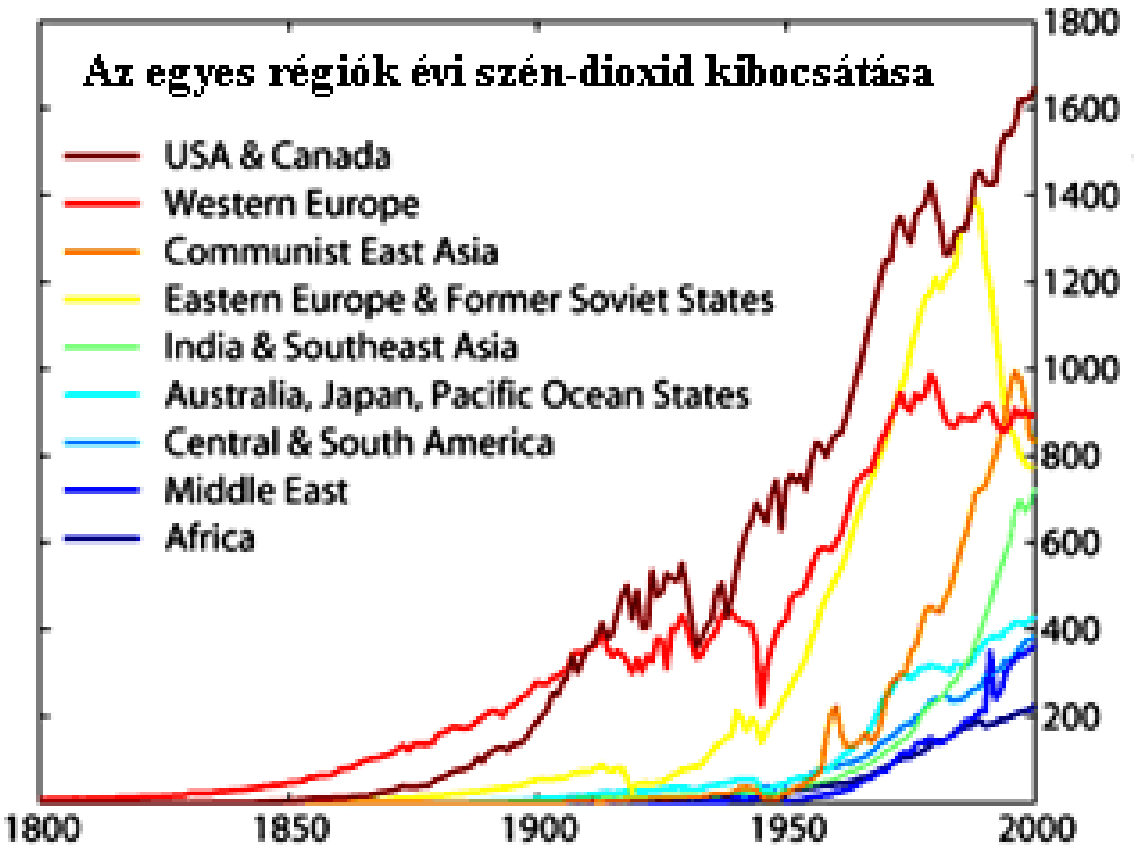
Az energiatermelés jövőjével kapcsolatosan napjaink egyik legfontosabb és a „nem szakértő publikum" által is a legtöbbet emlegetett problémája, hogy mi legyen az atomenergia sorsa a jövőben. Kérdés, hogy szükség van-e újabb erőművekre, a hagyományos típusokra vagy új generációs erőművekre, vagy éppen ellenkezőleg, ne épüljön több reaktor, sőt a meglévőket is be kellene zárni és le kellene bontani. Az iparilag fejlett és az intenzíven fejlődő országok hozzáállása a kérdéshez nagyjából egybehangzó. A szakértők a világ minden pontján egyetértenek abban, hogy az atomerőművek működtetési költsége relatíve a legalacsonyabb, továbbá az általuk termelt villamos energia is olcsóbb mint a gáz vagy széntüzelésű erőművek által termelt energia. Azt külön hangsúlyozni kell, hogy az utóbbiakkal ellentétben, a nukleáris erőművek nem szennyezik a légkört üvegházhatást okozó szén-dioxiddal. Ha manapság egy nukleáris energetikával foglalkozó mérnök vagy fizikus lelkébe látnánk, valószínűleg egy agilis természetvédőt fedeznénk fel benne. Számos környezetvédő, aki egy évtizeddel ezelőtt említeni sem volt hajlandó a nukleáris erőművek létjogosultságát, ma már alkalmanként helyeslően nyilatkozik a kérdést illetően. Az egyik legfontosabb fegyvertény, hogy az atomerőművek nem bocsátanak a légkörbe az éghajlatváltozásért felelős üvegház-gázokat (1.ábra) Természetesen nem szabad megfeledkezni az érme másik oldaláról, az erőművi balesetekről, a nukleáris hulladék tárolásának problémájáról, a gigantikus építési költségekről, a nukleáris fegyverek gyártásáról, vagy akár a lehetséges terrorcselekményekről. Ezek a problémák korántsem elhanyagolhatóak, különösen akkor, ha új erőművek építése kerül szóba. Mindezek ellenére a vezető környezetvédők részéről kissé csökkent az ellenállás az atomenergiával szemben.




1. ábra: Az egyes erőműtípusok légszennyezése $CO_2$-ekvivalens egységben [I.]

Az Amerikai Egyesült Államokban jelenleg 104 erőművi reaktor működik, tehát a Földön működő összes reaktorok egynegyede. Ennek ellenére az Egyesült Államok arra kényszerül, hogy villamos energia szükségletének a felét – a nukleáris erőművek esetén több milliárd dollárra rúgó építési költségeknél sokkal olcsóbban megépíthető, ámbár költségesebb működésű és környezetszennyező – fosszilis erőművekkel biztosítsa. Ennek az a következménye, hogy évente 2 milliárd tonna szén-dioxidot juttat a légkörbe [1].

Az 1970-es és 80-as években az előforduló üzemzavaroknak, baleseteknek, karbantartás és biztonsági átvizsgálás miatt bekövetkező leállásoknak köszönhetően az Egyesült Államok erőművei a teljes kapacitásuknak mindössze 65%-át szolgáltatták. Ma a biztonságosabb működési feltételeknek, a felhalmozódott tapasztalatoknak köszönhetően ez az arány meghaladja a 90%-ot. A szakértők véleménye egybehangzóan az, hogy a nukleáris energetika a reneszánszát éli napjainkban. Azt hangoztatják, hogy a nukleáris energetika már bizonyította alkalmasságát, hogy a 21. század energiaforrása legyen. Szerintük nem szükséges lebontani az erőműveket, nem kell elkeseredetten tiltakozni az atomenergia ellen, hanem meg kell barátkozni a gondolattal, mert a közeli jövőben nincs jobb lehetősége az emberiségnek (2. ábra).




2. ábra: A Föld egyes területein kibocsátott szén-dioxid mennyisége millió tonna/év egységben [II.]

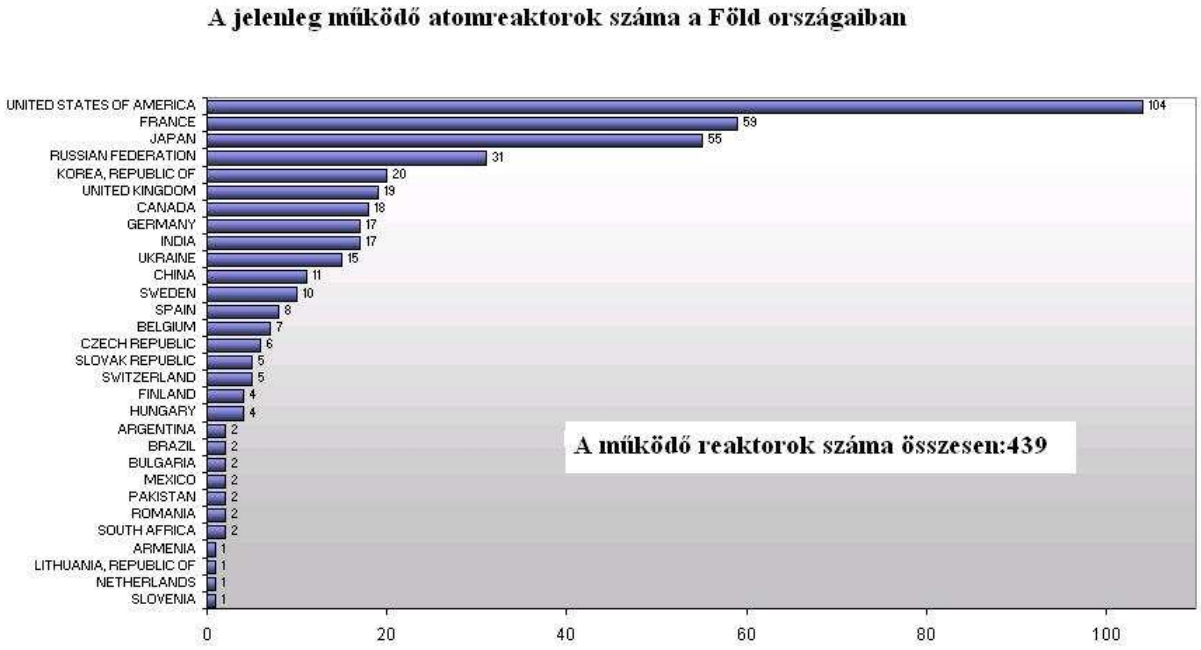
Franciaországban a teljes villamos energia szükséglet 78%-át biztosítják atomerőművekkel, az elöregedett erőműveket pedig újakkal helyettesítik. A villamos energia ipar intenzív virágzásnak indult Ázsiában is. Kínában egyre másra épülnek a széntüzelésű erőművek, és ambiciózus terveik vannak új atomerőművek építésére. Napjainkban 9 erőművi reaktoruk összesen 6600 MW teljesítménnyel dolgozik, de a tervek szerint ezt 40.000 MW-ra szeretnék növelni. Az 1,1 milliárd lakosú Indiában jelenleg 15 reaktor termel energiát és további 8 építése van folyamatban, több mint a világ bármely más országában. Az Indiai Atomenergia Hivatal hangoztatja a nukleáris erőművek üvegházhatással kapcsolatos előnyeit, a fő mozgatórugó azonban a „gigawattok iránti vágy". Balder Raj, az Indira Gandhi Atomkutató Központ igazgatója az ország energiapolitikáját röviden az alábbi módon fogalmazza: „Ha van rá mód, hogy energiát termelj, akkor mi azt mondjuk, hogy termelj olyan sokat, amennyit csak tudsz." Ezzel a politikával összefér, hogy annyi atomreaktort üzemeltetnek majd, amennyire csak lehetőségük adódik. Napjainkban is épül kettő 220 MW teljesítményű nehézvizes reaktor India délnyugati partvidékétől 30 km-re a dzsungelben a „tigris és a királykobra hazájában". Ez a két reaktor 3 millió ember energiaigényét hivatott majd fedezni. A tervek szerint e kettő mellé épül még két hasonló, a távolabbi jövőben pedig két újabb, melyek teljesítménye kétszerese lesz a most épülőknek. A teljes képhez azonban hozzátartozik az is, hogy az Indira Gandhi Központban jelenleg épül egy 500 MW teljesítményű tenyésztőreaktor is, amely 2010-ben kezdi meg működését. Ezt további 4 tenyésztőreaktor követi majd 2020-ig. Ezek arra szolgálnak, hogy az urán fűtőanyagban az urán egy részét átalakítsák plutóniummá. Így egyrészt lehetőség nyílik arra, hogy az erőművek nagyobb teljesítményűvé és nagyobb hatásfokúvá váljanak, de ugyanakkor előáll a lehetősége annak is, hogy a plutóniumból nukleáris fegyvert gyártsanak, illetve, hogy a plutónium illetéktelen kezekbe kerüljön.

## NEGYEDIK GENERÁCIÓS REAKTOROK

A nukleáris energetika biztonságával kapcsolatos, évtizedek óta tapasztalható fenntartások ellenére egyre inkább elfogadottá válik a gondolat, hogy jelen pillanatban az atomenergia az egyetlen környezetbarát módszer nagy mennyiségű villamos energia előállítására. Számos nemzet, köztük Brazília, Kína, Egyiptom, Finnország, India, Japán, Pakisztán, Oroszország, Dél Korea, Vietnam vagy tervezi atomerőművek építését, vagy ezek építése már folyamatban van. Érdekes, hogy ez a globális tendencia nem érvényesül az Egyesült Államok energiapolitikájában, ott ugyanis az utolsó ilyen projekt több mint 30 éve kezdett megvalósulni. Azonban még az atomenergia elkötelezett hívei is egyetértenek abban, hogy a jövőben csak új típusú, a hagyományos termikus reaktoroktól eltérő szerkezetű reaktorok alkalmazásának van perspektívája. Ha a tervek megvalósulnak, két-három évtized múlva az atomipar olyan negyedik generációs erőműveket üzemeltet majd, melyek magasabb hőmérsékleten, nagyobb hatásfokkal működnek. Ezek az urán fűtőanyag nagyobb hányadát hasznosítják a lánc-reakcióban, így egyrészt több energiát termelnek majd, másrészt – és ez legalább annyira fontos tulajdonság –, a nagyobb hatásfokú lánc-reakciónak és a reaktor termikustól eltérő szerkezetének, működésének köszönhetően a nukleáris hulladékok mennyisége és aktivitása is csökkenni fog, így rövidebbé válik a hulladékok tárolásának minimálisan szükséges időtartama. A tervek szerint ezeknek a reaktoroknak sokkal áttekinthetőbb lesz a biztonsági rendszere és kevésbé kifinomult vezérlést igényelnek majd.

Az új fejlesztéseknek köszönhetően a nukleáris energetika – melynek forrásai gyakorlatilag kimeríthetetlenek –, fenntarthatónak látszik a jövőben, anélkül, hogy ez az energiatermelő tevékenység hozzájárulna a klímaváltozásokhoz. A nukleáris technológia fejlesztéseinek köszönhetően úgy tűnik, a nukleáris ipar és a Föld lakossága megszabadulhat a jelenlegi technológia hátrányaitól, a reaktorbalesetektől, a nukleáris fűtőanyag és hasadási termékeinek proliferációjától, a nukleáris hulladékok kezelésének problematikájától.

Az innovációnak két aspektusa van [2]. Egyrészt kidolgoztak egy korszerűbb reprocesszálási módszert az ún. pyrometallurgiai eljárást, melynek során magas hőmérsékleten ismét alkalmassá teszik a reaktorban keletkezett kiégett fűtőelemet arra, hogy egy reaktorban ismét fűtőanyagként legyen alkalmazható. Ehhez azonban – és ez a fejlesztés másik iránya –, erre alkalmas, gyors neutronokkal is működő új típusú reaktorokra van szükség. A hatékony láncreakció létrejöttének feltétele, hogy a neutronok vagy lassúak (termikusak) vagy nagyon gyorsak legyenek. A termikus neutronok kinetikus energiája $E_{term} = 0{,}004\text{aJ} = 4 \cdot 10^{-21}\text{J}$, míg a gyors neutronoké $E_{gyors} = 0{,}3\text{pJ} = 3 \cdot 10^{-13}\text{J}$, tehát a két energia között van 8 nagyságrend eltérés. A Földön jelenleg működő energetikai reaktorok túlnyomó része, 439 db, termikus reaktor. (3.ábra) Ezekben a fűtőanyag az urán 235 tömegszámú izotópja, az ún. hasadóanyag („fissile”), amely nagy valószínűséggel elsősorban termikus neutronok hatására hasad. A természetes urán azonban nagyobb részben, ~99,3%-ban tartalmazza a nagyobb tömegszámú U-238 izotópot, amely termikus neutronokkal „csak hasítható” („fissionable”), de a termikus hasítás esélye jelentősen kisebb, sokkal nagyobb valószínűséggel hasad gyors neutronok hatására. További fontos sajátja ennek az izotópnak, hogy befoghat úgy neutront, hogy ennek következtében nem jön létre hasadás, hanem 239 tömegszámú plutónium izotóp keletkezik. A Pu-239 azonban az U-235 izotóphoz hasonlóan hasadóanyag, alkalmazása esetén biztosítva van az önfenntartó láncreakció. A termikus reaktorok viszonylag olcsón, jó hatásfokkal termelik a villamos energiát, de komoly hátrányuk, hogy szerkezetükből adódóan nem lehet csökkenteni a működés során keletkező radioaktív hulladék mennyiségét.




3. ábra: Atomreaktorok a Föld országaiban [III.]

Egy termikus erőmű üzemelése során a fűtőanyagban a nagy tömegszámú hasadóanyag(ok) atomjainak száma csökken, a fűtőelem „kiég". Egy új fűtőelem dúsított uránt tartalmaz amelyben az U-235 aránya 3-5% körüli érték a konkrét típustól függően. Ez az arány a reaktor 3 évi működése során nagyjából 1%-ra csökken. Ekkor az U-235 lecsökkent mennyisége és a sugárzás okozta anyagszerkezeti változások miatt a fűtőelemet a reaktorból el kell távolítani. Hangsúlyozzuk, hogy ebben az állapotban az U-238-ból termelődött Pu-239 izotóp hasadása már több mint 50%-át szolgáltatja a fűtőelem által termelt összes energiának. Mindent egybevetve, amikor a technikusok eltávolítják a reaktorból a „kiégett" fűtőelemet, az még tartalmazza a kezdetben benne levő, hasadásra képes atomok 95%-át. Másképpen fogalmazva, a fűtőelem eltávolításakor, a benne rejlő nukleáris energiának mindössze 5%-a hasznosult. Ehhez még hozzátartozik az is, hogy a bányából kitermelt uránércnek mindössze egytizede alakul át nukleáris fűtőanyaggá a dúsítási eljárások során. E két adatot egybevetve az adódik, hogy a napjainkban működő termikus erőművi reaktorokban a kitermelt uránércben rejlő energiának kevesebb mint 1%-a hasznosul [2].

Ha ezekre a számadatokra gondolunk, nem meglepő, hogy sok tudósban megérlelődött a gondolat, miszerint a „kiégett" fűtőelemek még alkalmasak lennének további energiatermelésre. Ha figyelembe vesszük, hogy a Föld uránkészletei végesek, továbbá azt, hogy az egyre növekvő számú termikus reaktor néhány évtizeden belül kimeríti a rendelkezésre álló készleteket, akkor nyilvánvalónak tűnik az igény, hogy a kiégett fűtőelemektől, a nukleáris hulladéktól illetve a dúsítási eljárás során keletkező meddőtől nem megszabadulni kell, hanem alkalmas folyamatokkal újra hasznosíthatóvá kell tenni azokat.

A kiégett fűtőanyag alkotórészei lényegében három osztályba sorolhatók. A hasadási termékek a nehéz magok hasadása során keletkező kisebb tömegszámú elemek atommagjai. Ezek keveréke nem haladja meg a fűtőelem teljes mennyiségének 5%-át. Ennek ellenére a hasadási termékek jelentik egyrészt a tényleges nukleáris hulladékot, mely különösen az első néhány évtizedben számottevően radioaktív. Az első évtized elteltével azonban a legtöbb izotóp gyakorlatilag elbomlik, a maradék aktivitás dominánsan két komponenstől, a Cs-137 és a Sr-90 izotóptól származik (1.táblázat). Mindkét anyag vízben oldható, így nagyon körültekintő módon kell megoldani a hosszú távú tárolás problémáját. Nagyjából 300-500 év elteltével csökken az aktivitás a kezdeti aktivitás szintjének 1/1000 része alá, innentől tekinthető a nukleáris hulladék veszélytelennek.

| Néhány hasadási termék radiológiai tulajdonságai | | | | |
|---|---|---|---|---|
| Rendszám | Ismert izotópok száma | Izotóp | Felezési idő | A radioaktív bomlás típusa |
| 27 | 29 | Cobalt-60 | 5,27 év | béta, gamma |
| 38 | 33 | Stronciumr-90 | 28,1 év | béta |
| 39 | 33 | Yttrium-90 | 2,66 nap | béta |
| 53 | 37 | Jód-131 | 8,02 nap | béta, gamma |
| 55 | 40 | Cézium-137 | 30,23 év | béta, gamma |
| 77 | 36 | Iridium-192 | 73,8 nap | béta, gamma |
| 84 | 33 | Polónium-210 | 138,37 nap | alfa, gamma |
| 86 | 34 | Radon-222 | 3,823 nap | alfa |
| 88 | 29 | Radium-226 | 1590 év | alfa, gamma |

1. táblázat

Néhány hasadási termék radiológiai tulajdonságait tartalmazza a táblázat. Tartalmazza még a táblázat a jelenleg ismert egyéb izotópok számát is, melyek 1-2 kivétellel szintén radioaktívak

A kiégett fűtőelem legszámottevőbb része maga az uránium, részaránya a teljes mennyiségnek körülbelül a 94%-a. Ez a fűtőelemben kezdetben meglevő uránium el nem hasadt része. Ebben az állapotban az U-235 részaránya megközelíti az uránércben tapasztalható természetes ~0,71% arányt. A fűtőanyagnak ez a komponense csak kevéssé radioaktív, ha sikeresen elválasztják a hasadási termékektől és az egyéb anyagoktól, akkor alkalmas arra, hogy jövőbeli felhasználás céljára, nem túl szigorú körülmények között raktározzák.

A kiégett fűtőanyag fennmaradó és egyben legtöbb problémát okozó komponense a 89 és 104 rendszám közötti transzurán elemek, az aktinidák periódusa, melyek között a legnagyobbrészt előforduló elemek a plutónium, amerícium és kűrium. A 2. táblázatban összefoglaltuk a kérdéskör szempontjából legfontosabb transzuránok radiológiai tulajdonságait. A 2. oszlopban a jelenleg ismert izotópok számát tüntettük fel, míg a következő három oszlop a leghosszabb felezési idejű izotóp adatait tartalmazza. A táblázatból kimaradt transzuránok felezési ideje csupán néhány nap, illetve néhány óra nagyságrendű, így a tárolás, kezelés szempontjából érdektelenek. Habár a transzuránok részaránya kevesebb mint 1%, napjainkban mégis ezen elemek okozzák a nukleáris hulladékok kezelésével, tárolásával kapcsolatos legtöbb gondot és problémát. Ezen izotópok felezési ideje ugyanis több tízezer sőt több milliárd év is lehet. Ez az oka annak, hogy a nukleáris hulladékok tárolását több ezer-tízezer év időskálán kell megoldani.

| Aktinidák radiológiai tulajdonságai | | | | |
|---|---|---|---|---|
| Rendszám | Ismert izotópok száma | Izotóp | Felezési idő | A radioaktív bomlás típusa |
| 89 | 31 | Actínium-227 | 21,7865 év | béta |
| 90 | 30 | Thorium-232 | $1{,}406 \cdot 10^{10}$ év | alfa |
| 91 | 29 | Protactínium-231 | 32,788 év | alfa |
| 92 | 26 | Urán-238 | $4{,}47 \cdot 10^{9}$ év | alfa |
| 93 | 20 | Neptunium-237 | $2{,}145 \cdot 10^{6}$ év | alfa |
| 94 | 20 | Plutónium-244 | $7{,}93 \cdot 10^{7}$ év | alfa |
| 95 | 19 | Amerícium-243 | 7388 év | alfa |
| 96 | 20 | Kűrium-247 | $1{,}56 \cdot 10^{7}$ év | alfa |
| 97 | 20 | Berkelium-247 | 1379 év | alfa |
| 98 | 20 | Californium-251 | 900,6 év | alfa |
| 99 | 19 | Einsteinium-252 | 1,2922 év | alfa |

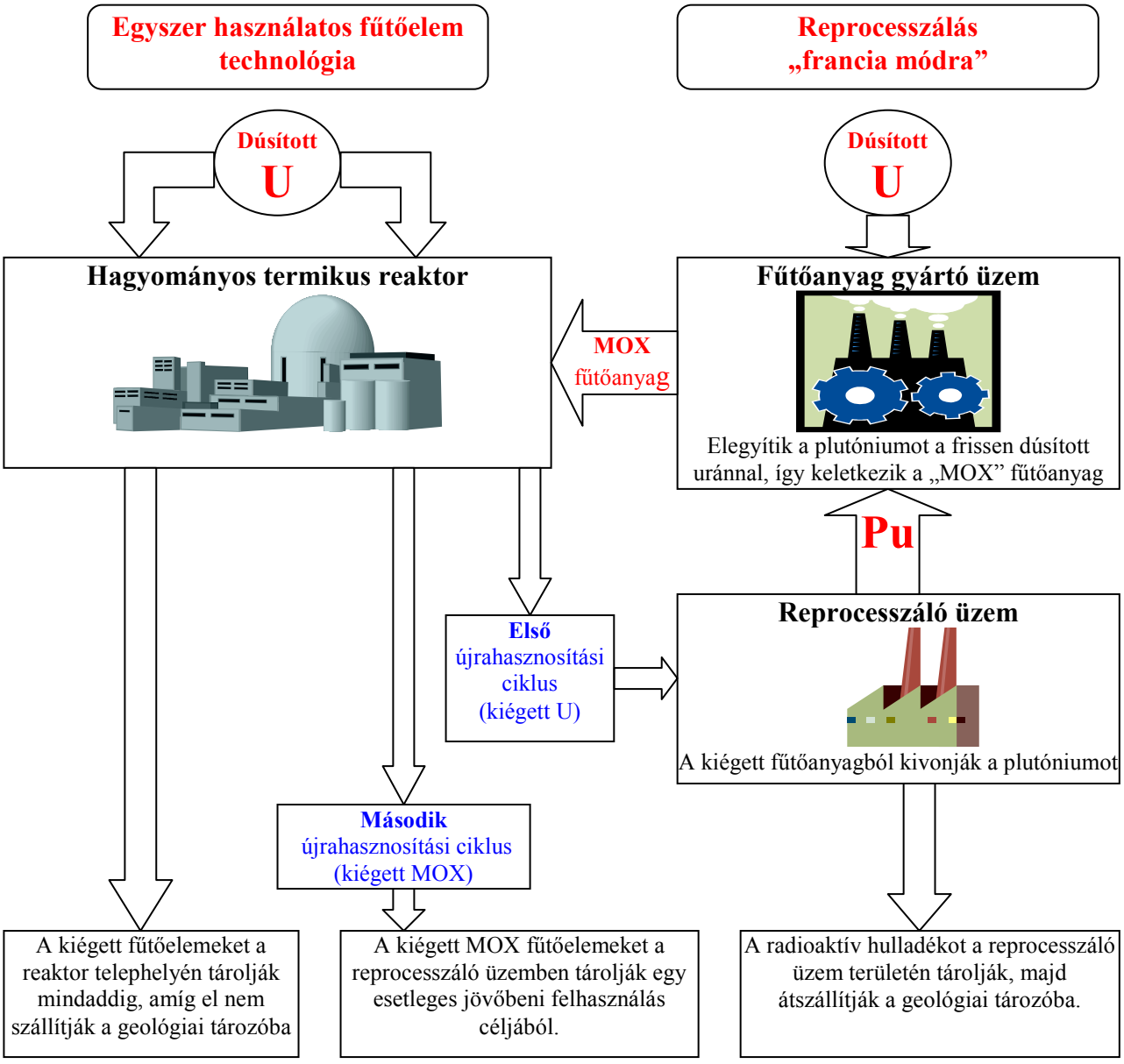
2. táblázat

# REPROCESSZÁLÁS

A termikus reaktorok fűtőanyagában keletkező plutónium reprocesszáló üzemekben elkülöníthető és alkalmazható gyors neutronokkal működő tenyésztőreaktorokban. A reprocesszálás technológiája nem újdonság. Ezen üzemek legnagyobb része Franciaországban és az Egyesült Királyságban működik továbbá 2006 óta, egy 20 milliárd $-os beruházásnak köszönhetően, már Japánban is működik egy ilyen létesítmény. Ezekben a gyors tenyésztőrektorokban, szerkezetükből adódóan, több neutron termelődik, mint amennyi a működés során elhasad. A reprocesszálás művelete kezdetben gyakorlatilag a plutónium kivonásának folyamatával volt egyenértékű. Ezt a reprocesszálási technológiát nevezik PUREX eljárásnak (*p*lutonium *ur*anium *ext*raction). A PUREX eljárást céltudatosan a fegyverek gyártásához szükséges tiszta plutónium előállítása érdekében fejlesztették ki. Azonban már a nukleáris energetika megszületését követően megfogant a gondolat a tudósokban, hogy a plutóniumot, a nagyobb hatásfok miatt, alkalmazni lehetne energetikai reaktorokban is. Azonban a plutónium kiválóan alkalmas hasadóanyag nukleáris bomba előállításához. A plutónium energiatermelési célokkal működő reaktorokban történő alkalmazása így előrevetítette a plutónium illetve a belőle előállított nukleáris fegyverek ellenőrizetlen proliferációjának problémáját. Egy nukleáris fegyver előállításához nagy tisztaságú Pu-239 izotópra van szükség. A hagyományos termikus reaktorokban alkalmazott fűtőanyag azonban számottevő mennyiségben tartalmaz egyéb izotópokat is, így közvetlen fegyvergyártásra alkalmatlan. Mindazonáltal nem elképzelhetetlen, hogy megfelelő technikai háttérrel a plutónium elkülönítése megoldható. Ennek okán Jimmy Carter 1977-ben, az Egyesült Államokban korlátozta a kiégett nukleáris fűtőanyag reprocesszálásának lehetőségét a polgári szférában. Carter elnök példát szeretett volna állítani ezzel a lépéssel a Föld többi nemzete számára. „Természetesen" voltak országok amelyek nem csatlakoztak a kezdeményezéshez. Így Franciaország, Oroszország, az Egyesült Királyság és Japán napjainkban is üzemeltet reprocesszáló üzemeket [2].

A hagyományos technológiájú reprocesszálás volumenében vezető Franciaország üzemeiben, a fűtőanyag a plutónium-dioxidnak és az U-238 oxidjának keveréke, amit röviden „MOX"-nak neveznek (*m*ixed *ox*ide). Egy kiégett MOX-fűtőelem plutónium tartalma azonban még mindig eléri a reprocesszálás eredményeként adódó koncentráció 70%-át, tehát a reprocesszálás folyamata sem biztosítja a reaktorokban a hasadóanyag hasznosítás hatásfokának jelentős növekedését. Ezek után kerül a kiégett fűtőelem a reprocesszáló üzem telephelyén kialakított megőrzőhelyre, határozatlan idejű tárolásra. Ezáltal Franciaországban a nukleáris hulladékok tárolásának problematikáját, az újrahasznosítási eljárás közbeiktatásával, egyszerűen áthelyezik az erőművek hatásköréből a reprocesszáló üzemekébe (4.ábra). Japán követi Franciaország példáját. Az Egyesült Királyság és Oroszország szintén tárolja tiszta plutónium-készleteit. A felhalmozódott nem katonai vonatkozású készletek mennyisége összesen 120 tonna volt 2005 végén. Ez nagyjából 15.000 atombomba készítéséhez elegendő. Ezek az országok azonban nem csak a saját erőműveikben keletkező kiégett fűtőelemeket alakították/alakítják újrahasznosíthatóvá, hanem exportálják is e tevékenységüket. Olyan nemzetek szállítottak/szállítanak ezen országokba kiégett fűtőanyagot reprocesszálás céljából, ahol vagy nem rendelkeznek ezzel a technológiával és a szükséges infrastruktúrával, vagy ahol a helyi antinukleáris aktivisták rábírták a kormányt – például Németországban –, hogy állítsa le az ilyen irányú tevékenységet. De világosan kell látnunk, hogy ezek az országok is csak átmenetileg oldják meg, inkább csak elodázzák ezzel összefüggő problémáikat, mert a tárolás feladatát, ha néhány évvel később is, de mindenképpen meg kell oldaniuk. A külföldön történő újrahasznosítás költségei is csillagászatiak, tonnánként 1 millió $, ami tízszerese a tároláshoz szükséges száraz konténerek előállítási költségének. Ezen okok miatt lassan megszűnik a külföldön történő reprocesszálásra vonatkozó igény. Ezért például az Egyesült Királyság azt tervezi, hogy néhány éven belül bezárja üzemeit. Az érintett területek megtisztításával, rekultiválásával kapcsolatban felmerülő költségek előreláthatólag elérik majd a 92 milliárd $-t. Oroszországban mindössze egy ilyen üzem működik, amely az országban keletkező nukleáris hulladéknak mindössze a 15%-át

képes újrahasznosíthatóvá alakítani. Tervezték, hogy bővítik a kapacitásokat, de az 1980-as gazdasági összeomlás után a tervek nem valósultak meg.




4. ábra: Az uránium alkalmazásának és kezelésének két hagyományos lehetősége.
Az „egyszer használatos fűtőelem technológia” és a PUREX eljárás alkalmazása során az urán fűtőelemek életútja, és a nukleáris hulladék kezelésének módja. [3]

Japán is elkötelezett a reprocesszálás terén, ez azonban egy kényszerhelyzet is, ugyanis Japánban nem sikerült hatóságilag engedélyeztetni a reaktorok területén a tárolókapacitás növelését. Franciaország 2000-ben még azt tervezte, hogy 2010-re bezárja az összes reprocesszáló üzemét, de ez súlyos anyagi hátrányokkal, a villamos energia termeléséből származó bevételek jelentős csökkenésével járna. Az Egyesült Államok a hidegháború idején Washington államban és Dél Carolinában működtetett egy-egy üzemet kifejezetten katonai célokkal. Ezekben a létesítményekben nukleáris fegyverekhez állítottak elő tiszta plutóniumot, mintegy 100 tonna mennyiségben. A plutónium tárolásával, kezelésével, a létesítmények további üzemeltetésével, tisztítási munkálatokkal kapcsolatosan a jövőben felmerülő költségek elérik a 115 milliárd $-t. New York államban is működött egy kizárólag polgári célokat szolgáló újrahasznosító üzem 1966-tól, ahol

„mindössze” 1,5 tonna plutónium halmozódott föl. Mivel a létesítmény működése nem volt gazdaságos, ezért 1972-ben bezárták. Az üzem átalakításával, a környezet megtisztításával kapcsolatos munkák több mint 5 milliárd $-t emésztettek fel [3].

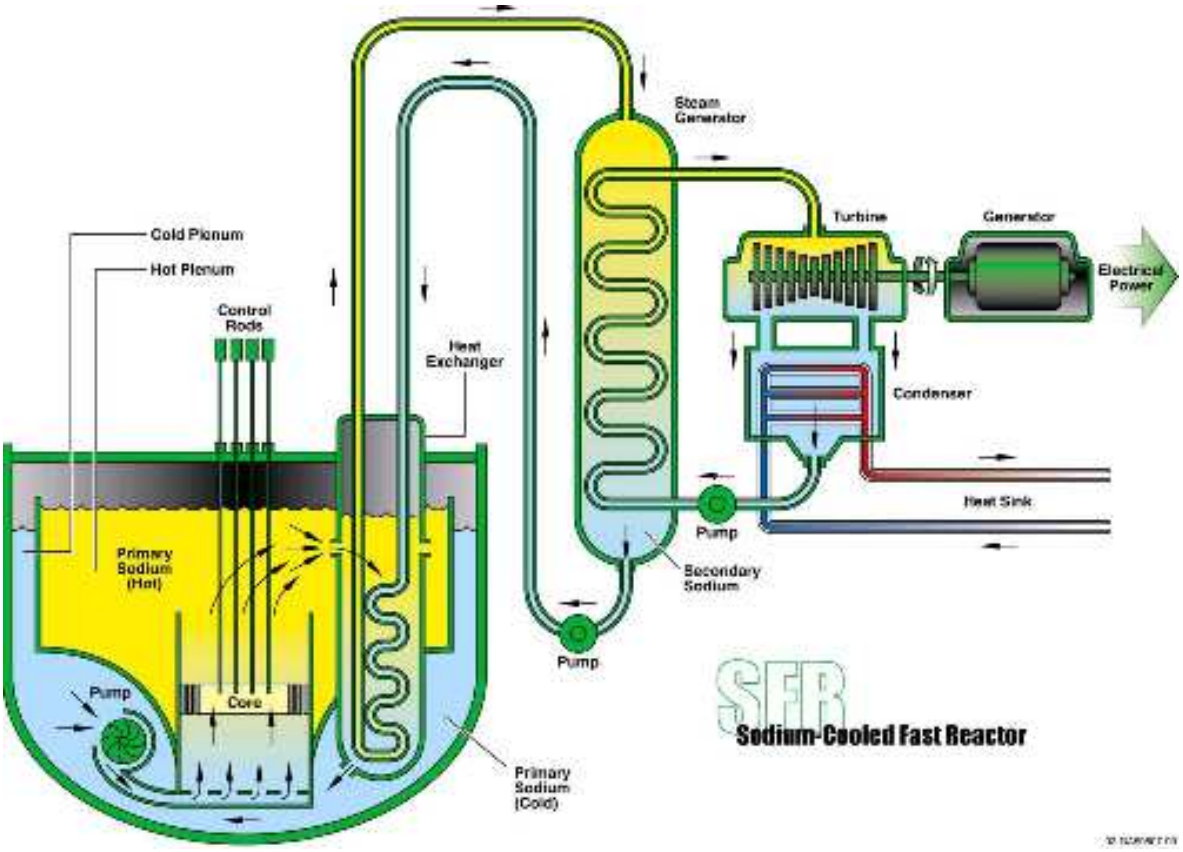
Felmerül a kérdés, hogy ilyen tetemes költségvonzatok mellett miért volt egyáltalán igény ilyen üzemek építésére és működtetésére. Az egyik ok, hogy a nukleáris ipar létét veszélyeztette az, hogy esetleg elfogynak a bányákból az uránkészletek. Ekkor azonban még csak elméletileg merült fel a plutónium proliferációjának problémája, amely később gyakorlatilag is megvalósult. 1974 májusában India felrobbantotta kísérleti plutónium bombáját, melyhez a plutóniumot a saját – mellesleg az Egyesült Államok közreműködésével felépített – reprocesszáló üzemében állította elő. A tudósok figyelmeztetés képpen ekkor emelték fel a szavukat, hogy a plutónium illetéktelenek, akár terroristák kezébe is kerülhet. Az Egyesült Államok, felismerve ennek veszélyét, a Ford-kormány kezdeményezésére, majd később a Carter-adminisztráció csatlakozásával felülvizsgálta a kérdést. A reprocesszáló üzemeket feleslegesnek sőt gazdaságtalannak minősítette és bezárta azokat, továbbá felszólította többek közt Franciaországot és Németországot, hogy szüntessék be reprocesszálási technológiájuk exportját Pakisztánba, Dél-Koreába és Brazíliába. Később Reagan elnök megpróbálta újjáéleszteni a technológiát, de mivel a súlyos költségvonzatok miatt nem volt versenyképes a hagyományos, termikus reaktorokban alkalmazott, „egyszer használatos fűtőelemek” technológiájával, az ilyen irányú tervekkel, legalábbis az Egyesült Államokban, úgy tűnik felhagytak.

A gyors reaktorok új generációja azonban egy korábbiaktól eltérő alternatívát kínál a kiégett fűtőelemek reprocesszálása terén. Ennek az újrahasznosítási folyamatnak egyetlen lépcsőjében sem kerül szóba a tiszta plutónium elkülönítése. Ezáltal az új, negyedik generációs gyorsreaktorok a minimálisra csökkentik a lehetőségét és a kockázatát annak, hogy a nukleáris fűtőanyagot fegyverek gyártására felhasználják, és jelenleg az egyetlen lehetőséget jelenti arra vonatkozólag, hogy a fűtőanyagból a maximális mennyiségű energiát kinyerjék. Ez utóbb tulajdonság annak köszönhető, hogy a gyors neutronok nagyobb valószínűséggel okoznak hasadást mint a termikus neutronok. Ez két okra vezethető vissza. Egyrészt a termikus neutronok nagyobb része abszorbeálódik, vesz részt olyan magreakciókban amely nem hasadás, másrészt a neutronok számottevő része reakció nélkül elhagyja a reaktort. A nagy kinetikus energiájú, gyors neutronok az ütközés során nagyobb valószínűséggel hasítják a nagy tömegszámú izotópokat, többek között az U-238 magot is, ami azt jelenti, hogy nem kizárólag az U-235 és a Pu-239 izotóp a „hasadóanyag”. Ennek továbbá az is egy következménye, hogy a gyors reaktorok működtetéséhez nincs szükség urándúsításra.

A termikus reaktorokban a primer körbeli víz kettős szerepet játszik. Egyrészt hűtőközeg, a víz szállítja el a fűtőelemekben keletkezett hőt a hőcserélőkbe, másrészt moderátor, tehát neutron lassító közegként is funkcionál. Innen világos, hogy gyors reaktorokban nem alkalmazható víz hűtőközegként, mert az lelassítaná a neutronokat. A gyors reaktorokkal kapcsolatos kutatások az 1950-es években kezdődtek az Egyesült Államokban. Ilyen reaktorok több típusát is kifejlesztették az elmúlt évtizedekben. Vannak köztük gázhűtésűek, és vannak olyanok amelyeket fémolvadék hűt. Az Argonne Nemzeti Laboratórium által az 1980-as években kifejlesztett típusban, amelyet alkalmasnak tartanak a közeli jövőben a széleskörű elterjedésre, folyékony nátriumot alkalmaznak hűtőközegként. Innen származik az elnevezés is: Advanced Liquid Metal Reactor, ALMR, azaz „Korszerű folyékony fémmel hűtött reaktor”. A folyékony fémnek, azon túl, hogy számottevően nem lassítja a neutronokat és nagy fajhője miatt hatékonyan szállítja el a keletkezett hőt, van egy óriási előnye a vízzel szemben. A vízhűtéses rendszerek nagyon nagy, néhány száz atmoszféra nyomáson működnek. Ennek a rendszernek komoly hátránya, hogy a primer vízkörben előálló bármely sérülés egyrészt azzal járhat, hogy a reaktorcsarnok megtelik gőzzel, a csarnokban túlnyomás keletkezhet, az épület ennek következtében sérülhet, másrészt gyorsan lecsökkenhet a reaktor hűtőközegének mennyisége. A folyékony fémmel hűtött rendszer azonban normál légköri nyomáson működik. Vízzel érintkezve azonban könnyen meggyulladhat, tehát körültekintő kezelést igényel. Megnyugtatónak tűnik azonban a kísérletekkel eltöltött évtizedek során felgyűlt jelentős mennyiségű tapasztalat, melynek birtokában a rendszert úgy fejlesztették, hogy relatíve egyszerűen

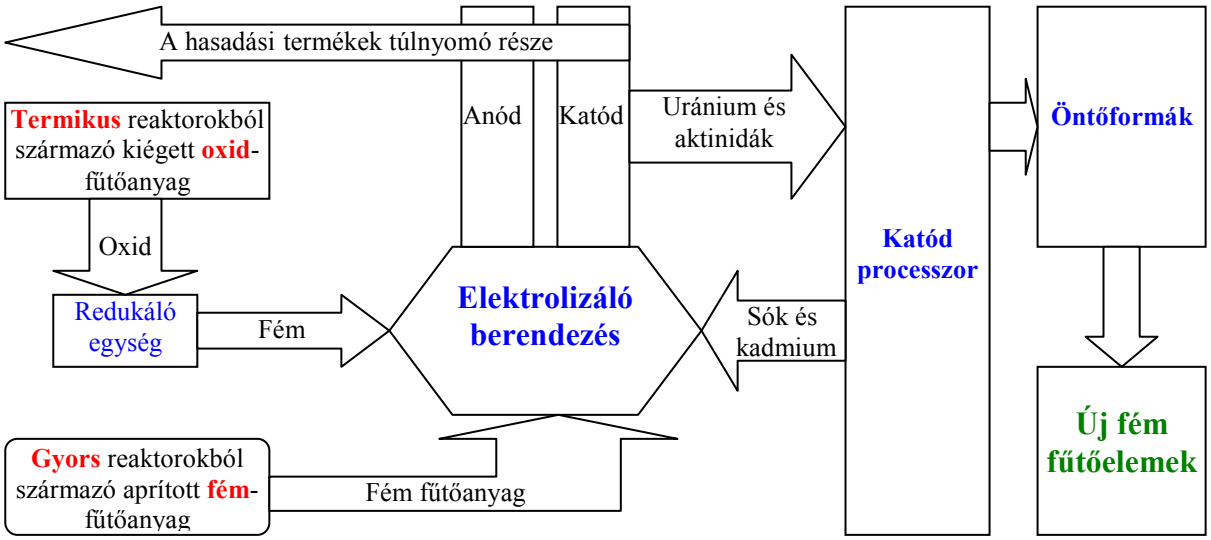
kezelhető és biztonságosan működtethető legyen. Előfordultak „természetesen” nátrium tűzesetek és valószínűleg a jövőben is előfordulnak majd. Egy ilyen eset történt 1995-ben a Monju gyorsreaktorban Japánban. Az eset azonban nem veszélyeztette a reaktorépület egységét, senki sem sérült meg és nem kapott számottevő többletdózist. A mérnökök nem tekintik a nátrium gyúlékonyságát jelentős problémának.

A termikus reaktorokban a fűtőanyag egy kerámia, az urán-oxid. Egy további eltérés ehhez képest, hogy a fémolvadékkal hűtött gyorsreaktorokban azonban a hasadóanyag fémes állapotú urán illetve plutónium és egyéb transzuránok. Az elmúlt évtizedek során számos gyorsreaktor típust kidolgoztak és tanulmányoztak, az ALMR számos előnnyel rendelkezik a többivel szemben. Egyrészt nagyobb biztonsággal működtethető, (a reaktor üzemelése során aktív biztonsági rendszerek a következők: 1. Működés közben nagy teljesítményű szivattyúk áramoltatják a folyékony fémet a primer körben. A rendszer úgy van kialakítva, hogy abban az esetben ha a szivattyú leáll a gravitáció keringteti tovább az olvadékot. 2. Ha a szivattyúk meghibásodnak, leállnak, akkor egy speciális biztonsági berendezésnek köszönhetően nagy számú neutron lép ki a reaktormagból, így szubkritikussá válik a rendszer és a hőmérséklet csökken. 3. Vészhelyzet esetén 6 db neutron elnyelő anyagból készült szabályozórúd esik a magba, így leállítja a láncreakciót. 4. Ha a láncreakció valamilyen oknál fogva mégis „megszalad”, akkor több ezer, neutron elnyelő bór-karbid–ból készült golyót juttatnak a reaktormagba, ezzel garantálva a reaktor leállását.), másrészt a többi gyorsreaktor típushoz képest nagyobb sebességgel lehet bennük reprocesszálni a kiégett fűtőanyagot, végül működése összekapcsolható a pyrometallurgiai eljárásnak nevezett újrahasznosítási folyamattal (5.ábra).




5. ábra: Folyékony nátrium hűtésű gyors reaktor szerkezete.
A reaktormagban (Core) keletkező hő a primer köri radioaktív nátriumnak (Primary Sodium) adja le a hőt közvetlenül. A hő egy közbülső hőcserélőben (Heat Exchanger) adódik át a szekunder körbeli nem radioaktív nátriumnak (Secondary Sodium). A hőt ez a közeg a gőzgenerátorba szállítja (Steam Generator) Itt adódik át a hő a harmadik körben keringő víznek, ahol az gőzzé alakul és magforgatja a tubinát (Turbine). [IV.]

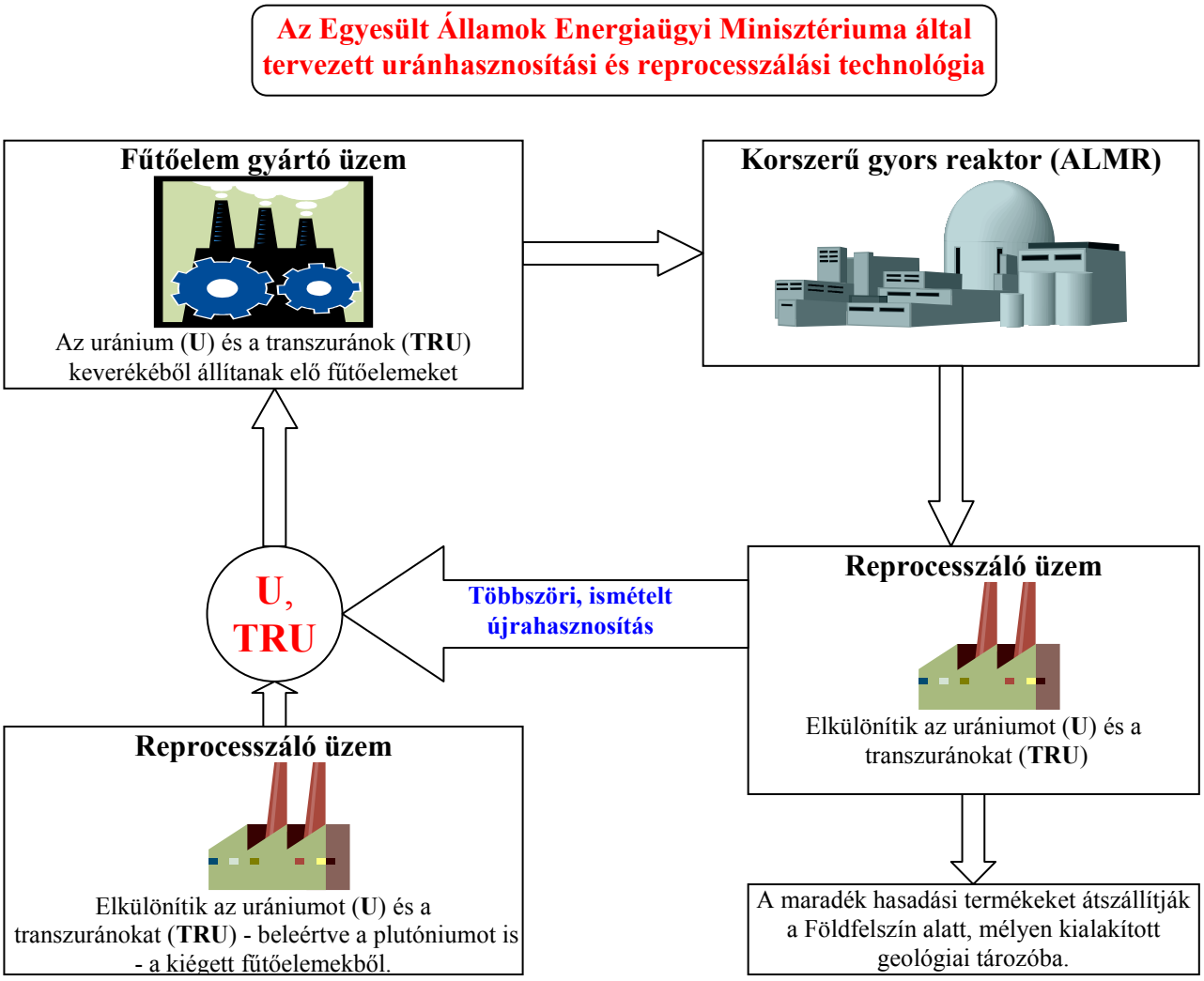
Két hasonló pyrometallurgiai reprocesszálási folyamatot is kidolgoztak, amely a kiégett fűtőelemek hasznosításának új módszere, az egyiket Oroszországban a másikat az Egyesült Államokban. Mindkettő tulajdonképpen egy elektrolízis, leglényegesebb különbség a kettő között az, hogy az oroszok kerámia, tehát oxid-formájú üzemanyagot alkalmaznak, míg az ALMR reaktorban a fűtőanyag fémes állapotú urán illetve plutónium. Utóbbi esetben a kiégett fűtőanyagot magas hőmérsékleten egy kémiai fürdőben feloldják. A gyors reaktorok fűtőelemei felaprítás után közvetlenül az elektrolizáló berendezésbe, egy magas hőmérsékletű kémiai fürdőbe kerülnek. A termikus reaktorok kiégett fűtőelemei pedig egy közvetett redukciós átalakítás után, szintén már fémes állapotban jutnak el az elektolízisig. Erős villamos árammal elektrolizálva az oldatot, a katódon – amely egy fém elektróda –, kiválik az urán, a plutónium és a többi transzuránok, tehát nem kizárólag a plutónium. Ebből a keverékből a „katód processzor" kivonja a sókat és a kadmiumot. Ezeket az anyagokat újra hasznosítják. A hasadási termékek jelentős része és elenyésző mennyiségű uránium és aktinida az oldatban marad. Ha az elektródára kellő mennyiségű anyag kivált, a technikusok eltávolítják azt az oldatból, leolvasztják róla a kivált keveréket, öntőformába töltik, majd lehűtik. Ha az oldat a hasadási termékekre vonatkozólag telítetté válik, akkor elkülönítik ezek keverékét az oldószertől és a végleges tárolóhelyre továbbítják. Végül pedig az uránium-aktinida keverék egy öntőberendezésbe kerül, ahol gyors reaktorok számára fűtőelemekké formálják. Az alkalmazott folyamatok áttekintését segíti elő a 6. ábra. A pyrometallurgiai eljárás során tehát hatékonyan szétválasztják az uránt és a transzuránokat – beleértve a plutóniumot is –, a hasadási termékektől. A transzuránoknak csak egy elenyésző hányada kerül így a hasadási termékekkel együtt nukleáris hulladék tárolókba, drasztikusan lecsökkentve így a biztonságos, elszigetelt tárolás minimálisan szükséges időtartamát.




6. ábra: Reprocesszálás pyrometallurgiai eljárással [2]

Az uránnak és a transzuránoknak az elektrolízis során keletkező keveréke teljesen alkalmatlan mind fegyverek előállítására, mind pedig arra, hogy termikus reaktor üzemanyagául szolgáljon, kiválóan alkalmas viszont arra, hogy egy gyors reaktor, az ALMR fűtőanyaga legyen. Az eljárás még nem alkalmas arra, hogy segítségével ipari méretekben állítsanak elő villamos energiát, mindazonáltal demonstrációs céllal mind az Egyesült Államokban mind pedig Oroszországban sikeres és biztató kísérleteket végeztek.

Az urán és a transzuránok jövőbeli, tervezett felhasználásának, kezelésének folyamata követhető végig a 7. ábrán.




7. ábra: Energiatermelés és reprocesszálás gyors (ALMR) reaktorok alkalmazásával [3]

Összehasonlítva a termikus és a gyors reaktorok működését, azokban számos hasonlóságot fedezhetünk fel, viszont bizonyos téren óriásiak a különbségek. Tekintsünk például egy 1000 MW elektromos teljesítményű termikus reaktort. Ennek működése során évente átlagosan 100 tonna radioaktív hulladék keletkezik, mely aktivitásához számottevő módon hozzájárulnak a transzuránok. Ezzel szemben egy gyors reaktor, ugyanekkora villamos teljesítményt számításba véve „mindössze” 1 tonna hulladékot termel, melyben csak nyomokban vannak transzuránok. Ennek köszönhetően jelentősen kevesebb gondot okoz a nukleáris hulladék tárolása. Mivel az ALMR reaktor működése során keletkező nukleáris hulladékban nincsenek nagyon hosszú felezési idejű aktinidák, a termikus erőművek hulladékainak tárolásához szükséges több tízezer év tárolási idő lecsökken néhány száz évre. Ennyi idő elteltével ugyanis, a hulladék aktivitása lecsökken az uránérc aktivitásának szintjére.

A 3. táblázatban összefoglaltuk a két, gyakorlatban már működő eljárás, illetve a tervezett uránhasznosítási technológia főbb lépésit, a szükséges tevékenységeket és a nukleáris hulladékok kezelésének módját.

| A nukleáris üzemanyag felhasználásának és további kezelésének három lehetősége | | |
|---|---|---|
| **Egyszer használatos fűtőelemek**<br>Az üzemanyagot termikus reaktorban használják, utána nem történik újrahasznosítás.<br>(USA) | **Egy lépéses reprocesszálás, PUREX eljárás**<br>Az üzemanyagot termikus reaktorban használják, majd a kiégett fűtőelemekből kivonják a plutóniumot.<br>(Egyéb iparilag fejlett országok, Franciaország) | **Több lépéses, ismételt reprocesszálás**<br>A termikus reaktorokban kiégett üzemanyagot pyrometallurgiai eljárással teszik újra hasznosíthatóvá, amelyet gyors ALMR reaktorokban tudnak ismét hasznosítani<br>(Prototípus technológia) |
| **Az üzemanyag hasznosítása** | | |
| **5% hasznosul**<br>**95% hulladék**<br>A kitermelt uránérc energiatartalmának kevesebb, mint 1%-a hasznosul, a fennmaradó urán hulladéknak minősül. A kiégett fűtőelemeket nem hasznosítják tovább. | **6% hasznosul**<br>**94% hulladék**<br>A kitermelt uránérc energiatartalmának kevesebb, mint 1%-a hasznosul, a fennmaradó urán hulladéknak minősül. A kiégett fűtőelemeket nem hasznosítják tovább. | **5% hasznosul termikus reaktorokban**<br>**94% hasznosul gyors reaktorokban**<br>A fűtőelemek energiájának a 99%-a hasznosítható. A kiégett fűtőelemekből újra fűtőanyagot készítenek gyors reaktorok számára. |
| **Szükséges létesítmények és műveletek** | | |
| - uránium bányászat<br>- urán dúsítás<br>- fűtőelem gyártás<br>- erőművek<br>- telephelyen történő hulladék tárolás<br>- legalább 10.000 éven át történő elszigetelt hulladéktárolás | - uránium bányászat<br>- urán dúsítás<br>- telephelyen kívüli fűtőelem gyártás<br>- telephelyen kívül történő PUREX reprocesszálás<br>- erőművek<br>- telephelyen történő hulladék tárolás<br>- a hulladék telephelyen kívüli kezelése<br>- legalább 10.000 éven át történő elszigetelt hulladéktárolás | - helyszíni fűtőelem előállítás<br>- helyszíni pyrometallurgiai eljárás<br>- erőművek<br>- a hulladékok helyszíni kezelése<br>- legalább 500 éven át történő elszigetelt hulladéktárolás<br>- évszázadokig nem szükséges uránium bányászat, soha többé nem szükséges urándúsítás |
| **A plutónium sorsa** | | |
| Egyre növekvő mennyiségű plutónium a kiégett fűtőelemekben.<br>A felhalmozódott plutónium mennyisége, a fűtőanyagba történő keveréssel csak lassan csökken. | Egyre növekvő mennyiségű plutónium a kiégett fűtőelemekben.<br>Ipari mennyiségben is rendelkezésre áll tiszta formában.<br>A felhalmozódott plutónium mennyisége, a fűtőanyagba történő keveréssel csak lassan csökken | A felhalmozott mennyiség pontosan annyi amennyi a működő reaktorok fűtőelemeiben illetve amennyi a reprocessáló üzemekben van.<br>A felhalmozott egyéb készletek gyorsan felhasználhatók a fűtőelem gyártáshoz.<br>A fűtőelemekben levő plutónium fegyvergyártáshoz nem elég tiszta. |
| **A nukleáris hulladék formái** | | |
| Az energiában gazdag használt fűtőelemek felszíni konténerekben és felszín alatti tárolókban vannak elhelyezve.<br>A hulladék olyan mértékben aktív, plutónium tartalma olyan magas, hogy még évszázadok múlva is alkalmas nukleáris fegyver gyártására. | Az energiában gazdag, stabilan sugárzó radioaktív hulladék.<br>A hulladék olyan mértékben aktív, plutónium tartalma olyan magas, hogy még évszázadok múlva is alkalmas nukleáris fegyver gyártására. | A relatíve rövid felezési idejű hulladék 500 év elteltével veszélytelenné válik.<br>A hulladékban gyakorlatilag nincs plutónium, így az nukleáris fegyver gyártásához alkalmatlan. |

3. táblázat [2]

A gyors reaktor rendszer a pyrometallurgiai eljárással társítva figyelemreméltóan sokoldalú, mondhatni rugalmas. Működhet a rendszer „fogyasztóként”, amikor is a működés során elhasad a plutónium és a többi, fegyver gyártására alkalmas anyag. Működhet „termelő” üzemmódban. Ekkor a rendszer arra képes, hogy más gyorsreaktorokba üzemanyagot illetve plutóniumot állítson elő. Ekkor az uránium befogja a neutronokat és plutóniummá illetve egyéb transzuránokká alakul. Végül működhet „stacionárius” módusban, amikor a reaktor „kiégett”, tehát lecsökkent U-235 tartalmú üzemanyagot igényel a működéshez. Ekkor a fűtőelemben időegység alatt annyival növekszik a transzuránok mennyisége a neutronbefogás miatt, amennyivel csökken ezen izotópok száma a hasadás miatt, átlagos mennyiségük tehát időben állandó.

Az elemző tanulmányok azt mutatják, hogy az új technológia gazdaságilag versenyképes lehetne a már meglevő nukleáris technológiával. A pyrometallurgiai eljárás lényegesen olcsóbb, mint a jelenleg működő reprocesszálási eljárások, a hosszú távú életképessége azonban csak akkor derülhet majd ki, ha a rendszer már széles körben, ipari méretekben működik.

Egy energiaforrás átfogó értelmű gazdaságossága azonban nem csak a közvetlen költségeken múlik. Ennek megítéléséhez figyelembe kell venni a technológia alkalmazásának következtében beálló hatásokat, következményeket is, amelyeket nehéz költség formában jellemezni. (Ilyen hatás például a fosszilis erőművek esetén a környezetszennyezés és az ennek következtében kialakuló egészségügyi ártalmak.) Figyelembe kell tehát venni egy ilyen erőmű társadalomra gyakorolt közvetett és közvetlen hatásait is, amely nem egyszerű dolog, de egy ezek nélkül elvégzett gazdasági elemzés irreális és félrevezető.

A napjainkban működő termikus reaktorok lassan az 50-60 évre tervezett működési idejük végéhez érnek. Ezeket mind helyettesíteni lehetne gyors reaktorokkal. Ha ez bekövetkezne, a jövőben évszázadokon át szükségtelen lenne az uránium bányászata és soha többé nem volna szükség urándúsításra sem, ugyanis a gyors reaktorok olyan hatékonyan működnének, hogy a meglevő urániumkészletek gyakorlatilag örökre biztosítanák a szükséges fűtőanyagot. Ha napjainkban elkezdődne ezeknek az erőműveknek a kivitelezése, akkor nagyjából 15 év múlva indulhatna be az első ilyen reaktor. Ha figyelembe vesszük a Földön nukleáris hulladékok számára jelenleg rendelkezésre álló, illetve a közeli jövőben tervezett tárolókapacitást, akkor ez az időskála figyelemreméltónak tűnik, ugyanis 15 év elteltével a termikus reaktorok kiégett üzemanyagát egyenesen a gyors reaktorokba lehetne szállítani, az addig felhalmozódó készletek nagy része pedig a meglévő illetve épülő hulladékmegőrzőkbe kerülhetne.

## „YUCCA MOUNTAIN”

A radioaktív hulladékok elhelyezése az Egyesült Államokban is komoly problémát jelent [4]. Jelenleg mindössze három olyan tároló létesítmény üzemel, ahová a kiégett fűtőelemek, nukleáris hulladékok illetve a leállított és bezárt erőművek lebontása során keletkező hulladékok elszállíthatók. Ezek a következők: a Utah állam északi részén fekvő Clive, Dél Carolina államban Barnwell és a Washington állambeli Hanford nukleáris központ. A legalacsonyabb aktivitású hulladék kerül Utah államba, Dél Carolinában fogadják a közepes aktivitási szintű hulladékokat, Hanford pedig a nagy aktivitású hulladékok lerakó- és tározó helye. Ha figyelembe vesszük, hogy a jelenleg működő 104 reaktor telephelyén a tárolókapacitások korlátozottak, továbbá azt, hogy ezen reaktorok mindegyikét előbb-utóbb le kell bontani, akkor világos, hogy az említett három létesítmény ehhez nem elegendő. Ezért folyamatban van egy gigantikus befogadóképességgel rendelkező megőrzőhely építése a Nevada állam déli peremén fekvő Yucca-hegy belsejében (8.ábra). A tervek szerint itt akár több tízezer évig is raktározhatják majd a radioaktív hulladékot – elsősorban a nagy aktivitású kiégett fűtőelemeket –, ennek megnyitására azonban még legalább egy-másfél évtizedet várni kell.

Az Egyesül Államok kormánya az 1970-es évek végén kezdte tanulmányozni a dél nevadai helyszínt mint lehetséges tárolóhelyet nukleáris hulladékok számára [5]. 1987-től ezt tekintették az egyetlen lehetőségnek az addigra összegyűlt 77.000 tonna kiégett fűtőelem és egyéb nagy aktivitású

nukleáris hulladék számára. Az azóta eltelt több mint 20 év során ez a mennyiség jelentősen megnövekedett, annyira, hogy a jelenlegi mennyiség az eredetileg tervezett tárolókapacitást meg is haladja, így a terveket az elmúlt két évtized során módosítani kellett. A törvénykezési és jogi eljárások elhúzódása miatt a Bush-kormányzat csak 2002-ben tudta elindítani az építkezést. Az Észak Amerikai kontinens eme központi nukleáris lerakóhelye azonban biztosan nem nyitja meg a kapuit 2017 egyesek szerint 2020 előtt. Ez azt is jelenti, hogy a mára felhalmozódott közel 100.000 tonna nagy aktivitású nukleáris hulladékot addig is országszerte – a nagy aktivitású „fiatal" hulladékot vízfűrdőben, ún. pihentető medencében, a kisebb aktivitású „idősebb" hulladékot száraz konténerekben –, erőművek szomszédságában kell tárolni. Ha a létesítmény megnyílik, helyet biztosít egyrészt az erőművi hulladékoknak, de ugyanakkor helyet ad majd az Egyesült Államok nukleáris védelmi rendszerének kiépítése és üzemeltetése során keletkezett nukleáris hulladék egyharmadának. Ez utóbbi kategóriába tartozó 7500 tonna hulladéknak továbbra sincs megfelelő helye.

8. ábra: A Yucca-hegy gyomrában épülő geológiai tározó bejárata [V.]

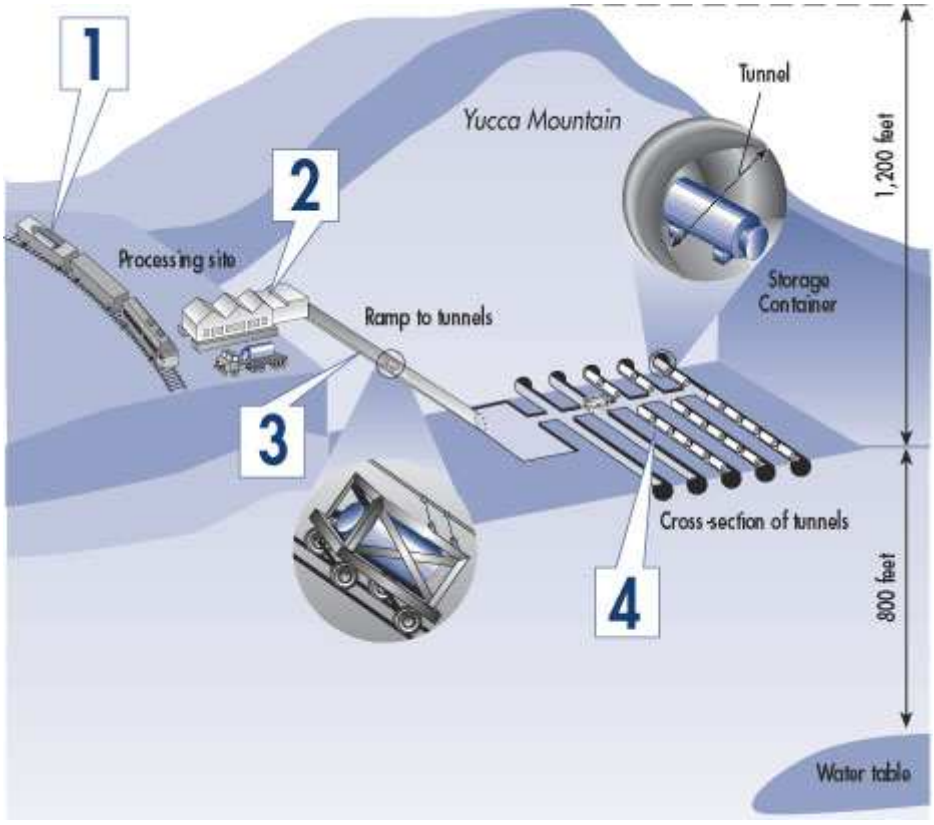
Az Egyesült Államok erőművi reaktorainak üzemelése során évente mintegy 2000 tonna nagy aktivitású nukleáris hulladék keletkezik. Ebben az ütemben haladva – a végső tervek szerint –, a Yucca-hegy–beli tároló 2035-re telik meg, amikorra az országban további 42.000 tonna nagy aktivitású hulladék halmozódik föl. Így annak ellenére, hogy a terveket többször módosították a befogadó kapacitás növelésének érdekében, a nukleáris hulladékok elhelyezésének problémája ezzel a létesítménnyel csak átmenetileg lesz megoldva.

A nevadai helyszínt elsősorban az éghajlat szárazsága tünteti ki. A radioaktív hulladékot – amelyet nagy aktivitása miatt 10.000 évig „halálos"-nak, további 250.000 évig pedig „veszélyes"-nek minősítenek –, acélötvözetből készült konténerekben helyezik majd el mélyen a Yucca-hegy gyomrában, a hegygerinccel párhuzamos alagutakban, a felszín alatt 400m mélységben. (9.ábra). Az elhelyezett radioaktív hulladék aktivitásának szintje az első 300 évben intenzíven csökken majd, ahogyan a hasadási termékek között domináns szerepet játszó cézium és stroncium izotópok elbomlanak (1.táblázat). Ennyi idő elteltével az aktivitás a kezdeti értéknek mindössze néhány %-a lesz. De a hosszú felezési idejű aktinidák mennyisége nem csökken számottevően (2.táblázat), még egymillió év elteltével is megtalálhatók majd a nukleáris hulladékban. Az Energiaügyi Minisztérium által alkalmazott számítógépes szimulációk azt mutatják, hogy a nikkel-ötvözetből készült konténerek – a száraz körülményeknek köszönhetően –, legalább 10.000 évig nem korrodálódnak, becslések szerint ennyi ideig nem fognak szivárogni. Ez az a minimális időtartam,

amelyet a Környezetvédelmi hivatal előír. A projekt ellenzői szerint a szivárgás hamarabb is bekövetkezhet. Pontosat azonban senki sem tudhat, mert a kérdéssel kapcsolatban nem végeztek kísérleteket. Az ellenzők ezen kívül felhívják még a figyelmet a hulladékok több államon keresztül történő szállításának biztonsági problémáira is.

2005 márciusában, amikor az építkezés már javában folyt, felfedeztek a hegy belsejében felszín alatti vízrétegeket, melyeknek megvizsgálták az áramlási tulajdonságait. Ennek ismeretében feltételezik, hogy egy esetleges szivárgás – melynek esélye egy természeti katasztrófa, például egy földrengés esetén fokozott –, veszélyezteti a talajvíz tisztaságát, megfertőzheti a környéken élő lakosság vízkészletét. Szakértők véleménye szerint, ha erre a geológiai jellemzőre 2002 előtt fény derül, az elég lett volna ahhoz, hogy leállítsák a projektet. Kérdés, hogy mekkora dózissal kell számolni a környéken élő lakosságot illetően. Ugyancsak számítógépes modellszámításokra hivatkozva a kormány szakértői azt állítják, hogy a maximális éves dózis, 400.000 év elteltével lesz tapasztalható, melynek szintje a természetes háttér szintjének legfeljebb kétszerese lesz, amely messze alatta marad majd a Környezetvédelmi Hivatal által megszabott 15 millirem/év egészségügyi korlátnak.

Tájékoztatásul megemlítjük még azt is, hogy az építés és az első 100 év működtetési költségei becslések szerint elérik majd az 58 milliárd $-t, az üzemeltetéshez szükséges személyzet létszáma pedig nagyjából 500 fő lesz.




9. ábra: A Yucca-hegy belsejében a nagy aktivitású nukleáris hulladékok elhelyezése a tervek szerint. [VI.]

Azonban a Yucca-hegy–beli létesítmény megnyitása már eddig is csúszott két évtizedet, az erőművekben rendelkezésre álló vízhűtésű tárolómedencék telítettsége lassan eléri a befogadóképesség maximumát. Az „idősebb”, kisebb aktivitású kiégett fűtőelemek tárolása már csak száraz, léghűtéses konténerekben lehetséges. Ezek vastag betontalapzaton álló, betonból és acélból készült henger alakú tartályok, melyek befogadóképessége 10 tonna, előállítási költségük pedig 1 millió $ (10.ábra). Egy 1000 MW teljesítményű erőmű nukleáris hulladékai évenként átlagosan 2 ilyen tartályt töltenek meg . Ha ehhez hozzászámítjuk még a szükséges infrastruktura

kiépítésének és üzemeltetésének a költségeit, akkor ez évi 300 millió $ kiadást jelent. Ezek a költségek jelentik az egyik mozgatórugóját annak a tendenciának, hogy az Egyesült Államok a reprocesszáló technológiák és erőművek új generációjának kidolgozásán munkálkodik már több mint 20 éve. Azonban a nukleáris ipar ezen jövőbeli útja nagyon költséges és egyáltalán nem veszélytelen.

## AZ ÚJ TECHNOLÓGIA VALÓBAN A HELYES MEGOLDÁS?

Frank N. von Nippel fizikus – aki az Egyesült Államok Nemzetbiztonsági Hivatalának helyettes igazgatója és a kormány tanácsadója volt nukleáris ügyekben –, korántsem látja olyan kecsegtetőnek a jövőt, véleménye szerint felmerülnek kétségek a korszerűbb reaktorok és reprocesszálási technológiák alkalmazásával kapcsolatban [3]. Egyrészt költségek oldalról tekintve, a kiégett fűtőelemek újrahasznosításának folyamata, a hasadási termékek kivonása majd a fűtőanyaggá történő újraalakítás jelentős költségekkel járó művelet. Másrészt a kockázatok oldaláról közelítve a kérdést, továbbra is fennáll majd a lehetősége, hogy – megfelelő technikai háttérrel –, a transzuránok keverékéből kivonható a tiszta plutónium, amiből fegyver gyártható. Az új reprocesszálási technológia tehát csak elenyésző mértékben csökkenti a korábban is fennálló gondokat.

A 2008-ban leköszönő Bush-kormányzat keltette ismét életre a nukleáris hulladékok újrahasznosításának gondolatát, amely az erőművek új generációja kialakulásának részét képezi. Ebben a programban a transzurán elemek nem egy alkalommal lesznek hasznosítva, hanem újra és újra visszakerülnek majd a reaktorba, melynek során a transzuránok kisebb rendszámú, rövidebb felezési idejű izotópokká hasadnak majd. Ennek köszönhetően redukálódik jelentős mértékben a nukleáris hulladékok tárolásának időtartama. De felmerül a kérdés, hogy ez a kétségtelenül hatékonynak tűnő eljárás valóban a problémák bölcs megoldását jelenti?

A gondolat nem új. Az Egyesült Államok Energiaügyi Minisztériuma már az 1990-es évek közepén megbízást adott az Egyesül Államok Tudományos Akadémiájának, hogy készítsen egy tanulmányt a hosszú felezési idejű radioaktív izotópok mennyisége csökkentésének lehetőségéről. Az eredmény meglehetősen elriasztónak mutatkozott, legalábbis anyagi téren. A tanulmány szerint, az addigra felhalmozódott készletből annak a 62.000 tonna nukleáris hulladéknak az újrahasznosítása, amelyet a tervek szerint a Yucca-hegy gyomrában helyeznek majd el, legalább 50 milliárd $ költséggel járna, de az is lehet hogy a költségek elérik majd a 100 milliárd $-t. Ez személyekre lebontva azt jelenti, hogy minden amerikai állampolgárnak 500 $-ral kellene hozzájárulni ehhez a tevékenységhez. Ha ezt kiterjesztjük az összes működő reaktor tervezett teljes működési ideje során várhatóan felhalmozódó mennyiségre, akkor ez az összeg akár meg is duplázódhat.

Miért ezek a gigantikus költségek? Azért mert a hagyományos reaktorok erre a célra nem alkalmazhatóak. A vízhűtéses-vízmoderátorú termikus reaktorokban a lelassított neutronok ugyanis nem tudják hasítani a transzuránokat. Ehhez a művelethez gyorsreaktorok kellenek. Az 1960-as és 70-es években a vezető ipari országok, közöttük az USA, mai értékre átszámolva nagyjából 50 milliárd $-t költött gyorsreaktorokkal összefüggő kutatásokra. A cél az volt, hogy ipari méretekben is lehessen energiát termelni gyorsreaktorokkal, amelynek az elmúlt évtizedekben több típusát is kifejlesztették. Ezen típusok egy része alkalmas plutónium termelésére, tehát tenyésztő reaktorként is működhet. A távlati terv az volt, hogy a termikus reaktorokat intenzív ütemben lecserélik gyors reaktorokra. A probléma nem elhanyagolható módon abban áll, hogy a gyorsreaktorok építési költsége jelentősen magasabb mint a termikus reaktoroké, és általában a biztonságos üzemeltetésük is több gondot okoz. Ezen okok miatt a legtöbb ország felhagyott az ilyen irányú terveivel.

A jelenlegi tervek olyan gyors reaktorok létesítését célozzák, amelyek – miután a reaktormag szerkezetét módosították –, plutónium termelő üzemmód helyett plutónium és transzurán fogyasztó üzemmódban is képesek működni. Az Egyesült Államok 40-75 db ilyen típusú, egyenként 1000 MW teljesítményű ilyen reaktor építését tervezi. Ezek építési költsége egyenként 1-2 milliárd $-ral

haladja meg egy ugyanekkora teljesítményű termikus reaktor konstrukciós költségeit. Ezen felül az újrahasznosítást biztosító létesítmények és szükséges infrastruktura építési és működtetési költsége további 100-200 milliárd $-t igényel, de előreláthatólag még így is szükség van 40-150 milliárd $-os további állami támogatásra. A projektet ezen jelentős költségek miatt előreláthatólag nehezen lehet majd megvalósítani.

Ha a projekt beindul, várhatóan 2020-ra épül meg az első új igényeket kielégítő, pyrometallurgiai eljáráson alapuló reprocesszáló üzem. Ha azonban az ALMR reaktorok nem épülnek fel, akkor a nukleáris hulladékok sorsa ugyanaz, mint eddig, marad a határozatlan idejű tárolás problémája az ország számos pontján. Az 1960-as években elindult reprocesszálási program öt évtizede során összegyűlt nagyjából 100 tonnányi tiszta plutónium biztonságos tárolása több tízmilliárd dollárba kerül. Azonban a nukleáris hulladékok erőművek illetve reprocesszáló üzemek telephelyén, meghatározatlan időskálán történő tárolása nem lehet a kívánatos stratégia, mert ezeken a helyeken a plutónium nagyon sérülékeny. A Royal Society 1998-ban készített egy jelentést az Egyesült Királyságban a polgári szférában keletkező, évről-évre növekvő mennyiségben felhalmozódó plutóniummal kapcsolatban. A jelentés alapgondolata, hogy „különös tekintettel kell figyelembe venni annak lehetőségét, hogy a felhalmozódott plutónium illetéktelen kezekbe kerül, és azt felhasználhatják nukleáris fegyverek előállítására”. A Royal Society 2007-ben megjelent, a kérdést érintő második tanulmánya megerősíti ezt a gondolatot: „Hosszú távon semmiképpen sem elfogadható alternatíva a plutónium és a hozzá hasonló veszélyes anyagok mennyiségének további növelése.”[3]

10.ábra: Kiégett fűtőelemek tárolása száraz konténerekben [VII.]

Világos, hogy biztonsági okokból nem szabad a plutóniumot olyan módon tárolni, hogy illetéktelenek eltulajdoníthassák, sőt egyáltalán nem volna szükséges a tiszta plutóniumot kivonni a kiégett fűtőelemekből. Mindazonáltal, amíg a Yucca-hegy–beli hosszú távú tárolóhely rendelkezésre nem áll, a nukleáris hulladék ott marad, ahol keletkezett, az erőművekben. Felmerül a kérdés, hogy mennyivel növeli meg a kockázatot a kiégett, alacsony aktivitású fűtőelemek száraz konténerekben történő tárolása (10.ábra). Szakértők véleménye szerint ennek járuléka a már fennálló nukleáris kockázati tényezők mellett csaknem elhanyagolható. Tekintsünk ugyanis, egy 20 éves, 10 tonna tömegű kiégett fűtőelem köteget, egy léghűtéses száraz konténerben, melynek hőteljesítménye 10 kW. Egy páncéltörő gránáttal, vagy repülőgép becsapódással elkövetett lehetséges terrortámadás esetén egy viszonylag kis terület szennyeződne alacsony aktivitású

radioaktív szennyezőanyaggal. Ezzel szemben a „szomszédban” működő reaktor primer köre elleni terrorcselekmény esetén, ha figyelembe vesszük az esetleges hűtővíz vesztést, és ennek következtében a fűtőelemek túlmelegedését és sérülését, akkor ez esetben percek alatt, számottevő mennyiségű, igen nagy aktivitású radioaktív szennyeződéssel kellene számolni. Akkor sem sokkal jobb a helyzet, ha a nagy aktivitású, „fiatal” kiégett fűtőelemek vízhűtéses pihentetőmedencéi elleni támadás következményeit vesszük számításba.

## REAKTOROK LEBONTÁSA

A radioaktív hulladékok elhelyezésével, tárolásával, kezelésével kapcsolatos gondok nem csak a működő reaktorok kiégett fűtőelemeivel kapcsolatban merülnek fel. Meg kell oldani a már nem működő, lebontásra ítélt reaktorok szétszerelése, bontása során keletkező radioaktív és nem radioaktív hulladék, törmelék, elhasználódott szerkezeti elemek (reaktortartály, csővezetékek, hőcserélők, stb.) biztonságos elhelyezésének, tárolásának feladatát is. Ennek a kérdéskörnek a problematikáját legjobban egy konkrét példán keresztül tudjuk bemutatni [6].

Az említett probléma előbb-utóbb a Föld minden olyan országát érinteni fogja amely üzemeltett reaktorokat. Mivel azonban az Egyesült Államok alkalmaz legrégebben nukleáris erőműveket, természetes, hogy ez a kérdés is először ebben az országban vetődött föl. Az Egyesült Államokban valaha üzembe helyezett 123 erőművi reaktorból 104 még ma is működik. A leállított 19 reaktor közé tartozik a Maine államban, Portlandtől 40 mérföldre északkeletre található „Maine Yankee” erőmű (11.ábra), amely az ország egyik első nagy teljesítményű nyomottvizes erőműve volt. Ez 1972-től 1996 végéig termelte a villamos energiát. Az erőművet lebontásra ítélték, amely szituáció számos új feladat és probléma elé állította a mérnököket, a tudósokat és a hatóságokat is. Szögezzük le mindenek előtt, hogy a lebontás, szétszerelés nem jelent „semlegesítést”, mindössze arról van szó, hogy a radioaktív anyagot az adott helyről egy másik helyre szállítják és ott a hatóságok által előírt minimális ideig tárolják. A „Maine Yankee” esetében ez jelent nagyjából 100.000 tonnányi hulladékot. Ebből a mennyiségből körülbelül 65.000 tonna beton, és valamivel több mint a fele, hozzávetőlegesen 55.000 tonna radioaktív hulladék. A kivitelezők előtt álló feladat ennek a tetemes mennyiségű hulladéknak, törmeléknek az elszállítása. A „Maine Yankee”-t követően épült 50%-kal nagyobb teljesítményű reaktorok esetében ezek az adatok némileg nagyobbak.

11.ábra. A „Maine Yankee” mielőtt befejezte működését, illetve a bontási művelet során [VIII-IX.]

A bontási művelet azzal kezdődött, hogy a reaktorcsarnok falában vágtak egy nyílást, hogy eltávolíthassák a reaktor egyes komponenseit. A 3db gőzgenerátort és a nyomás szabályozásáért felelős térfogat kompenzátort egyenesen Barnwellbe szállították (12. ábra). Ezek után került sor a reaktortartály kiemelésére. Ezt először feltöltötték betonnal, majd ugyancsak előkészítették a barnwelli lerakóhelyre történő elszállításra. A legalacsonyabb szintű aktivitással rendelkező

komponensek a Utah állambeli Clive-ba kerülnek, a nem radioaktív törmeléket pedig New York állambeli építkezéseknél használják talajfeltöltésre.


12. ábra: Nukleáris hulladék tárolása a dél carolinai Barnwell-ben. [X.]

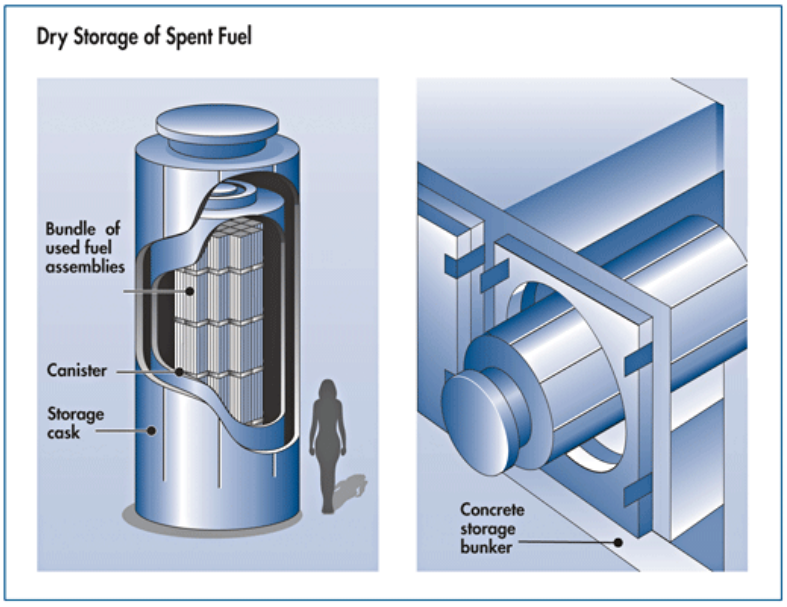
A bontás során keletkező hulladéknak a legtöbb gondot jelentő része nyilvánvalósan a radioaktív hulladék. Termikus reaktorról lévén szó, ezek között is kiemelkedő jelentőségű a kiégett fűtőelemek elhelyezésének problémája. A fűtőanyag urán-oxid kerámia, amelyet pasztillákká préselnek, majd egy fémötvözetből készült csőbe forrasztják. A reaktor működése során előfordulhat – ahogyan ez a „Maine Yankee" esetében is megtörtént –, hogy ezek a fémcsövek megrepednek, kilyukadnak és ezáltal radioaktív atommagok, hasadási termékek jutnak a primer kör vizébe. Ez a radioaktív szennyeződés rárakódik mind a reaktortartály, mind a primer kör csővezetékeinek a falára. Ezekkel a tényekkel tisztában kell lenni, hiszen ez határozza meg a kezelés módját és az elszállítás célállomását. A szállítást megelőzően, a szennyeződések csökkentése érdekében a technikusok átmosták az említett csővezetékeket olyan oldószerekkel, amelyek lemarják a csövek faláról az ott kivált csapadékot. A nagy aktivitású kiégett fűtőelem rudakat átmenetileg a helyszínen, száraz tároló konténerekben helyezték el arra az időre, amíg a központi Nevada állambeli elhelyezésre lehetőség nem nyílik. A belső szerkezeti elemek, a fémváz, amely a reaktorban a fűtőelemeket tartotta és vezette a primer kör hűtővizét, szintén a helyszínen, száraz tározóban kap átmenetileg helyet. Mindezekkel együtt összesen 64 db, külön-külön egy-egy betonbunkerbe elhelyezett tartály átmeneti felügyeletét, őrzését kell a helyszínen megoldani, még legalább egy-másfél évtizedig (13.ábra).

A felületen szennyeződött betonrétegekből vagy lefaragnak, vagy nagy nyomású légborotvával lefúvatnak szükség szerint néhány mm vagy cm vastagságú réteget. A lefúvott port nagy teljesítményű filter rendszerekkel szűrik ki a levegőből.

Ha egyetlen csővezeték vagy fűtőelem sem szivárog akkor is számolni kell a radioaktív szennyeződés egy másik fajtájával, ez pedig a neutronok hatására bekövetkező felaktiválódás. A reaktor szerkezeti anyagának atomjai befoghatják az urán hasadása során keletkező neutronokat anélkül, hogy hasadnának. Így instabil, radioaktív izotópok keletkezhetnek. A tartály betonfalában például még 60cm mélyen is található felaktiválódott atom. Ha egy reaktor évtizedeken át működik, egyes szerkezeti elemek olyan mértékben felaktiválódhatnak a neutronsugárzás hatására, hogy nagy aktivitású radioaktív hulladékként kell azokat kezelni. A dominánsan jelen levő felaktiválódott izotóp a Co-60. Ez vagy a Co-59 vagy a Ni-60 izotópból keletkezik neutronok hatására. Ezek az elemek jelen vannak a reaktor szerkezeti elemeit alkotó különböző ötvözetekben. A Co-60 5,27 év felezési idővel alakul át stabil Ni-60 izotóppá. Ez még viszonylag „kedvező időskálának" számít, ugyanis például a felezési idő négyszeresének, azaz kerekítve 21 évnek az elteltével a kezdetben

jelen levő izotóp mennyiségének csak az $(1/2)^4$=1/16 része marad meg, tehát aktivitása jelentősen csökken. Ez az időtartam a tárolás, kezelés szempontjából kellően rövidnek mondható.

A reaktorok lebontásával kapcsolatos további gondot egyrészt a magas költségek, másrészt a jogi szabályozók jelentik. Az idő előrehaladtával a költségek jelentősen növekednek, de a bontási projekt vezetői legalább ennyire tartanak a nukleáris hulladékok kezelésével kapcsolatos jogszabályok változásától. Ahogyan ezek jelentősen késleltették annak idején az erőművek építését úgy most a bontás folyamatát hátráltatják. Az ezzel kapcsolatos egyik legégetőbb kérdés a kis és közepes aktivitású hulladékok elhelyezésének a problémája. Ha ugyanis a jelenleg még működő két, e célt szolgáló megőrzőhely telítettsége eléri kapacitása maximumát, és közben nem nyitnak meg új létesítményeket, akkor a helyszínen történő ideiglenes tárolás költségei magasak lehetnek. 2003-ban például 1 $m^3$ hulladék tárolási költsége meghaladta az évi 20.000 $-t.



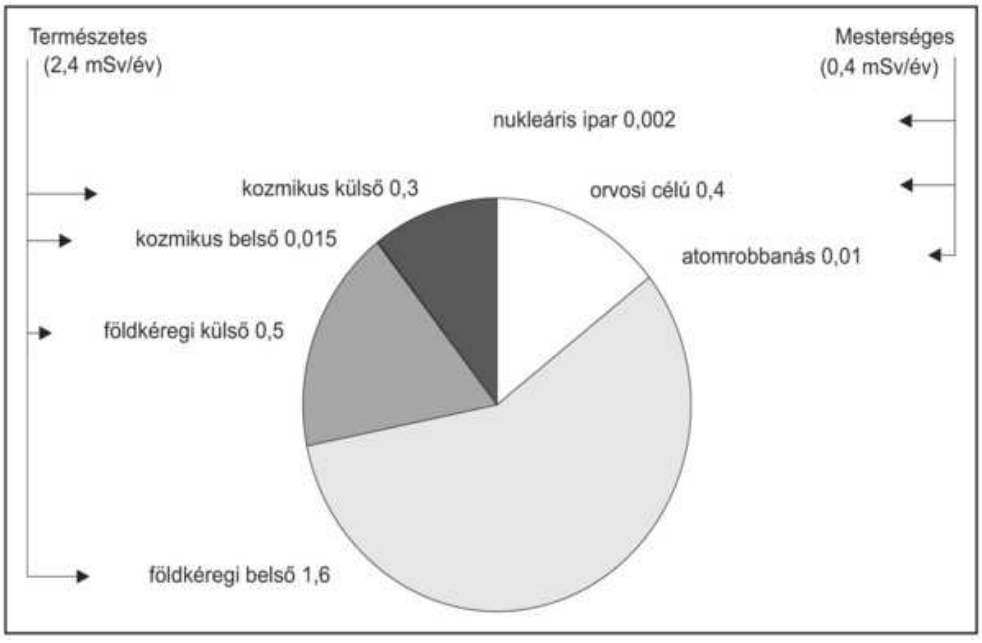

13.ábra: Nukleáris hulladékok tárolásának módja a lebontott „Maine Yankee” erőmű területén.
A száraz tároló konténereket vízszintes helyzetben, betonfalakkal körülvéve helyezik el az erőmű területén. Egy konténer tárolókapacitása 10 tonna kiégett fűtőelem [XI.]

Nem kis probléma megfelelni a hatóságok által előírt sugárzási korlátozásoknak sem, amelyek az évek során egyre szigorúbbak lesznek. A Nukleáris Szabályozó Hivatal (Nuclear Regulatory Commission, NRC) által megállapított előírás, hogy a sugárzás szintje legyen „annyira alacsony amennyire csak lehet”. Kvantitaíve, a polgári lakosságot illetően, a természetes háttérsugárzás szintjét nem lehet megnövelni évi 25 millirem dózisnál nagyobb értékkel (az egészségügyi korlát más mértékegységben kifejezve: 0,25 millisievert, 100millirem = 1mSv). Ugyanakkor a Környezetvédelmi Hivatal által megszabott korlát évi maximum 15 millirem többletdózis, amelynek legfeljebb 4 millirem része származhat a talajvíztől. A hivatal az utóbbi értéket arra alapozva kalkulálta ki, hogy a statisztikai kimutatások szerint 15 millirem többletdózis éppen egy milliomod értékkel növeli meg a rákos megbetegedés valószínűségét. Az NRC hangoztatja, hogy az általa előírt korlát megfelelő biztonságot garantál, ez jelenleg az Egyesült Államok egészére kiterjedő szövetségi standard. A végső döntés a kérdést illetően azonban az egyes államok hatáskörébe tartozik. Maine állam törvényhozása csökkentette ezt az egészségügyi korlátot 10 millirem többletdózisra, melynek szintén legfeljebb 4 millirem része származhat a talajvíztől. A szomszédos államok (Massachusetts, New York, New Jersey) csatlakoztak ehhez a lépéshez, bár az utóbbi kettő nem is üzemeltet olyan erőművet, amely a közeli jövőben lebontásra szorulna.

Szakértők véleménye szerint a Maine állambeli lépés rossz példa. Az egészségügyi korlátokat ugyanis szigorúan tudományos alapokon kell megállapítani, nem pedig érzelmi alapállásból.

Tudományos szempontból pedig a 25 millirem és a 10 millirem többletdózis lényegében ugyanazt jelenti. Ezen többletdózisok egészségügyi következményeit ugyanis kizárólag statisztikai módszerekkel lehet vizsgálni, azonban még a 25 millirem többletdózis következményeinek statisztikai megbízhatósága, szignifikanciája is kérdéses. Nincs minden kétséget kizáróan bizonyítva, hogy egy ekkora dózisnak vannak-e egészségügyi következményei. Ez a dóziskorlát annyira alacsony, hogy még a kimutatása, a mérése is komoly problémát okoz, csaknem lehetetlen. Ehhez figyelembe kell még venni, hogy ilyen alacsony dózisok esetén a mérés hibája a mért érték nagyságrendjébe esik. Célszerűbb ilyen esetben mérés helyett modelleket, szimulációkat készíteni a kérdés tanulmányozására. Fizikusok és orvosok egybehangzó véleménye szerint semmiféle egészségügyi hatást nem lehet kimutatni 10 millirem besugárzási dózis alatt. Az olyan akut következmények mint az émelygés, hányinger, hajhullás, csak akkor tapasztalható, ha a besugárzási dózis eléri a néhányszor 10 rem értéket. Ennél a pontnál azonban hangsúlyoznunk kell a különbséget az egyéni és a kollektív dózis között. A matematikai modell, amelyet az egészségügyi korlátok megállapításánál alkalmaznak, azt jósolja, hogy 10.000 rem kollektív dózis 1 és 8 közötti halálos kimenetelű rákos megbetegedést okozhat. Ez a helyzet azonban sokféle módon előállhat: 10.000 ember mindegyike kap 1 rem többletdózist, 1.000.000 ember közül mindenki kap átlagosan 0,01 rem = 10 millirem dózist, stb. Az egyénekkel kapcsolatos következmények azonnal más fényt kapnak. Összehasonlításképpen megemlítjük az ún. félhalálos dózist, melynek értéke 350 rem/személy. Ez az a besugárzási dózis, amely esetén – orvosi kezelés nélkül –, a besugárzott személyek felénél alakul ki végzetes következményekkel járó rákos betegség.

A kép akkor teljes, ha figyelembe vesszük egy átlagos körülmények között élő amerikai állampolgár sugárterhelését. A természetes háttérsugárzásból és a gyógykezelésből adódó dózis átlagosan évi 280-300 millirem (14.ábra). Ez annyit jelent, hogy a lebontott reaktorok – a dóziskorlátok betartása esetén –, nagyjából egy havi „természetes” dózisnak megfelelő többletdózissal járulnak hozzá az éves sugárterheléshez. Összehasonlításképpen ez körülbelül annyi, amennyit egy átlagos, Maine állambeli, tengerszinten élő lakos kap, amikor elutazik az 1600m tengerszint feletti magasságban fekvő Denverbe. Ezen a szinten ugyanis a vékonyabb atmoszféra miatt intenzívebb a kozmikus sugárzás. Los Alamos-i tudósok megmérték illetve kiszámították, hogy a természetes háttér részét képező kozmikus sugárzás dózisa tengerszinten évi 25-30 millirem, de 3000m tengerszint feletti magasságban azonban az évi 90 millirem értéket is elérheti.




14.ábra: Az átlagos évi 280 millirem = 2,8 mSv dózis megoszlása az egyes források között [XII.]

A bontás következtében a polgári lakossággal kapcsolatosan irányadó 25 millirem egészségügyi korlát értékéhez viszonyításképpen megemlítjük, hogy a jelenlegi szabályozás szerint, egy működő reaktor környezetében élő lakosságra vonatkozó dóziskorlát 100 millirem/év, bár hangsúlyozzuk, hogy normál üzem esetén a tényleges dózisok ennél a korlátnál lényegesen kisebbek. Az erőműben dolgozó személyzetre vonatkozó dóziskorlát pedig, a munkakörtől függően 2-5 millirem/év, de az alkalmazottak túlnyomó többsége ennek a dózisnak is csak töredékét kapja.

Visszatérve a „Maine Yankee" erőmű bontási munkálataira, a kivitelezők a minimálisra csökkentették a környező lakosságot terhelő többletdózist. Nagy teljesítményű elszívó- és szűrőberendezésekkel a radioaktív por nagy részét megkötik. A művelet hatékonyságát mutatja, hogy a bontás helyszínén, a munkálatok teljes időtartamára integrált teljes személyi dózis 1115 rem. Ennek értékeléséhez vegyük tekintetbe, hogy amikor a reaktor fűtőelemeit az utolsó alkalommal cserélték, az egész aktuális évre integrált személyi dózis 440 rem volt.

A felsorolt adatoknak egy átlagos állampolgárt érintő vonatkozásai megítéléséhez álljon itt ismét egy példa. Világos, hogy a környezetszennyezés fokozott mértékben érinti azokat akik sok időt töltenek a szabadban. Tegyük fel, hogy egy farmer az év 250 napján napi 8 órát dolgozik a földjén – ami nem igazán jellemző Maine államban –, majd a saját földjén termelt élelmiszert fogyasztja. Ebben a különleges esetben – ha még feltesszük, hogy a sugárzás szintje valóban eléri az egészségügyi korlátokat –, a farmer által elnyelt többletdózis kevesebb lesz, mint ha egy alkalommal repülőgéppel átrepülne a Föld egyik pólusa felett.

## Hivatkozások:


1. Charles Petit: Nuclear Power. National Geographic. Április, 2006.
2. William H. Hannum, Gerald E. Marsh, George S. Stanford: Smarter use of nuclear waste. Scientific American. December, 2005.
3. Frank N. von Hippel: Rethinking Nuclear Fuel Recycling. Scientific American. Május, 2008.
4. Michael E. Long. America's nuclear waste: National Geographic. Július, 2002.
5. http://www.sacredland.org/endangered_sites_pages/yucca_mountain.html (2008.06.)
6. Matthew L. Wald: Dismantling nuclear reactors. Scientific American. Március, 2003.


**Képek jegyzéke**:


I. http://www.news24.com/Images/SpecialComponents/20070302095524kenny_graph1.gif (2008.06.)
II. http://www.tesionline.com/intl/img/focus/emission.gif (2008.06.)
III. http://www.iaea.org/cgi-bin/db.page.pl/pris.oprconst.htm (2008.06.)
IV. http://nuclear.inl.gov/gen4/i/sfr-pool-layout-lg.jpg (2008.06.)
V. http://www.wnfm.com/Yucca-pics/Entrance (2008.06.)
VI. http://www.clemson.edu/caah/history/facultypages/PamMack/lec124/yucca-drawing.jpg (2008.06.)
VII. http://whyfiles.org/275nukewaste/images/dry_cask_storage.jpg (2008.06.)
VIII. http://eyeball-series.org/npp2/pict443.jpg (2008.06.)
IX. http://www.mindfully.org/Nucs/2003/Dismantling-Reactors1mar03.htm (2008.06.)
X. http://i.usatoday.net/news/_photos/2007/12/10/wastex.jpg (2008.06.)
XI. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dry-cask-storage.html (2008.06.)
XII. http://www.hik.hu/tankonyvtar/site/books/b108/kepek/7-6.jpg (2008.06.)

HADMÉRNÖK

III. Évfolyam 3. szám - 2008. szeptember

**Körmendi Krisztina**

PROTAN Zrt.
kormendi@dcs.vein.hu

**Solymosi József**

Zrínyi Miklós Nemzetvédelmi Egyetem
solymosi.jozsef@zmne.hu

# AZ EURÓPAI ÖSSZEKAPCSOLT VILLAMOSENERGIA-RENDSZER 2006. NOVEMBER 4-I ÜZEMZAVARÁNAK ÁTTEKINTŐ ÉRTÉKELÉSE

***Absztrakt***

*2006. november 4-én éjszaka az európai UCTE villamosenergia-rendszeren súlyos zavar lépett fel. A zavar az észak-német átviteli hálózatban keletkezett, ahol egy 318 kV-os távvezeték túlterhelődés következtében kikapcsolódott, ami további vezetékek kaszkádbomlását indította el, az UCTE rendszer három részre szakadt. A rendszerirányítók azonnali, az UCTE biztonsági előírásokon alapuló intézkedéseivel megakadályozták az európai méretű áramszünet kialakulását. 2006. november 5-én az UCTE vizsgáló bizottságot állított fel, mely kivizsgálta a rendszerösszeomlás okait és javaslatokat dolgozott ki a hasonló összeomlások elkerülésére teendő intézkedésekre. A vizsgálóbizottság jelentésének vizsgálata alapján a cikkben röviden bemutatjuk az európai UCTE villamosenergia-rendszer jellemzőit, áttekintjük a villamosenergia-rendszer zavarához vezető eseményeket, valamint vázoljuk az UCTE vizsgálóbizottság által feltárt, az üzemzavar kialakulásához vezető okokat, a vizsgálóbizottság által levont következtetéseket és a hasonló esetek elkerülését szolgáló ajánlásokat.*

*In the night of November 4$^{th}$ 2006 a serious disturbance occurred in the European UCTE interconnected grid. The incidents originated from the North German transmission grid, where the tripping of a transmission line indicated cascading line tripping, and the UCTE system split into three islands. Due to the immediate actions taken by the Transmission System Operators according to the UCTE standards the Europe-wide blackout was prevented. On the 5$^{th}$ of November 2006 the UCTE set up a UCTE Investigation Committee to investigate the causes of the incident and to develop recommendations to reduce the possibility of future disturbances. Based on the final report of the UCTE Investigation Committee, this article introduces the main characteristics of the European UCTE electric power system, describes the major events lead to the disturbance, the main causes of the*

*incident, the conclusions and recommendations identified by the Investigation Committee.*

***Kulcsszavak**: rendszer-üzemzavar, alacsony frekvenciájú terület, magas-frekvenciájú terület, reszinkronizáció, vezeték kaszkádkiesések, N-1 kritérium ~ system disturbance, under-frequency area, over-frequency area, resynchronisation, cascading line tripping, N-1 criterion*

## BEVEZETÉS

Az energiabiztonság és ezen belül a villamosenergia-ellátás biztonsága mára az egyik legfontosabb globális biztonsági problémává vált, mely az Európai Unióban is jelentős hangsúlyt kap. A villamosenergia-ellátás folyamatossága, biztonsága alapvető társadalmi, gazdasági érdek.

A folyamatos, biztonságos ellátás biztosításának alapfeltétele a villamosenergia-rendszer megbízható működése, azaz, hogy a villamosenergia-rendszer mindenkor képes legyen kielégíteni a fogyasztói villamosenergia igényt (megfelelőség) valamint a váratlan meghibásodások, zavarok kezelhetők legyenek (biztonság).

A villamos energia nem tárolható ipari méretekben, így a termelés és fogyasztás egyensúlyát folyamatosan kell fenntartani. Az egyensúly fenntartása gondos tervezést, folyamatos felügyeletet és beavatkozást igényel. Jelen cikk keretei között ezen egyensúly megbomlását mutatjuk be a 2006. november 4.-i európai üzemzavar példáján.

A nevezett példa választását egyrészt az indokolja, hogy ez az üzemzavar a legsúlyosabb zavarok közé sorolható Európában [1], mely az összekapcsolt rendszer bomlásával járt. A három részre bomlott rendszer két területén az egyensúly hiányát a termelt villamosenergia hiány, míg egy területén többlet okozta, így ezen a példán mindkét esetre bemutathatóak az egyensúly megbomlásának következményei illetve a rendszer helyreállítása érdekében megtett intézkedések.

Az üzemzavar 2006. november 4-én éjszaka 22:10 körül kezdődött, az üzemzavar következtében több mint 15 millió európai háztartás villamosenergia-ellátása szűnt meg időlegesen, a zavarok a legtöbb európai országot érintették. Az érintett rendszerirányítók azonnali intézkedéseinek köszönhetően azonban a zavar nem nőhetett európai méretű áramszünetté, a normál rendszerüzemet kevesebb, mint két óra alatt helyreállították valamennyi érintett területen. [1]

Az európai rendszerirányítókból álló szövetség, az UCTE (Union for the Coordination of Transmission of Electricity) tagtársaságai részvételével Vizsgáló Bizottságot állított fel az üzemzavar okainak kivizsgálására és a hasonló esetek bekövetkezésének megakadályozását szolgáló javaslatok kidolgozására. [1]

A továbbiakban az UCTE vizsgálóbizottságnak az üzemzavarról készített jelentése [1] alapján összefoglaljuk a 2006. november 4-i üzemzavar főbb eseményeit, a rendszerirányítók által megtett intézkedéseket a rendszer helyreállítására, valamint a vizsgálóbizottság által kidolgozott, a hasonló esetek elkerülését szolgáló ajánlásokat.

## AZ UCTE RENDSZER

Az UCTE villamosenergia-rendszer a legnagyobb összekapcsolt rendszer Európában, immár több mint 50 éve létezik, 24 országban 450 millió fogyasztót lát el. [2]

Az UCTE rendszerben a rendszerirányítás szervezete decentralizált, többszintű. A rendszer szabályozási területekre (control areas) osztható. Általában egy ország vagy egy

villamosenergia-ipari társaság területe képez egy szabályozási területet. Egy szabályozási területen belül egy átviteli-rendszerirányító végzi a rendszerirányítást. A szabályozási területek szabályozási blokkokba (control blocks) sorolhatók, egy szabályozási blokkot egy vagy több szabályozási terület alkothat. A szabályozási blokkok műszakilag és földrajzilag körülhatárolható alrendszerek, melyek leválva az összekapcsolt rendszerről, attól függetlenül üzemeltethetők. A szabályozási területek és blokkok felügyeletét, koordinációját a szomszédos területekkel, blokkokkal a szabályozási központok végzik. [2] [3]

Magyarország egy önálló rendszerirányítási területet képez, melyen belül a Magyar Villamosenergia-ipari Átviteli Rendszerirányító ZRt. (MAVIR) végzi a rendszerirányítást. A magyar, a cseh, a lengyel és a szlovák rendszerek a lengyel PSE-Operator SA irányította közös szabályozási blokkot alkotnak; szabályozási központjuk az RWE Brauweiler-i központja. [4] [5]

Az elmúlt egy-két évtizedben az európai átviteli-hálózat működtetésének körülményei megváltoztak. A villamosenergia-piaci kereskedelem révén a határkeresztező szállítások mennyisége valamint a szállítások távolsága megnőtt; továbbá a pontosan nem előre jelezhető, időszakosan működő villamosenergia-termelés (pl. szélerőművek) gyors térhódítása volt megfigyelhető. Ezek a kontinenst átszelő, egyre növekvő nagyságú áramlásokat idéznek elő, melyeket a rendszer kezdeti tervezésénél nem vettek figyelembe. A megváltozott körülmények miatt a rendszert a biztonsági követelmények szerinti határokhoz közel üzemeltetik, mely körülmények között a napi hálózatüzemeltetés sokkal kihívóbb feladattá vált. Így volt ez 2006. november 4-én is. [1]

## AZ ÜZEMZAVAR ESEMÉNYEI [1]

2006. november 4.-én, szombaton, több átviteli hálózati elem üzemen kívül volt; a szokásos módon a kisebb fogyasztású hétvégi időszakra ütemezett karbantartási és építési munkák miatt. 22:09-kor, közvetlenül az üzemzavart megelőzően a termelés 274.000 MW körülire volt becsülhető, melyből kb. 15.000 MW szélerőművi termelés volt. A Németországból származó jelentős szélerőművi termelés miatt erős áramlások alakultak ki Németországból Hollandia és Lengyelország felé.

A németországi E.ON Netz rendszerirányító – a Meyerwerft hajógyár kérésére – a Diele-Conneforde 380 kV-os kétrendszerű távvezeték 2006. november 5.-én 01:00-kor történő kikapcsolását tervezte, hogy a kérelmező egy hajója az Ems folyón az Északi-tengerhez haladhasson. Korábban már volt példa ilyen ok miatt a vezeték kikapcsolására, akkor az semmilyen negatív következményekkel nem járt a villamosenergia-rendszer működésének biztonságát illetően. Az E.ON Netz és az általa értesített szomszédos rendszerirányítók, a TenneT és RWE TSO, elvégezte hálózataikra vonatkozóan az előírt vizsgálatokat, melyek azt mutatták, hogy a vezeték kikapcsolás folytán az N-1 elv nem sérül azaz, az adott hálózati állapot mellett, egyik rendszerelem váratlan kiesése esetén sem kerül veszélybe az összekapcsolt rendszer üzemének biztonsága.

November 3-án a hajógyár kérésére az E.ON Netz előrehozta a tervezett kikapcsolást november 4-én 22:00 órára, miután az előírt vizsgálatok továbbra is azt mutatták, hogy hálózata erősen terhelt, de biztonságos lesz. A kikapcsolás időpontjának előrehozataláról azonban csak november 4-én 19:00 óra körül értesítette a szomszédos TenneT és RWE TSO rendszerirányítókat.

A kikapcsolás eredetileg tervezett időpontja környékére vonatkozóan (november 5-én 00:00-06:00 között) a rendszerirányítók az E.ON Netz hálózatából a TenneT hálózatába történő határkeresztező kapacitás 350MW értékkel történő csökkentésében valamint a Németország és Hollandia között, november 5-re tervezett, határkeresztező kapacitás további csökkentésében állapodtak meg; hogy az áramlásokat uralni tudják. Az E.ON Netz késői

bejelentése miatt azonban a Németország és Hollandia közötti csereprogramok csökkentése a kikapcsolás előrehozott idejére már nem volt lehetséges. Ekkor az E.ON Netz és a TenneT a Meeden alállomáson a transzformátor beállítások módosításában állapodott meg, hogy csökkentsék rendszereik közötti várható erős áramlást (a Diele-Meden rendszerösszekötő vezetéken.)

November 4-én 21:30 körül – mintegy fél órával a kikapcsolás tervezett időpontja előtt – mindkét szomszédos rendszerirányító (TenneT és RWE TSO) visszaigazolta az E.ON Netz felé, hogy hálózatuk biztonságos lesz és belegyezett a Conneforde-Diele vezeték kikapcsolásába.

Az E.ON Netz diszpécserei 21:29-kor terheléseloszlás számítást végeztek, amely nem mutatott határérték túllépést. Az N-1 elv megsértésére azonban nem végeztek vizsgálatot, hanem a hálózati állapot empirikus értékelésén alapulva feltételezték, hogy a tervezett vezeték kikapcsolás után az N-1 kritérium teljesülni fog a rendszerben.

Az üzemzavarhoz vezető események alábbiakban bemutatott sorrendjét az UCTE vizsgálati jelentésére alapoztuk.

21:38-kor az E.ON Netz kikapcsolta a Conneforde-Diele vezeték első rendszerét.

21:38-kor az E.ON Netz kikapcsolta a Conneforde-Diele vezeték második rendszerét.

21:39-kor figyelmeztető üzenetek érkezett az E.ON Netz-hez két távvezetéken folyó nagy áramlásokról.

21:41-kor a szomszédos RWE TSO tájékoztatta az E.ON Netz-t a hálózatukat összekötő egyik, a Landesbergen-Wehrendorf vezeték biztonsági határértékéről, de ekkor az áramerősség még e határérték alatt volt.

A nevezett rendszerösszekötő vezeték két oldalán a védelmi beállítások különbözőek voltak, az E.ON Netz által Landesbergenben alkalmazott határértékek (maximális megengedett érték és kioldási áram) magasabbak voltak az RWE TSO által Wehrendorfban alkalmazottaknál.

21:46 és 21:52 között a rendszerirányítók által folytatott telefonbeszélgetés során a diszpécserek a helyzetet többször is súlyosnak ítélték meg.

22:05 és 22:07 között a Landesbergen-Wehrendorf vezetéken a terhelés 100MW-al növekedett, 22:08-kor elérte az RWE TSO-nál alkalmazott riasztási értéket, amit az RWE TSO azonnal jelzett az E.ON Netz felé és azonnali beavatkozást kért.

22:10-kor – előzetes terheléseloszlás számítás és egyeztetés nélkül – az E.ON Netz a terhelés csökkentésére összekapcsolta a gyűjtősíneket a Landesbergen alállomáson. Az intézkedés eredményeként 80A-es áramerősség csökkenést vártak, azonban – az üzemzavar kivizsgálása során végzett ex-post szimulációk szerint – ellentétes hatás jelentkezett, az áramerősség 67A-el növekedett; a vezetéket a távolságvédelmi relék automatikusan kikapcsolták a Wehrendorf alállomáson.

A Landesbergen-Wehrendorf 380 kV-os vezeték kiesése további vezeték kaszkádkieséseket indított el az UCTE rendszer területén. Az első fázisban a vezetékeket a fellépő túlterhelődés miatt a távolságvédelem kapcsolta ki, a Majna folyótól délre eső vezetékeket pedig az impedanciacsökkenés védelem kapcsolta ki a drasztikus feszültégcsökkenés következtében.

A vezetékkiesések következtében az UCTE rendszer 22:10-kor három részrendszerre szakadt.

A **nyugati területen** (Spanyolország, Portugália, Franciaország, Olaszország, Belgium, Luxemburg, Hollandia, Németország egy része, Svájc, Ausztria egy része, Szlovénia, Horvátország nyugati része) a hiányzó import révén 8.940 MW teljesítményhiány alakult ki, mely következtében a frekvencia – kevesebb, mint 8 mp alatt) 49 Hz-re csökkent (az előírt 50 Hz-es normál értékkel szemben).

Az **észak-keleti területen** (Ausztria egy része, Cseh Köztársaság, Németország egy része, Magyarország, Lengyelország, Szlovákia, Ukrajna) több mint 10.000 MW termelés többlet alakult ki - ahogy a bomlás elvágta az észak-németországi erős szélerőművi termelésből származó tranzit útját Nyugat- és Dél-Európa irányába. A frekvencia gyors ütemben 51,4 Hz-re nőtt, majd az automatikus intézkedések (pl. primer szabályozás) és a magas frekvenciára érzékeny szélerőművek automatikus kiesése miatt 50,3 Hz-re csökkent. Néhány perccel később a szélerőművek automatikus visszakapcsolódása miatt ismét nőni kezdett.

A **dél-keleti** területen (Montenegro, Horvátország, Görögország, Bosznia-Hercegovina, Szerbia, Albánia, Dél-Magyarország, Bulgária, Románia) a nyugati területhez hasonlóan szintén termelés hiány jelentkezett, bár jóval kisebb: 700 MW körüli mennyiségben, a frekvencia 49.79 Hz-re csökkent.

## INTÉZKEDÉSEK A RENDSZEREGYENSÚLY HELYREÁLLÍTÁSÁRA [1]

A szétvált rendszer **nyugati részterülete** jelentős (majdnem 9000MW) teljesítményhiánnyal küzdött, mely következtében a frekvencia lecsökkent (49 Hz). A frekvenciacsökkenés aktiválta a termelőegységeken felszerelt védelmi rendszereket, az automatikus fogyasztói terheléskorlátozó rendszereket, valamint szivattyús tározós egységek kieséséhez vezetett.

A hirtelen frekvenciacsökkenés következtében számos termelő egység esett ki, tovább növelve az import elvesztéséből származó teljesítmény hiányt. A kiesett termelőegységek 40%-a szélerőmű volt, az üzemzavar előtt hálózaton levő szélerőművek 60%-a, az üzemben levő kombinált ciklusú erőművek 30%-a esett ki a frekvenciacsökkenés során. Ezek az elosztóhálózatra csatlakozó kiserőművek a rendszerirányítók által közvetlenül nem szabályozhatók. Az átviteli hálózatra csatlakozó erőművek közül csupán egy, kb. 700 MW névleges teljesítményű hőerőművi blokk esett ki Spanyolországban, ám a kiesett kiserőművek nagy száma miatt így is jelentős teljesítményhiány keletkezett a rendszerben (összesen 10.900 MW esett ki), tovább növelve a megszűnt import következtében hiányzó mennyiséget. Amint a frekvencia és a feszültség ismét a megengedett tartományba került, a kiesett kiserőművek automatikusan visszakapcsolódtak a hálózatra, rendszerirányítói beavatkozás lehetősége nélkül.

Megközelítőleg 17.000 MW fogyasztói korlátozást rendeltek el a területen, valamint 1.600 MW szivattyús teljesítményt kapcsoltak le. A frekvencia helyreállítására a rendszerirányítók – rendszerújrafelépítési terveik szerint – indították az üzemzavari tartalék termelőegységeket. A rendelkezésre álló 18.500 MW tercier tartalékból 16.800 MW-t – tehát majdnem a teljes mennyiséget – el kellett indítani. Ezekkel az intézkedésekkel a frekvenciát viszonylag rövid idő alatt sikerült az 50Hz-es értékre visszaállítani.

A frekvencia automatikus stabilizálása után a rendszerirányítók információcserébe kezdtek, de a teljes rendszer állapotát valamint a zavar okát nem tudták azonnal meghatározni. A tercier tartalékok indítását valamint a fogyasztói korlátozások visszavonását az egyes rendszerirányítók speciális koordináció nélkül végezték, a legtöbb országban a hálózatbomlással sem voltak tisztában.

A fentiekkel összhangban a frekvencia a következők szerint változott a nyugati részterületen:

22:10:28 Az UCTE rendszer szétvált, a frekvencia gyorsan csökkenni kezdett.

22:10:39 A szivattyús tározós egységek a védelmi tervek szerint kiestek, a frekvenciacsökkenés megállt.

22:10:42 A védelmi tervek szerint végrehajtott az automatikus terheléskorlátozás következtében a frekvencia növekedni kezdett.

22:11:19 A primer tartalékok aktiválásával a frekvencia tovább nőtt, 49.2 Hz-en stabilizálódott, majd a primer és szekunder tartalékok kimerülése miatt ismét csökkenni kezdett.

22:12:30 A termelés növelésével, további termelő egységek manuális indítása hatására frekvencia lassan növekedni kezdett; de a növekedés ütemét lassította, hogy néhány rendszerirányító – a rendszerirányítók közötti koordináció és a teljes rendszerállapot ismerete hiányában - időközben megkezdte a fogyasztói korlátozások visszavonását.

22:25 körül a frekvencia elérte a normál 50 Hz-es értéket.

Az **észak-keleti területen** több mint 10.000 MW termelés többlet alakult ki, melynek következtében a frekvencia gyors ütemben 51,4 Hz-re nőtt, majd az automatikus intézkedések (pl. primer szabályozás) és a magas frekvenciára érzékeny szélerőművek automatikus kiesése miatt 50,3 Hz-re csökkent. A szétválás után állandósult 50.3 Hz frekvenciájú állapot elfogadható nagyságú teljesítmény-áramlásokat eredményezett, melyek néhány kivételtől eltekintve nem veszélyeztették súlyosan a rendszer üzemét.

Néhány perccel a bomlás után a kiesett szélerőművek kezdtek automatikusan visszakapcsolódni. A visszakapcsolódó teljesítmény nagysága meghaladta a primer szabályozás útján végzett termelés csökkentés nagyságát, a feszültség lassú növekedésbe kezdett. További manuális intézkedésekkel: üzemben levő blokkok teljesítményének csökkentésével, blokkok leállításával, szivattyús tározós erőművek indításával sikerült a termelést csökkenteni, a frekvenciát 50,3 Hz-es értéken stabilizálni.

A termelőkapacitás többlet elnyelése azonban nem egyenletesen történt az érintett területeken, ami jelentős és veszélyes teljesítmény-áramlásokat generált. A többlet mintegy 58%-át a lengyel, cseh, szlovák, magyar rendszerirányítókból álló CENTREL szabályozási blokk nyelte el, miközben Észak-Németországban a szélerőművek visszakapcsolódása miatt növekedett a termelés. Emiatt az Észak-Németország felől Lengyelország és a Cseh Köztársaság felé megnőtt az áramlás nagysága, a rendszerösszekötő vezetékek terhelése jelentősen megnőtt, megnövelve a további bomlás veszélyét. A rendszerirányítóknak a délnyugat-lengyelországi termelés növelésével valamint a németországi termelés csökkentésével a túlterhelődést néhány percig sikerült feloldaniuk, majd a nyugati területtel történő sikeres reszinkronizációt és összekapcsolódást követően a villamosenergia-rendszerek 23:30-ra a normál üzemi helyzetbe tértek vissza.

A **dél-keleti** területen mintegy 770 MW teljesítményhiány keletkezett, a frekvencia 49,79 Hz-re csökkent. A frekvencia az üzemzavar során mindvégig az automatikus terheléskorlátozás első küszöbértéke felett volt, így automatikus korlátozásra nem került sor. A rendszer az N-1 elv szempontjából mindvégig üzembiztos volt. Horvátországi vízerőművi

egységek indításával, és a rendelkezésre álló szekunder tartalékok felhasználásával 22:40-re a frekvenciát a megengedett tartományon belüli értékre visszaállították. Az események alatt a rendszerirányítók aktívan kommunikáltak egymással.

Az Olaszország és Görögország közötti egyenáramú összekötetés nem szakadt meg az események során, így a szállítás Görögország felé a 312 MW tervezett menetrenddel folyamatos maradt. Továbbá az üzemzavar időpontjában a felhasználói terhelés - természetes módon, vagyis nem korlátozás hatására – lecsökkent.

A nyugati és észak-keleti területeket közötti kapcsolatot 23:24-re helyreállították, 23:57-re a dél-keleti területet is visszakapcsolták. Az UCTE rendszer teljes reszinkronizációja a bomlás után 38 perccel befejeződött, a rendszerirányítók a normál üzemállapotot az összes európai országban 2 órán belül helyreállították. A szétválást követően az egyes szabályozási területeken alkalmazott automatikus és manuális intézkedések elkerülhetővé tették a rendszerállapot további romlását és az európai méretű áramszünetet.

## AZ UCTE VIZSGÁLÓBIZOTTSÁG ÁLTAL FELTÁRT OKOK

Az UCTE vizsgálata [1] az üzemzavar hátterében húzódó alábbi fő okokat tárta fel:

**1. Az N-1 elv megsértése.**
A Conneforde-Diele vezeték kikapcsolását követően az E.ON Netz hálózatán **nem teljesült az N-1 biztonsági követelmény**.

A kikapcsolást követően a Landesbergen-Wehrendorf vezetéken folyó fizikai áramlás olyan közel volt a vezeték védelmi rendszerének beállításaihoz, hogy egy viszonylag kis teljesítményáramlás eltérés is kaszkádkieséseket indíthatott. Az N-1 elv sérülése elkerülhető lett volna, ha az UCTE által előírt megfelelő vizsgálatokat elvégezték volna.

Annak ellenére, hogy a vezetéken a terhelés a 22:02-22:10 között fokozatosan növekedett, az E.ON Netz nem tett javító intézkedéséket az áramlások csökkentésére, majd a 22:10-kor elrendelt javító intézkedés (a gyűjtősínek összekapcsolása, mely topológia változtatásról empirikus értékelés alapján döntöttek mindenféle szimuláció nélkül) nemhogy csökkentette, hanem növelte a vezetéken folyó áramlást. A vizsgálat szerint nem konkrétan a gyűjtősínek összekapcsolása tekinthető az üzemzavar okának, hanem az, hogy az E.ON Netz hálózata nem volt az összekapcsolás előtt üzembiztos.

22:00 és 22:10 között az E.ON Netz hálózatában néhány blokk növelte a teljesítményét, amely szintén növelte a vezetéken folyó áramlást.

**2. Elégtelen koordináció a rendszerirányítók között.**
Az E.ON Netz a szomszédos **rendszerirányítók** irányában tett, a Conneforde-Diele vezeték kikapcsolásának átütemezéséhez kapcsolódó **koordinációs intézkedései nem voltak megfelelőek**.

A rendszerirányítók közötti megfelelő koordináció – a hosszú távú tervezéstől a valósidejű üzem időhorizontjáig – alapvető fontosságú a rendszerbiztonság fenntartása szempontjából. Az E.ON Netz a vezeték kikapcsolása tervezett időpontjának előrehozásával kapcsolatos koordinációs intézkedései azonban nem voltak megfelelőek.

Bár a kikapcsolást az eredeti időpontra az érintett rendszerirányítókkal megfelelően előkészítették, az előrehozott időpontra vonatkozóan – az E.ON Netz késői bejelentése miatt – ugyanez már nem mondható el. Így a kikapcsolás nem volt kellően előkészítve és ellenőrizve az üzem-előkészítés fázisában. Továbbá az E.ON Netz nem vette figyelembe a Wehrendorf alállomáson alkalmazott védelmi beállításokat, mely információ kritikus volt a Landesbergen-Wehrendorf vezeték igen nagy terhelése miatt.

Bár mindhárom érintett rendszerirányító (E.ON Netz, TenneT, RWE TSO) nagy áramlásokat várt a hálózaton a Conneforde-Diele vezeték kikapcsolását követően, nem számítottak vészhelyzetre. A Landesbergen-Wehrendorf vezeték túlterhelődése által jelentett vészhelyzetet nem ismerték fel, így az E.ON Netz nem tett azonnali javító intézkedéseket. Ezt követően – a szükséges sietség miatt – a Landesbergen alállomáson történő gyűjtősín összekapcsolásról az E.ON Netz nem egyeztetett az érintett rendszerirányítókkal.

A fenti két fő ok mellett a vizsgálati jelentés [1] az alábbi, kritikus tényezőket említi meg:

*A termelés szerepe a villamosenergia-rendszer viselkedésében*

Az elosztóhálózatra kapcsolódó termelő egységek lekapcsolására vonatkozó követelmények általában kevésbé szigorúak, mint az átviteli hálózatra csatlakozók esetében, azaz kisebb frekvencia eltérés hatására kapcsolódnak le. November 4-én a rendszer szétválása után létrejött nyugati területen a termelőegységek az alacsony, az észak-keleti területen a magas frekvencia miatt estek ki. A nyugati területen a kiesések a teljesítményhiány tovább növelésével rontottak a helyzeten, az észak-keleti területen a kiesések kezdetben segítették a teljesítménytöbblet csökkenését, azonban a szélerőművek automatikus, a rendszerirányítók ellenőrzésén kívüli visszakapcsolódása akadályozta a rendszeregyensúly helyreállítását.

A rendszerirányítók csak az átviteli hálózatra csatlakozó erőművekkel állnak szabályozási kapcsolatban, mivel az elosztó hálózatra kapcsolódó kiserőművek korábban nem voltak jelentős hatással a villamosenergia-rendszer egészére. Ez a helyzet az elosztott termelés – főleg a szélfarmok - gyors fejlődése következtében megváltozott, egyes területeken a szélerőművi termelés – nagy részaránya és az időjárási körülményektől függő időszakos viselkedése miatt – jelentősen képes befolyásolni a villamosenergia-rendszer üzemét. A szélerőművi termelés hatása november 4-én egyértelműen negatív volt az észak-keleti területen. Az észak-németországi szélerőművi termelést a lengyelországi és cseh köztársasági termelés befogadással sikerült ellensúlyozni (de igen kritikus hálózati problémák előidézése mellett)

*Intézkedések a hálózati szűk keresztmetszetek kezelésére*

A szűk keresztmetszetekre kezelésére teendő intézkedéseket a nemzeti jogszabályok és a rendszerirányítók belső szabályzatai határozzák meg az egyes szabályozási területek rendszerirányítói számára. A német rendszerirányítóknak a 2006. november 4-én hatályos jogszabályok értelmében először a direkt költséggel nem járó intézkedéseket kell alkalmazniuk, ezek elégtelensége esetén alkalmazhatnak pénzügyi következményekkel járó intézkedéseket, melyek a rendszerirányítók és a piaci szereplők között érvényben levő szerződéseken alapulnak. A határkeresztező kapacitások csökkentésére, az újraterhelosztásra és az ellenkereskedelemre vonatkozó intézkedések tekintetében a tranzakciót megelőző második naptól a tranzakció valós idejéig terjedő időszakban a lehetséges intézkedések tartománya viszonylag kicsi volt.

A 2006. november 4-én hatályos szabályozás szerint a határkeresztező menetrendeket a tranzakciót megelőző napon 8:00 után már nem lehetett csökkenteni, kivéve ha vészhelyzet lép fel. Az adott időszakban az E.ON Netz-nek volt érvényben levő szerződése mely alapján az újraterhelosztásra és ellenkereskedelemre vonatkozó intézkedéseket tehetett volna, az újraterhelosztásra vonatkozó intézkedések aktiválásához azonban legalább 15 percre lett volna szükség, ami túl hosszú idő hirtelen hálózati változások esetén. Továbbá ezeket az intézkedéseket az E.ON Netz csak akkor alkalmazhatta volna, ha korábbi intézkedései nem érték el e kívánt hatást, így a vészhelyzet időben történő felismerése kritikus fontosságú lett volna.

*Védelmi- és rendszerhelyreállítási tervek*
A vizsgálati jelentésben foglaltak értelmében a nyugati területen a rendszerirányítók által alkalmazott védelmi tervek az UCTE előírásoknak megfelelő várt, kielégítő hatást mutatták. Ezen a területen az alkalmazott terheléskorlátozás megállította a frekvencia csökkenését és lehetővé tette az új rendszeregyensúly beállítását. Az egyes rendszerirányítási területek különböző okok miatt eltérő mennyiségben részesedtek az összes terheléskorlátozás nagyságából, ezek az eltérések azonban nem feltétlenül jelentettek hátrányt az UCTE rendszer biztonságára nézve.
A fogyasztói korlátozások visszavonására alkalmazott rend szabályozási területenként való eltérései azonban további egyensúlyhiányt okoztak és meghosszabbították a rendszeregyensúly helyreállításának folyamatát. Egyes elosztóhálózati engedélyesek a fogyasztók visszakapcsolását rendszerirányítói koordináció nélkül kezdték meg. A fogyasztók visszakapcsolására vonatkozó intézkedések olyan nemzeti szabályozáson alapultak, melyek lehetővé tették a fogyasztók lokális visszakapcsolását az összekapcsolt villamosenergia-rendszer globális helyzetének figyelembe vétele nélkül. Az ilyen fogyasztói visszakapcsolások csökkentették a frekvencia növelésére rendelkezésre álló teljesítmény mértékét, így a frekvencia kívánt értékre történő visszaállítása folyamatát lassították.

*Reszinkronizáció*
A reszinkronizáció a szétesést követő 40 percen belül befejeződött. A folyamatot a rendszerirányítók decentralizált módon hajtották végre, egyes esetekben a teljes összekapcsolt hálózat pontos állapotának ismerete nélkül. Azt, hogy a reszinkronizáció ilyen rövid idő alatt végbement, a decentralizált megközelítés tette lehetővé, ami a rendszerirányítási felelősségek decentralizált eloszlási módjának hatékonyságát támasztja alá.

*Diszpécseri tréningek*
A Vizsgáló Bizottság a diszpécserek felkészítésének módját a védelmi intézkedések és a rendszer újrafelépítési folyamatok alkalmazását érintően vizsgálta. A vizsgálat azt mutatta, hogy a zavarok kezelését a diszpécserekkel nem minden rendszerirányító esetében gyakoroltatták be; továbbá, hogy a szomszédos rendszerirányítókkal történő közös szimulációs tréningek nem képezték az általános gyakorlat részét.

*A rendszerirányítók közötti kommunikáció*
A rendszerirányítók közötti kommunikáció a vészhelyzetben elvárt módon történt. Az egyes rendszerirányítóknak kb. 15 percre volt szükségük a saját hálózatuk állapotának feltárására és az első szükséges intézkedések megtételére. A teljes rendszer állapotát érintő információ nem állt azonnal a rendszerirányítók részére, mely információ hiány következtében nem volt világos és teljes képük az UCTE rendszer pontos állapotáról.

## AZ UCTE VIZSGÁLÓBIZOTTSÁG ÁLTAL LEVONT KÖVETKEZTETÉSEK ÉS KIDOLGOZOTT AJÁNLÁSOK

A vizsgálat feltárta az UCTE szabványok és azok a rendszerirányítók általi alkalmazására vonatkozó előírások tökéletesítésének valamint a jogi és szabályozási keretek európai szintű harmonizációjának szükségességét. A vizsgálóbizottság az alábbi öt ajánlást [1] fogalmazta meg:

**Az N-1 kritérium alkalmazása előírt módjának felülvizsgálata**
A vizsgálóbizottság az N-1 kritérium alkalmazására vonatkozó UCTE előírás oly módú felülvizsgálatát és módosítását javasolta, mely révén az alkalmazásra vonatkozó előírások biztosítják, hogy az N-1 kritériumnak való megfelelés vizsgálatánál a rendszerirányítók a szomszédos rendszerek helyzetét is figyelembe veszik, továbbá a gyorsan változó rendszerkörülmények vizsgálatára, javító intézkedések előkészítésére és hatékonyságának rendszeres ellenőrzésére numerikus számításokat végezzenek.

**Alap-Terv az UCTE szintű vagy regionális üzemzavarok kezelésére**
A vizsgálóbizottság az UCTE előírásainak kiegészítését javasolta az UCTE kiterjedésű vagy regionális üzemzavarok esetén alkalmazandó vészhelyzeti üzem alapelveinek lefektetésével és a rendszerirányítók kötelezettségeire vonatkozó előírásokkal.

**A rendszerirányítók regionális koordinációja**
A vizsgálóbizottság UCTE előírás kidolgozását javasolta
- a rendszerirányítók regionális és régiók közötti koordinációjának módszerére,
- a közös tréningekre,
- az adatok, a biztonsági vizsgálatok eredményeinek és a tervezett javító intézkedések cseréjének tökéletesítésére.

**UCTE szintű információs rendszer**
A vizsgálóbizottság olyan információs rendszer kialakítását javasolta, mely gyűjti és a rendszerirányítók rendelkezésére bocsátja a teljes rendszer állapotának felméréséhez szükséges valós idejű adatokat; annak érdekében, hogy a rendszerirányítók eredményesen és hatékonyan tudjanak reagálni az esetleges üzemzavarok esetén.

**Erőművek viselkedése és szabályozása**
A vizsgálóbizottság a jogi keretrendszer módosítását javasolja a következők érvényre juttatása érdekében:
- a rendszerirányítók irányítani tudják a termelőegységeket (menetrend változtatás, blokk indítás vagy leállítás)
- az elosztóhálózatra csatlakozó kiserőművek frekvencia és feszültség változásai során tanúsított viselkedésére vonatkozó követelmények szigorítása
- az átviteli hálózatra csatlakozó termelőegység üzemeltetőjének kötelezése a rendszerirányító tájékoztatására a termelőegység termelési menetrendjének alakulásáról illetve annak változásairól
- a rendszerirányítók kapjanak legalább 1 perces on-line adatokat az elosztóhálózatra csatlakozó termelésről

## ÖSSZEFOGLALÁS

Az UCTE villamosenergia-rendszer a legnagyobb összekapcsolt rendszer Európában, immár több mint 50 éve létezik, 24 országban 450 millió fogyasztót lát el.

Az elmúlt egy-két évtizedben az európai átviteli-hálózat működtetésének körülményei alapvetően megváltoztak. A villamosenergia-piaci kereskedelem és a pontosan nem előre jelezhető, időszakosan működő villamosenergia-termelés térhódítása révén az európai rendszer a kontinenst átszelő, egyre hosszabb távolságú és növekvő nagyságú áramlások színterévé vált. A megváltozott körülmények miatt a rendszert a biztonsági követelmények szerinti határokhoz közel üzemeltetik, mely körülmények között a napi hálózatüzemeltetés sokkal kihívóbb feladattá vált. Így volt ez 2006. november 4-én is. [1]

Aznap egy tervezett távvezeték kikapcsolás időpontjának előre hozatala ellehetetlenítette a kikapcsolás megfelelő előkészítését. Ennek következtében az összekapcsolt rendszerben az E.ON Netz rendszerirányító területén az UCTE által előírt N-1 elv többé már nem állt fenn, egy túlterhelődött vezeték lekapcsolódása kaszkádbomlást indított el, az UCTE rendszer 3 területre bomlott, melyből 2 termelés hiánnyal és a frekvencia csökkenésével, egy pedig termelés többlettel és a frekvencia növekedésével küzdött.

A megfelelő automatikus és manuális ellenintézkedések révén a rendszerállapot további romlása és az európai áramszünet elkerülhetővé vált. A reszinkronizáció a bomlás után 38 perccel befejeződött, a normál rendszerüzem valamennyi érintett területen 2 órán belül visszaállt.

Az elosztóhálózatra csatlakozó termelés szabályozatlan működése megnehezítette a normál üzemállapot helyreállítását. A reszinkronizációs folyamat gyorsaságát a rendszerirányítói felelősségek decentralizált eloszlása tette lehetővé.

A vizsgálóbizottság az üzemzavar kialakulásának 2 fő okaként az N-1 elv sérülését és a rendszerirányítók közötti elégtelen koordinációt jelölte meg. Vizsgálta továbbá a termelőegységek viselkedésének a rendszer állapotára gyakorolt hatását, a szűk keresztmetszetek kezelésére alkalmazható intézkedések hatékonyságát, a védelmi és rendszer-újrafelépítési tervek koordinációjának szükségességét, a reszinkronizációs folyamat sikerességét, valamint a diszpécserek vészhelyzeti felkészülésére alkalmazott módszerek megfelelőségét.

Mindezek alapján a vizsgálóbizottság az UCTE előírások fejlesztését, kiegészítését valamint a nemzeti jogi és regulációs szabályozás európai szintű keretrendszerben történő összehangolását javasolta az N-1 elv alkalmazási módjának felülvizsgálata, az UCTE kiterjedésű vagy regionális üzemzavarok kezelésének alapelvei kidolgozása, a rendszerirányítók közötti koordináció és adatcsere módszerei fejlesztése, a teljes UCTE rendszer aktuális állapotának értékelését lehetővé tevő valósidejű adatok rendszerirányítók számára történő biztosítása, valamint a termelő egységekre vonatkozó szabályozás fejlesztése, összehangolása tárgyában.

Jelen cikk keretei között csupán a 2006. november 4-i események illetve ezek következményeinek és hatásainak rövid bemutatására törekedtünk, azonban a fenti konkrét esemény kialakulásának és okainak a mélyreható, elemző értékelése további tanulságokkal szolgálhat a jövőben a villamosenergia-rendszerek működési zavarai komplex problematikájának tanulmányozásában, a hasonló jelenségek megelőzése vagy felszámolása érdekében a villamosenergia-szektor, mint a kritikus infrastruktúra jelentős alkotó eleme terén.

## HIVATKOZÁSOK


[1] Union for the Co-ordination of Transmission of Electricity: System Disturbance on 4. November 2006., Final Report http://www.ucte.org/_library/otherreports/Final-Report-20070130.pdf (Letöltés dátuma: 2008.03.13)

[2] How the UCTE synchronous system operates http://www.ucte.org/aboutus/tsoworld/systemoperation/ (Letöltés ideje: 2008.03.20)

[3] Key Characteristics of Electric Transmission Systems http://www.ucte.org/aboutus/tsoworld/keycharacteristics/ (Letöltés ideje: 2008.03.20)

[4] MAVIR ZRt.: Nemzetközi szerepünk http://www.mavir.hu/domino/html/www/mavirwww.nsf/vAllPages/pNemzetkoziSzerepunk_WEB?OpenDocument (Letöltés ideje: 2008.03.21)

[5] MAVIR ZRt.: A villlamosenergia-rendszer szabályozása http://www.mavir.hu/domino/html/www/mavirwww.nsf/vAllPages/78D623653362C24FC1256FFF003D9E22/$FILE/szabalyozas20050512.pdf (Letöltés ideje: 2008.03.21)

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Szombati Zoltán**
MH 93. Petőfi Sándor Vegyivédelmi Zászlóalj
szombati60@freemail.hu

**Földi László**
Zrínyi Miklós Nemzetvédelmi Egyetem
foldi.laszlo@zmne.hu

# A MAGYAR HONVÉDSÉG KATASZTRÓFAVÉDELMI FELADATOKRA KIJELÖLT ERŐI, KÜLÖNÖS TEKINTETTEL AZ MH 93. PETŐFI SÁNDOR VEGYIVÉDELMI ZÁSZLÓALJ LEHETŐSÉGEIRE

***Absztrakt***

*A természeti- és ipari katasztrófák következményeivel szinte minden nap szembesülünk. Az ellenük való védekezés az egész világon kiemelt fontossággal bír. A katasztrófavédelem hazánkban is több szervezet együttműködését igénylő, összetett feladat. A hatályos jogszabályok a Magyar Honvédséget is kötelezik az ilyen helyzetek kezelésében való részvételre. Az MH 93. Petőfi Sándor Vegyivédelmi Zászlóalja nukleáris baleset-elhárításban vesz részt. A szerzők ismertetik az alakulat fenti feladatra kijelölt erőit, eszközeit és bemutatják a zászlóalj speciális szaktechnikai eszközeit.*
*Anyone can meet the consequence of natural disasters and industrial catastrophes almost every day. The protection against them is high priority all over the world. The disaster management is a complex task that requires the cooperation of several organisations. The legal force obligates the HDF to participate in the maintaining process of this kind of situation. The 93 NBC def. bn. takes part in the nuclear accident prevention. The authors delineate the appointed strength, equipment of this organisation for the mission written above, and introduce the special technical equipment of the battalion.*

***Kulcsszavak:*** *katasztrófavédelem, jogszabályi háttér, Magyar Honvédség, MH 93. Petőfi Sándor Vegyivédelmi Zászlóalj, szaktechnikai eszközök ~ disaster management, Hungarian Defence Forces, legal system of the disaster management, HDF 93 NBC def. bn.*

## BEVEZETÉS

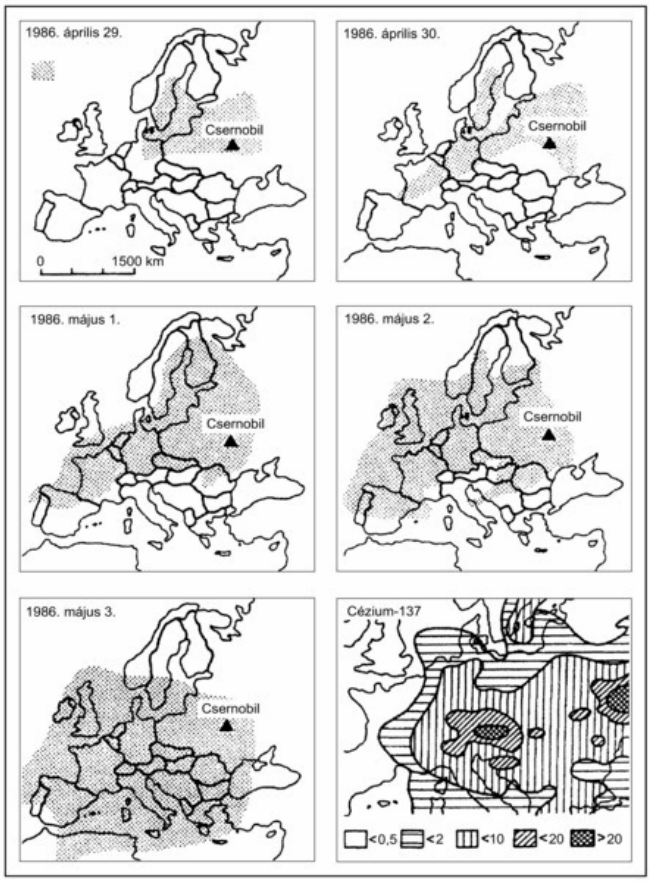
Napjainkban egyre többször találkozunk tragikus hírekkel a hazai és nemzetközi elektronikus és nyomtatott médiában. Sokszor ismétlődik a gyászos hangzású „KATASZTRÓFA” szó. Hallatán képzeletünkben halottak, sérültek, hontalanok, elpusztult házak, felégett, elárasztott földek jelennek meg. Gyakran szembesülünk azzal, hogy a világban emberek estek áldozatul és súlyos anyagi, természeti károk keletkeztek.

De pontosan mit is nevezünk katasztrófának?

Az általánosan elfogadott megfogalmazás szerint a katasztrófa „az életet, az életfeltételeket, az anyagi javakat, a természeti környezetet jelentős mértékben és súlyosan károsító vagy veszélyeztető többnyire váratlan elemi csapás, természeti, ipari (civilizációs) rendkívüli esemény, szerencsétlenség, amely nagy területeket, nagy tömegeket érint, és amelynek károsító hatásuk elleni védekezés az állami, önkormányzati szervek, magán és jogi személyek, más szervezetek összehangolt együttműködését, és szükség esetén rendkívüli intézkedések megtételét igényli.” [1]

A civilizáció fejlődésével a Földön bekövetkező katasztrófák száma és súlyossága növekvő tendenciát mutat. Az elmúlt században mintegy 3,5 millió ember esett a természeti katasztrófák áldozatául, és az 1990-es években a természeti katasztrófák összesen 535 milliárd dollárnyi kárt okoztak. [2]

Sajnos, hazánkban is több alkalommal fordult elő valamilyen katasztrófa helyzet; legjellemzőbb közülük az árvíz. Magyarországot több nagy vízhozamú folyó szeli át, ezért területünkből 21 300 km² árvíztől veszélyeztetett. A jelentősebb folyók szabályozását követően is az utóbbi 150 év alatt több mint 30 jelentős árvíz volt Magyarországon.




1. ábra: A radioaktív felhő terjedése Európában a csernobili reaktorbaleset (1986. április 26.) utáni napokban. A jobb alsó ábra: cézium-137 izotóp felszíni aktivitása 1000 Bq/m2-ben Park C.C. (1989) szerint [3]

Másik jelentős veszélyforrás a téli rendkívüli időjárási viszonyok okozta veszélyhelyzet. Bár talán a klímaváltozás következtében teleink egyre enyhébbé válnak, mindannyian emlékezhetünk hófúvások okozta közlekedési károkra.

A földrengés viszonylag ritka hazánkban, a tüzek okozta károk pedig általában nem érik el azt a szintet, amely katasztrofális következményekkel járna.

A különböző civilizációs veszélyek, ezen belül a vegyipari és kiemelten a nukleáris balesetek potenciális veszélye azonban indokolttá teszi az ellenük való védekezés megszervezését.

Csupán emlékeztetőül: a csernobili atomerőmű baleset következményeit Európa összes országa (köztük hazánk is) megszenvedte. Hatását egy ábra segítségével szeretném szemléltetni.

A katasztrófák elleni védekezés olyan komplex feladat, amely nem lehet csak egyetlen szervezet kötelessége; olyan összehangolt tevékenységsorozat, ahol minden résztvevő képességei legjavát kell nyújtania.

Célunk: áttekinteni a Magyar Honvédség katasztrófavédelemre kijelölt erőit, kiemelten az MH 93. Petőfi Sándor Vegyivédelmi Zászlóalj feladatait, kijelölt erőit és rendszeresített technikai eszközeit ezen a területen.

## A MAGYAR HONVÉDSÉG KATASZTRÓFAVÉDELMI FELADATAINAK JOGSZABÁLYI HÁTTERE

A Magyar Honvédség katasztrófavédelmi feladatait a hatályos törvények szabályozzák.

A 2006. évi VIII. törvénnyel módosított 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a személyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről 1.§-a megállapítja, „A katasztrófák megelőzése és az ellenük való védekezés (a továbbiakban katasztrófavédelem) nemzeti ügy. A védekezés egységes irányítása állami feladat.” [4]

A továbbiakban felsorolja a katasztrófavédelemben részt vevők körét: „A védekezést és a következmények felszámolását ….. a Magyar Honvédség….bevonásával, illetve közreműködésével kell elhárítani.”

A törvény meghatározza a Honvédelmi Miniszter és a honvédelmi ágazat katasztrófavédelemmel kapcsolatos feladatait (14.§, 53.§), melynek nyomán ez bekerült a honvédelemről szóló 2004. évi CV. törvénybe:

**„70. §** (1) A Honvédség feladatai:

*h)* hozzájárulás a katasztrófavédelmi feladatok megoldásához,” [5]

A jogszabály fontosnak tartja hozzátenni: „(3) Az (1) bekezdés *g)-j)* pontjában meghatározott feladatokat a Honvédség fegyverhasználati jog nélkül látja el.”

72. § (1) bekezdés szabályozza az igénybe vehető létszámkereteket és az időtartamot: „A 70. § (1) bekezdésének *h)-j)* pontjában meghatározott feladatok teljesítésére alárendelt szervezeteitől legfeljebb 100 fő 21 napi időtartamot meg nem haladó igénybevételéről a Honvéd Vezérkar főnöke, az ezt meghaladó létszámú vagy időtartamú igénybevételről a honvédelemért felelős miniszter dönt. A 3000 főt meghaladó igénybevételről a honvédelemért felelős miniszter - a döntéssel egyidejűleg - az Országgyűlést tájékoztatja.”.

A törvényi felhatalmazás alapján a Honvédelmi Minisztérium 23/2005. (VI. 16.) HM rendeletben szabályozta a Honvédelmi Katasztrófavédelmi Rendszer működését, meghatározta a feladatra kijelölt vezetők feladatait. A felsorolt jogszabályok alapján a Honvéd Vezérkar Főnöke a 14/2007. (HK. 4.) HM HVKF intézkedésével módosított 82/2005. (HK. 20.) HM HVKF intézkedéssel szabályozta a Magyar Honvédség feladatait. Ezeket kiegészíti a HM Atom-, Biológiai-, Vegyi-, Riasztási, és Értesítési Rendszere működésének szabályozásáról szóló 308/2001. (HK. 17.) HVKF Intézkedés.

A veszélyhelyzetek felsorolása a polgári védelemről szóló 1996. évi XXXVII. törvény 2.§(2) bekezdésében található. Eszerint a katasztrófák lehetséges típusai a következők:

a) természeti (elemi) csapásokkal összefüggő (vizek áradása, rendkívüli időjárási helyzet, földrengés, stb.) katasztrófák;
b) nukleáris tevékenységgel összefüggő katasztrófák;
c) ipari, vegyipari üzemekkel, anyagokkal összefüggő katasztrófák;
d) veszélyhelyzeti szintet elérő környezetkárosodás, illetve közlekedési balesetek (légi, közúti, vasúti, vízi);
e) humán járványügyi katasztrófák;
f) humanitárius segítségnyújtás tömeges méretű migráció esetén;

A különböző katasztrófahelyzetek eltérő létszámú, összetételű, felszerelésű és felkészültségű szervezetek tevékenységét igénylik.

## A MAGYAR HONVÉDSÉG KATASZTRÓFAVÉDELEMRE KIJELÖLT ERŐI

A Magyar Honvédség erőivel leggyakrabban az árvizekről beszámoló híradásokban találkozunk.

A legismertebb pillanatképek: helikopterek repülnek homokzsákokkal, kétéltű járművek mentik az elöntött falvak lakóit, katonák erősítik a töltéseket, építik az ideiglenes gátakat, és tehergépkocsik szállítják az élelmiszert. A felsoroltakból kitűnik, hogy a légierő, a szárazföld és a logisztika egyaránt kiveszi a részét a katasztrófák elleni küzdelemből. Sokszor azonban nem elegendő a nemzeti összefogás. Már Csernobil kapcsán láthattuk, hogy a különböző veszélyhelyzetek nem ismerik a határokat, gyakran regionális hatásúak. A nemzetközi méretű összefogás szükségességére egyik legjobb példa a többnemzeti Tisza Műveleti Zászlóalj.

A Magyar-Román-Szlovák-Ukrán Tisza Műveleti Zászlóalj rendeltetése a Tisza vízgyűjtő területén bekövetkezett katasztrófa esetén a lakosságnak történő segítségnyújtás és a károk megszüntetésében való részvétel. A zászlóaljat létrehozó nemzetek vállalták, hogy felkérés esetén limitált erőkkel és hasonló típusú eszközökkel sietnek egymás segítségére. Árvíz esetén több katonai szervezet állományából különböző rendeltetésű csoportok kerültek kijelölésre, pl. búvár csoport, emelőgép csoport, légi csoport, nehéz kétéltű mentő csoport, robbantó csoport, védelmi és romeltakarító kézi munkát végző csoport, tábori ellátó csoport.

A honvédségi katasztrófavédelmi tevékenység másik fontos területe a téli rendkívüli időjárási helyzet kezeléséhez kapcsolódik.

Olyan, téli veszélyhelyzetet felszámoló és mentő munkacsoportok kerültek kijelölésre, amelyek különféle terepjáró eszközökkel mentik az úton rekedt járművökből az utasokat, elzárt körzeteket láthatnak el élelmiszerrel, gyógyszerrel, és biztosíthatják a rászorulók orvoshoz vagy gyógyintézetbe jutását.

A különböző ipari katasztrófák esetén a HAVARIA laboratórium képes az objektumok sérülésekor kialakult szennyezettség felderítésére, a kiszabadult anyagok minőségi és mennyiségi analízisére, és javaslatot tehet a kárelhárítási tevékenységre.

Az esetleg előforduló humán járványügyi katasztrófák esetén a Megelőző Orvosi Laboratórium, a Mobil Orvos Csoport és az Orvosi Ellátó Csoport nyújthat segítséget a rászorulóknak.

Nukleáris balesetelhárítási feladatokra az ABV felderítő, ABV mentesítő csoport, a légi sugárfelderítő raj, HAVARIA laboratórium, a Sugáregészségügyi Laboratórium, Mobil Orvos Csoport, Orvosi Ellátó Csoport, nehéz és könnyű földmunkagép és gépi romeltakarító csoport, átkelő csoport, tábori ellátó csoport és az ágazati információs központ jelölhető ki.

## AZ MH 93. PETŐFI SÁNDOR VEGYIVÉDELMI ZÁSZLÓALJ KIJELÖLT ERŐI, LEHETŐSÉGEI KATASZTRÓFAHELYZETBEN

A vegyivédelmi zászlóalj a Magyar Honvédség katasztrófavédelmi rendszerében elsősorban a nukleáris balesetelhárítási feladatokban vesz részt, bár korlátozott mértékben, egyes speciális felszerelést vagy szaktudást nem igénylő árvízvédelmi vagy téli rendkívüli veszélyhelyzeti tevékenységet is képes ellátni.

A zászlóalj alapító okirata az alábbiakat rögzíti: „a költségvetési szerv állami feladatként ellátandó alaptevékenysége: „a.) kijelölt állományával és technikai eszközeivel a Honvédelmi Katasztrófavédelmi Rendszer feladataiban, valamint az ország területén bekövetkezett nukleáris baleset következményei felszámolásában való részvétel.” [6]

A feladat magában foglalja:

A.) Szükséges okmányok, tervek kidolgozását, folyamatos pontosítását.

A legfontosabbak:

a) az MH 93.PS.VV.Z. Katasztrófavédelmi Alkalmazási Terve, amely tartalmazza a zászlóalj feladatait a felkészülés, a védekezés és a helyreállítás időszakában; a vezetés rendjét; a kijelölt erőket, eszközöket; a riasztás, a kirendelés, az alkalmazás és a jelentések rendjét; a híradás, a logisztikai és az egészségügyi biztosítás tervét.

b) a zászlóaljparancsnok intézkedése katasztrófavédelmi feladatok végrehajtására

c) munkatérképek (az Operatív Csoport, a tiszti felderítő járőr, az alegységparancsnokok részére)

d) riasztási terv

e) féléves kiképzési intézkedés és kiképzési terv levezetési tervek

f) egyéb vezetési okmányok (hadműveleti napló, napi összefoglaló jelentések)

B) a kijelölt állomány általános katonai és speciális szakmai felkészítését.

A felkészítés főbb rendezvényei (csak a nukleáris baleset-elhárítás tekintetében):

a) nukleáris baleset-elhárítási kiképzés: évente két alkalommal, tavasszal és ősszel kerül levezetésre 7-7 nap időtartamban; alegység gyakorlattal zárul.

A kiképzés célja: megismertetni a katonákkal:

- az általános és a katonai szervezet felelősségi körzetében lévő potenciális veszélyforrásokat
- a környezetbe kerülhető veszélyes sugárzó anyagok legfontosabb fizikai és kémiai jellemzőit, hatásait a környezetre, az élővilágra
- az ellenük való védekezés módjait
- a katonák, az alegység várható feladatai végrehajtásának sajátosságait.

A fentiek alapján be kell gyakoroltatni a katonákkal az alkalmazási tervben meghatározott feladatok gyors és pontos végrehajtását a nukleáris balesetek következményeinek felszámolása során.

b) légi-, sugárfelderítő kiképzés: évente egy alkalommal 4 nap időtartamban (2 nap elméleti felkészülés, 1 repülési nap, 1 repülési tartaléknap, amennyiben az eredeti időpontban az időjárási viszonyok vagy a helikopterek egyéb irányú elfoglaltsága nem teszi lehetővé a repülést).

Célja: a tiszti felderítő járőr és a kijelölt ABV felderítő állomány felkészítése sugárszennyezett útvonalak és körzetek légi-, sugárfelderítésének végrehajtására, biztosítva a gyors felderítési adatokat az értékelések mielőbbi végrehajtása érdekében.

c) ABV Riasztási és Értesítési Rendszergyakorlat: évente egy alkalommal 2-3 nap időtartamban az MH Görgey Artúr Vegyivédelmi Információs Központ által kidolgozott levezetési terv alapján.

Célja: az ABV értékelő szakállomány ismeretszintjének fejlesztése, értékelések végrehajtása, az információáramlás, az adatok jelentésének, az értékelt adatok bejuttatásának gyakorlása.

d) ABV RIÉR együttműködési nap: havonta egy nap

Célja: az összekötetés a rendszer működőképességének, az információáramlásnak az ellenőrzése.

C) A szükséges technikai eszközök hadrafoghatóságának biztosítását, az anyagi készletek megállapítását és frissítését.

A technikai eszközök hadrafoghatósága biztosítása kiemelt fontosságú feladat, mivel a terveket pontosítani, okmányokat kidolgozni csak idő (és szakemberek) kérdése. A harc- és gépjárművek javításához azonban javítóanyag, javítókapacitás szükséges, márpedig ezekből soha nincs elegendő. Különösen nagy gond a 40 éves FMG-68 folyadékos mentesítő gépkocsik üzemképességének folyamatos fenntartása. Ezek az eszközök – életkorukból adó viszonylagos megbízhatatlanságuk miatt – gyakrabban romlanak el, mint fiatalabb társaik és javításuk után sem prognosztizálható üzemképességük időtartama.

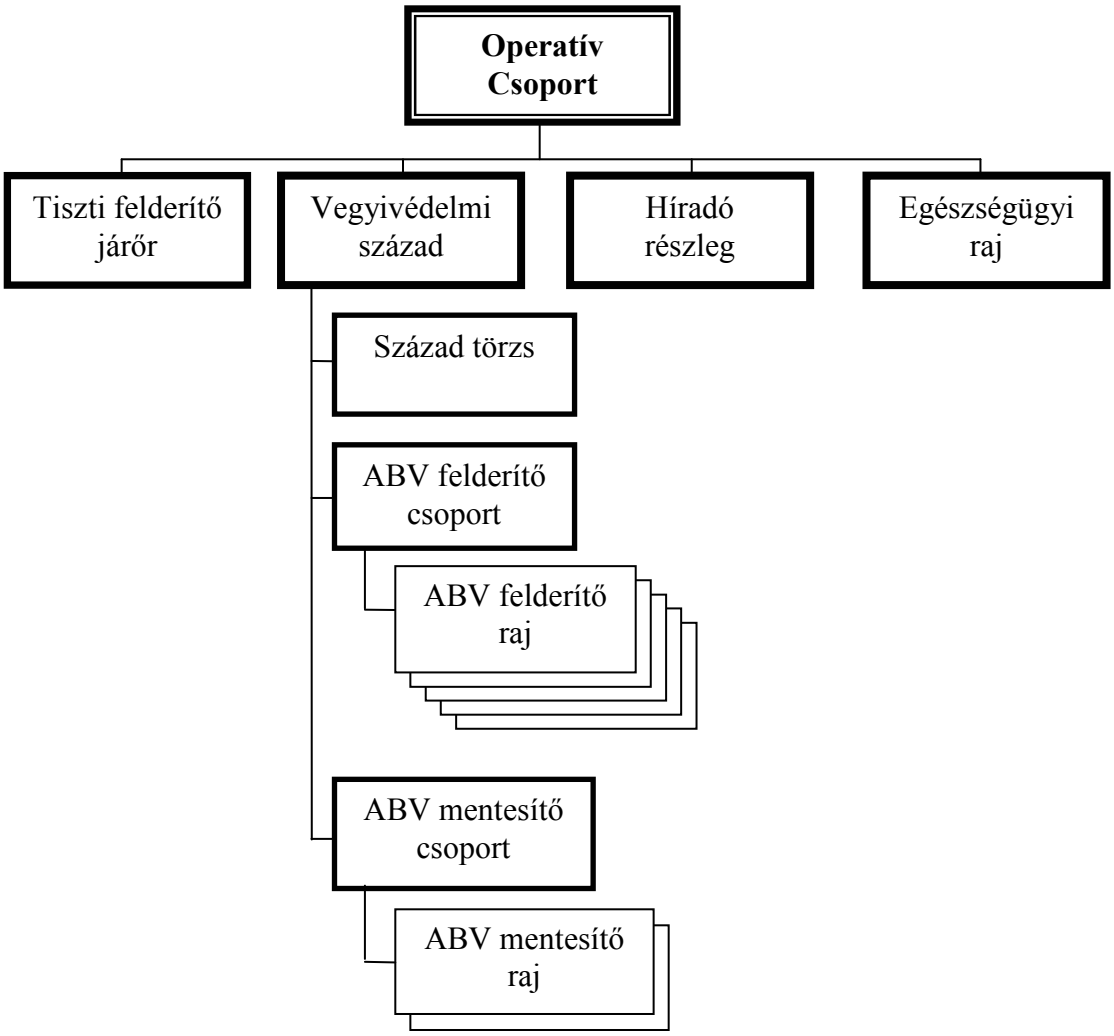
A kijelölt alegység 3 napi önálló tevékenységre számvetett anyagi készlettel vonul el. Amennyiben a feladat időtartama ennél hosszabb, a kijelölt bázislaktanyából látják el őket.

D) Az együttműködés megszervezését. Erre a konkrét feladat elrendelése után kerül sor.

E) A feladatra kijelölt állomány riasztását. Ezt a készenlét fokozására kidolgozott riasztási terv és a szolgálatvezénylési parancs alapján végzi a laktanya-ügyeleti szolgálat. A zászlóalj hadműveleti részlege a riasztási okmányban naponta pontosítja a készenléti szolgálatba vezényelt katonák nevét és munkaidőn túli elérhetőségét.

F) A feladatok vezetését. A kijelölt Operatív Csoport részére berendezett vezetési teremben kialakításra kerültek a vezetés technikai feltételei: Internet, intranet, városi, valamint HM telefon és telefax vonal áll rendelkezésre az összeköttetések felvételére. Itt vannak a vezetési okmányok is (munkatérkép, híradó összeköttetés tervei, logisztikai számvetések, kimutatások, jelentések, mintaokmányok). Az Operatív Csoport tagjainak a felkészítése törzsfoglalkozásokon és törzsgyakorlásokon történik.

A zászlóalj állományából a Honvédségi Katasztrófavédelmi Rendszerbe az alábbi erőket jelölték ki:




Összesen: 62 fő, 22 db technikai eszköz

Az alegység állományából 13 fő lát el készenléti szolgálatot (tiszti felderítő járőr, egy ABV felderítő és egy ABV mentesítő raj).

A kijelölt erők, eszközök az alábbi képességekkel rendelkeznek (napi 10 órás szaktevékenység esetén):

A) Az ABV felderítő csoport feladata: sugárszennyezett területek földi felderítése, személyek, tárgyak, objektumok, anyagok sugárszennyezettségének ellenőrzése. A csoport naponta képes 1250-1500 km útvonal, vagy 2500-3000 km² terület sugárfelderítésére, vagy 380-390 km² terület figyeléssel történő ellenőrzésére, 5 sugárfigyelő őrs telepítésére vagy 5 sugárfelderítő járőr működtetésére.

B) A légi-, sugárfelderítő tiszti járőr feladata: légi sugárfelderítésben való részvétel. Képes a talaj sugárszintjének meghatározására helikopterekből vagy más repülőeszközből. Meghatározott paraméterű repülés esetén (pl. 120 km/ó repülési sebesség, 100 m repülési magasság) kellő pontosságú adatok szolgáltatására képes.

C) Az ABV mentesítő csoport feladata: technikai eszközök, anyagok, felszerelési tárgyak, szilárd burkolatú utak, objektumok, személyek sugármentesítése. A csoport képes naponta 1000 fő, 120-160 db technikai eszköz vagy 10 km szilárd burkolatú (beton vagy aszfalt) út sugármentesítésére.

D) A híradó részleg feladata: a vezetés folyamatossága érdekében a katasztrófavédelembe bevont erők híradásának biztosítása az aktivizált ügyeletes rádióállomások, valamint az érintett helyőrségek között. Az állományba tartozó R-142

rádióállomás képes egyidőben 3 db URH (20 MHz-52 MHz között maximum 40 km távolságig) és 1db RH rádióforgalmi rendszerben (1,5 MHz-11 MHz között, telepített antennától függően 50-350 km távolságban ) összeköttetést működtetni.

E) Az egészségügyi raj feladata: első szaksegély, amely magában foglalja az életmentő elsősegélynyújtást és a meghatározott egyéb segélynyújtási formákat. A raj képes egy fordulóval 4 fekvő és 1 ülő, vagy 2 fekvő és 4 ülő sérült szállítására. Napi átlagos sebesültszállítási teljesítmény 150 km.

## AZ MH 93. PETŐFI SÁNDOR VEGYIVÉDELMI ZÁSZLÓALJ KATASZTRÓFAVÉDELMI FELADATOK VÉGREHAJTÁSÁRA ALKALMAZOTT SZAKTECHNIKAI ESZKÖZEI

A sugárfelderítés végrehajtására a különböző csoportoknál az alábbi eszközök állnak rendelkezésre:

A) Tiszti felderítő járőr: szakfeladatait az SSM-1 sugárszint és dózisteljesítmény-mérő műszerrel látja el.


2. kép: SSM-1 sugárszint- és dózisteljesítmény-mérő műszer

A műszer és a szonda főbb technikai adatai:
A mért mennyiség: dózisteljesítmény-egyenérték
Sugárzás típusa: gamma
Detektorok: GM-cső
Kijelzés: digitális és analóg, akusztikus jelzés
Méréstartomány: 0,1 μsv/h - 5 Sv/h
Kijelzési tartomány: 0,03 μsv/h - 5 Sv/h
Terhelhetőség: 200 Sv/h-ig
Energiafüggőség: 50 keV - 1,3 MeV
Ajánlott mérésirány: merőleges a szondatengelyre
Működési hőmérséklettartomány: -30 $^{o}$C - +50 $^{o}$C-ig
Méret (szonda): 40 mm x 390 mm
Tömeg (szonda): 0,7 kg
Tömeg (műszer): 2,5 kg

B) ABV felderítő csoport: legfontosabb technikai eszköze a VSBRDM-2M vegyi-, sugárfelderítő harcjármű.

3. kép: VSBRDM-2M vegyi-, sugárfelderítő harcjármű

Kezelőszemélyzete: 3 fő (rajparancsnok, kezelő, harcjármű vezető)
Súlya: 8000 kg
Sebessége úton: max. 80 km/ó
Alkalmas vegyi-, sugárfelderítésre, vegyi és sugárszennyezett területek határainak megjelölésére, minták vételére, talajmenti meteorológiai adatok mérésére.
A harcjármű nukleáris balesetelhárítási feladat esetén alkalmazott szakfelszerelései:

a) IH-99D harcjármű fedélzeti sugárzásmérő műszer

4. kép: az IH-99D harcjármű fedélzeti sugárzásmérő műszer szondája

Rendeltetése:

A dózisteljesítmény-távadó egyaránt alkalmazható folyamatos felderítésre alacsony és rendkívül magas radioaktív sugárszint mellett.

A távadó kijelzővel és belső akkumulátorral nem rendelkezik, a mérési eredményeket soros vonalon továbbítja IBM PC kompatibilis számítógép, vagy más adatgyűjtő és kijelző egység felé.

Fontosabb technikai adatai:

- Detektor: energia-kompenzált GM-cső
- Indikálási tartomány: 10 nGy/h - 100 Gy/h
- Mérési tartomány: 50 nGy/h - 1 Gy/h

A mérési tartomány fölött 100 Gy/h-ig az adatküldés monoton növekvő. A mérési tartomány alatt 10nGy/h ... 1 µGy/h tartományban a maximális 4 perces átlagolási idő alatt a statisztikus hiba nagyobb, mint 10 %

- Energia tartomány: 50 keV - 1,5 MeV
- Átlagolási idő: 2 s - 4 perc, automatikus

b.) IH-95 sugárszint és -szennyezettség mérő műszer


5. kép: IH-95 sugárszint– és szennyezettség mérő műszer

Az IH-95 sugárszint- és szennyezettség mérő műszer alkalmas:

- a gamma sugárszint mérésére Gy/h mértékegységben;
- a gamma sugárszint gyors, folyamatos keresésére Gy/h mértékegységben;
- a sugárszint integráljaként gamma dózis mérésére Gy mértékegységben;
- a beállított dózisteljesítmény-, vagy dózis küszöbszintet meghaladó esetben riasztásra;
- felületi béta szennyezettség mérésére Bq/cm$^2$ mértékegységben;
- felületi alfa szennyezettség indikálására Bq/cm$^2$ mértékegységben;
- béta radioaktív koncentráció mérésére Bq/l mértékegységben,
- összegzett alfa, béta, gamma beütésszám indikálására felületi radioaktív szennyeződés keresése céljából.

Alkalmazhatóság:

A műszer mérési tartománya lehetővé teszi a terep sugárfelderítését nukleáris környezetellenőrzés és baleset-elhárítás során, valamint atomtámadásokat követően.

Sugárszint (gamma dózisteljesítmény) mérés:

- Mérési tartomány: 50 nGy/h - 0,5 Gy/h
- A kijelzési tartomány fölött 0,5 - 10 Gy/h-ig a kijelzés monoton növekvő (a kijelzett érték előtt „-" hibajelzés van, jelezve, hogy a mérési eredmény kívül eshet a megadott alaphibán), 10 Gy/h fölött pedig túlterhelésjelzés van (>10 Gy/h)
- Energia tartomány: 60 keV - 1,5 MeV
- Mérési idő: 2 s - 4 perc, automatikus
- Bemelegedési idő: 30 s
- Hőmérséklet-függés (a -25 °C - +50 °C tartományban): ± 10%.
- Tápfeszültség-függés: ± 10%.
- Elnyelt gamma dózismérés
- A dózisteljesítmény-mérés adataiból összegzéssel képzett dózis adat.
- Mérési tartomány: 10 nGy - 10Gy

- A dózis adat képzése és kijelzése a megadott felső határérték fölött is folytatódik.
- Az adatok a műszer kikapcsolt állapotában is tárolódnak, törlésük menüből lehetséges.
- Tárolási idő a műszer kikapcsolt állapotában, feltöltött telepekkel: 6 hónap
- Tárolási idő telep nélkül: 1 nap

c) IH-99 L Központi adatgyűjtő és IH-99 LDC kijelző egység

6. kép: IH-99 L Központi adatgyűjtő és IH-99 LDC kijelző egység

Az IH-99L központi adatgyűjtő egység feladata a járműfedélzeti műszerek (IH-99D sugárszintmérő detektor, GID-3 fedélzeti vegyi felderítő) jelzéseinek, a GPS helymeghatározó, valamint a telepített TVS-3ML meteorológiai állomás által szolgáltatott adatok fogadása és tárolása, továbbá a mérési adatok feldolgozása.

IH-99 LCD kijelző egység:

A kijelző egység soros vonalon keresztül fogadja a központi adatgyűjtő egységről érkező mérési eredményeket és megjeleníti azokat. A gyűjtött adatok alapján ATP 45 szerinti jelentést készít. (A képen az adatgyűjtő üzemmód működik). Riasztási eseménykor működteti az eseményjelző egységet.

d) TVS-3 Meteorológiai felszerelés

A TVS-3 mobilizálható meteorológiai állomás rendeltetése a vegyi és a radioaktív sugárzás terjedésének meghatározására szolgáló meteorológiai jellemzők mérése, illetve meghatározása, adatok továbbítása az IH-99L központi adatgyűjtő egységhez.

Az állomás az alábbi adatok mérésére alkalmas:

- szélirány
- szélsebesség
- talajhőmérséklet
- levegő hőmérséklet (50 cm és 2 m magasságban)
- légnyomás
- relatív páratartalom.

7. kép: TVS-3 Meteorológiai felszerelés

e) Vegyi- és sugárszennyezettség mintavevő felszerelés


8. kép: Vegyi- és sugárszennyezettség mintavevő felszerelés

A VSMF rendeltetése szilárd, folyadék és légnemű anyagokból mintavétel stabil és mobil vegyivédelmi laboratóriumok számára. A VSMF a vegyi- és sugárfelderítő raj eszköze. Lehetővé teszi, hogy a raj mintákat szolgáltasson a laboratóriumok számára. A hordozható egységként kialakított VSMF alkalmas a minták begyűjtésére, készletezett fogyóeszközei a minták tárolására és szállítására szolgálnak.

f) DS-10 csapatmentesítő készlet

A DS 10 csapatmentesítő készlet autonóm mentesítő berendezés, mely a hozzá rendszeresített (gyártó által jóváhagyott) mentesítő anyagok felhasználásával csapatoknál a harc- és gépjárművek, egyéb haditechnikai és felszerelési eszközök részleges és teljes vegyi-, sugár- és biológiai mentesítésére (fertőtlenítésére) szolgál.

Műszaki adatok:

- magasság: 704 mm
- átmérő: 210 mm

– tömeg (töltet nélkül): 9,5 kg
– tartály térfogata: 15 liter
– hasznos térfogat: 10 liter
– megengedett üzemi nyomás: maximum 6 bar
– megengedett üzemi hőmérséklet: maximum 60 $^{o}$C
– tárolható: -40 – +70 $^{o}$C között

9. kép: DS-10 csapatmentesítő készlet

g) SOR/T doziméter


10. kép: SOR/T doziméter

Alkalmas személyek és csoportok elnyelt sugáradagjának pontos mérésére.
Harcászati, technikai adatok:

- üzemi hőmérséklet: -21 °C – +50 °C
- tárolási hőmérséklet: -40 °C – +71 °C
- vízállóság: 1 m 2 óra alatt
- hosszúság: 80,4 mm
- szélesség: 48 mm
- magasság: 9,6 mm

- súly: 55 g
- tartózsinór: 80 cm
- dózismérési tartomány: 10 cGy – 10 Gy
- pontosság: ± 30%
- telítettségjelző: 9,999 Sv/h felett

h) XOM/T író-olvasó (kiértékelő) készülék

11. kép: XOM/T író-olvasó (kiértékelő) készülék

Képes a doziméter adatainak olvasására, adatok megváltoztatására, doziméter aktiválására, inaktiválására. Alkalmazható adatok gyűjtésére a dozimétérektől, az adatok tárolására és keltezésére, adatkivitelre a készülékről számítógépre.

Harcászati, technikai adatok:

- hosszúság: 263 mm
- szélesség: 188 mm
- magasság: 80 mm
- súly: 1,8 kg akkuk nélkül
- kommunikációs tartomány 40 cm
- üzemi hőmérséklet: -31°C – +50 °C
- tárolási hőmérséklet: -40 °C – +71 °C

A fenti technikai eszközökön és műszereken túl a csoport (a rajok, illetve a katonák) más szakfelszerelésekkel is rendelkeznek, például a GID-3 fedélzeti vegyifelderítő berendezés, CAM-2 kézi vegyifelderítő berendezés, kimutatócső készlet, 93 M védőruha és gázálarc, jelzőzászló készletek, fegyverzeti-, műszaki- és híradó eszközök. Jelen dolgozatnak azonban nem célja a teljes eszközrendszer, mindössze a konkrét feladat végrehajtásához szükséges eszközök bemutatása.

C) ABV mentesítő csoport: a rajok legfontosabb szaktechnikai eszköze az FMG-68 folyadékos mentesítő gépkocsi.

Rendeltetése a fegyverzet, a harci- és szállítóeszközök vegyi- és sugármentesítése, a terep vegyimentesítése, a személyi állomány fürdetése, tüzek oltása, mentesítő oldatok bekeverése és kisebb mentesítőeszközök feltöltése, függőleges felületek lemosása és mentesítése, víz és mentesítő oldatok szállítása.

Fontosabb technikai adatai:

– alváza: Csepel-346

- kezelőszemélyzete: 3 fő,
- sebessége úton: 80 km/ó, terepen: 45 km/ó.
- víztartályának térfogata: 2000 l

12. kép: FMG-68 folyadékos mentesítő gépkocsi

A bemutatott szaktechnikai eszközök technikai paraméterei lehetővé teszik a vegyivédelmi zászlóalj katasztrófavédelmi feladatai eredményes végrehajtását, bár az FMG-68 folyadékos mentesítő gépkocsi még a Magyar Néphadsereg technikai színvonalán álló jármű, korszerűbb típussal történő felváltása elengedhetetlen.

## ÖSSZEGZÉS

A katasztrófavédelem a Magyar Honvédség fő feladatai közé tartozik. Írásunkban áttekintettük a vonatkozó jogszabályokat, a Magyar Honvédség erre kijelölt csoportjait és részletesen bemutattuk a MH 93. Petőfi Sándor Vegyivédelmi Zászlóalj speciális képességeit. A zászlóalj jellegéből, felszereltségéből, létszámából adódóan a nukleáris, balesetelhárítási feladatrendszerben vesz részt. Ismertettük teljesítőképességét és legfontosabb, e területen használt szaktechnikai eszközeit. Ezek nagy része korszerű, a kor színvonalán álló műszer, de a mentesítés alapeszköze, az FMG-68 folyadékos mentesítő gépkocsi az idén ünnepli 40. születésnapját, így cseréje nemcsak indokolt, de elengedhetetlenül szükséges egyrészt a fentebb ismertetett feladatok miatt, másrészt a magyar kormánynak a prágai NATO Csúcsértekezleten tett vállalása miatt is.
A zászlóalj szerepe a későbbiekben, az eszközrendszer fejlesztése mellett – elsősorban a vegyi azonosító és a biológiai felderítő képesség megteremtésével – a vegyipari katasztrófák következményei felszámolásában való részvétellel bővíthető.
A vegyivédelemi zászlóalj a Magyar Honvédség egyetlen speciális ABV felderítő és mentesítő képességekkel rendelkező alakulata. Alaprendeltetésében – az idézett miniszteri alapító okirat szerint – a nukleáris balesetelhárítási feladatok meghatározó fontosságúak. Ez a tervezési és a kiképzési feladatok végrehajtása során egyaránt érvényesül.

## IRODALOMJEGYZÉK

[1] Hadtudományi Lexikon, Főszerkesztő: Szabó József, Magyar Hadtudományi Társaság, Budapest, 1995, 624. o.

[2] A Magyar Honvédség feladatai a Magyar Köztársaság katasztrófaelhárítási rendszerében, Kézikönyv, Szerző feltüntetése nélkül, Budapest, 2004, 7. o.

[3] http://www.hik.hu/tankonyvtar/site/books/b108/ch08s05s02s03.html/ 2008-04-19

[4] http://www.magyarorszag.hu/kereses/jogszabalykereso/pf/SearchLaw/searchLaw/ 2008. április 19.

[5] http://www.magyarorszag.hu/kereses/jogszabalykereso/pf/SearchLaw/searchLaw/ 2008. április 19.

[6] A Honvédelmi Miniszter 35/2007. (HK. 4.) határozata, Honvédségi Közlöny, 2007. évi 4. szám, 233-234. o.

[7] Mentesítési szakutasítás, szerző feltüntetése nélkül, Budapest, 1987, 28. o.

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Sipos Jenő**
Zrínyi Miklós Nemzetvédelmi Egyetem
sipos.jeno@zmne.hu

**Apostol Attila**
Zrínyi Miklós Nemzetvédelmi Egyetem
apostol.attila@gmail.com

# KALIBRÁLÁSI MŰVELETEK: DIGITÁLIS ÉS ANALÓG MULTIMÉTEREK

***Absztrakt***

*Nem elegendő egy műszer alkalmasságára csupán a megvásárlásakor gondolni, a későbbiekben is gondoskodni kell arról, hogy az általa mutatott értékek és a mérendő mennyiség helyes értéke között az összefüggés megmaradjon. Erre szolgál a mérőeszközök zöménél a kalibrálás, amelyet meghatározott periódusidőnként el kell végezni, ha biztosítani kívánjuk a műszerünk által mutatott értékek elfogadhatóságát. Ez a cikk alkalmazási segédletként szolgál az MSZ EN ISO/IEC 17025:2005 szabvány szerinti kalibrálási eljárások készítéséhez, célszerűen követi a NAR-18-VIII dokumentum felépítését.*

*Thinking about an instrument's adequacy when you buy it is not enough, later on you must take care of it to keep the coherence between the values showed by the instrument and the adequate value of the amounts to be measured. For this reason, for the most of the meters we use calibration, which is needed to be done periodically in order to guarantee the acceptability of the values showed by our instrument. This article is used as an application aid for preparing calibration proceedings in accordance with the standard MSZ EN ISO/IEC 17025:2005, and it expediently follows the structure of the NAR-18-VIII document.*

***Kulcsszavak:*** *kalibrálás, etalon, mérőeszköz, eredő bizonytalanság ~ calibration, etalon, meter, resultant uncertainty*

## 1. A kalibrálási eljárás hatálya

Ez a kalibrálási eljárás olyan digitális vagy analóg kijelzésű elektromos mérőeszközök kalibrálására vonatkozik, amelyek az alábbi üzemmódok közül eggyel vagy többel (multiméterek) rendelkeznek:

- egyenfeszültség mérése a 0…1000 V feszültségtartományban;
- szinuszos lefolyású váltakozó feszültség effektív értékének mérése a 0…100 V feszültség- és a 10 Hz…100 kHz frekvenciatartományban, a 100…300 V feszültség- és a 40 Hz…30 kHz frekvenciatartományban, illetve a 300...1000 V feszültség- és a 40 Hz...10 kHz frekvenciatartományban.

- egyenáram mérése a 0…20 A áramtartományban;
- szinuszos lefolyású váltakozó áram effektív értékének mérése a 0…300 mA áram- és a 10 Hz…30 kHz frekvenciatartományban, illetve a 0,3…20 A áram- és a 10 Hz…10 kHz frekvenciatartományban;
- egyenáramú elektromos ellenállás mérése 2- és/vagy 4-vezetékes kapcsolásban, a 10 Ω…400 MΩ ellenállás-tartományban.[1]

A kalibrálható mérőeszközök kézi vagy asztali kialakításúak lehetnek, legfeljebb $5^1/_2$ digit ($N_{max} \sim 200000$) kijelzés mellett.

## 2. A kalibrálás elve

A kalibrálandó mérőeszközök minden üzemmódját etalon státusú célműszerrel (esetünkben Wavetek-9100 tip. kalibrátor) reprodukált mennyiségek közvetlen mérésével kalibráljuk.

## 3. A kalibrálással meghatározandó metrológiai jellemzők

A metrológiai jellemzők meghatározásának alapja általában a kalibrálandó mérőeszköz gyári specifikációja. Az üzemmódok, a méréshatárok, a frekvenciatartományok meghatározása és az alapfokozat kijelölése, illetve az alkalmazandó kiegészítők (mérővezetékek, stb.) megválasztása ennek segítségével történhet. Általában azonban a kalibrálás a gyári specifikáció hiányában is elvégezhető egyéb pl. a megrendelő kívánsága szerint, a műszaki gyakorlatra alapozva.

A jelen eljárás szerint kalibrált mérőeszközök metrológiai jellemzőit a következők szerint határozzuk meg.

### 3.1 Linearitás

A linearitás a kalibrált mérőeszköz hibájának, vagy eltérésének – a mért és a helyes érték különbségének – függése a mért értéktől. A linearitás ellenőrzését az alapfokozatnak megfelelő méréstartomány (8.1 pont) alsó és felső méréshatárai között általában egyenlő közűen kijelölt pontokban végezzük el.

Multiméterek áram-, és ellenállásmérő üzemmódjában a linearitást nem ellenőrizzük, csak pontosságellenőrzést végzünk. Egyfunkciós ellenállásmérők linearitás ellenőrzését azoknak az 1 kΩ-hoz legközelebbi méréstartományában végezzük el.

### 3.2 Pontosság

A pontosság a mérőeszköz értékmutatása és a mért mennyiségnek a kalibráló etalonnal megvalósított értéke közötti egyezés kvantitatív jellemzése a talált eltéréssel. A talált eltérés a kalibrált mérőeszköz hibájának becslése. A mérési hibák a mért értékkel arányosak, ezért a mérőeszköz pontosságát a méréstartományok felső határán, vagy annak közelében ellenőrizzük azokban a méréstartományokban, amelyekben linearitás ellenőrzést nem végeztünk.

[1]Természetesen a mérendő mennyiségek, a méréstartományok esetleg a befolyásoló mennyiségek felsorolása tovább folytatható abban az esetben, ha ez az eszköz használata, illetve a kalibrálás eredménye szempontjából fontos. [1]

### 3.3 Frekvenciafüggés

A frekvenciafüggés a mérőeszköz pontosságának függése az etalonnal generált (szinuszos lefolyású) mérendő mennyiség frekvenciájától. A frekvenciafüggésből eredő járulékos mérési hibák a mért értékkel arányosak, ezért azt a méréstartományok felső határán ellenőrizzük, a gyárilag specifikált alsó- és felső határfrekvencián.

### 3.4 Egyéb (megrendelői) igények

A teljes körű kalibráláshoz tartozó metrológiai jellemzők egy részének meghatározásától el lehet tekinteni pl. a megrendelő írásbeli megbízása alapján, tehát lehetőség van részkalibrálásra. Minden, a specifikációnak megfelelő teljes körű kalibrálástól a megrendelő igényei miatti eltérést a kalibrálási bizonyítvány megjegyzésében jelezni kell.

## 4. Jelölések és mértékegységek

A jelen kalibrálási eljárásban használt mennyiségek jelét, megnevezését és az alkalmazható (mérték) egységeket a következő táblázat tartalmazza.

| Jel | Megnevezés | Egység |
|---|---|---|
| $X_m$ | a kalibrálandó mérőeszközzel mért mennyiség | V, A, Ω |
| $X_h$ | az etalonnal generált mennyiség (helyes érték) | V, A, Ω |
| $u_{ek}$ | az etalon kalibrálásának standard bizonytalansága | V, A, Ω, vagy relatív |
| $u_{es}$ | az etalon stabilitásának standard bizonytalansága két visszavezetés között | V, A, Ω, vagy relatív |
| $\Delta_e$ | az etalon specifikált hibatartománya | V, A, Ω, vagy relatív |
| $\Delta_{sp}$ | kalibrált mérőeszköz specifikált hibatartománya | V, A, Ω, vagy relatív |
| $U_{kal}$ | kalibrálási mérés kiterjesztett bizonytalansága | V, A, Ω, vagy relatív |
| $u_f$ | a kalibrált műszer véges felbontása miatti standard bizonytalanság | V, A, Ω, vagy relatív |
| $u_{le}$ | a kalibrált műszer leolvasási standard bizonytalansága | V, A, Ω, vagy relatív |
| $U_{LMK}$ | a laboratórium legjobb mérési képessége | V, A, Ω, vagy relatív |
| h | mérési hiba, $h = X_m - X_h$ | V, A, Ω |
| k | kiterjesztési tényező | 1 |
| t | környezeti hőmérséklet | $^oC$ |

## 5. Eszközök

### 5.1 Etalonok

A kalibráláshoz etalon jelforrásként esetünkben a Wavetek-9100 típusú kalibrátort alkalmazzuk. Az ezzel az etalonnal kalibrálható mérőeszközök körét a következők szerint határozzuk meg:

- A mérőeszközöknek csak olyan funkcióit és/vagy méréstartományait kalibráljuk, amelyekre nézve a laboratórium legjobb mérési képességének háromszorosa nem nagyobb,

mint a kalibrálandó mérőeszköz gyári specifikációjának megfelelő ± $\Delta_{sp}$ hibatartomány fél szélessége, azaz a kalibrálás pontossági tartaléka legalább 3. Azaz:

$$\Delta_{sp} \geq 3 \cdot U_{LMK} \tag{5.1}$$

A legjobb mérési képességek meghatározását lásd a 8.3 pontban. [2]

- Nem kalibrálunk $5^1/_2$ digit-nél ($N_{max}$ ~ 200000) hosszabb kijelzésű mérőeszközöket.

### 5.2 Egyéb mérőeszközök

A környezeti hőmérsékletet a kalibrálás során hőmérővel mérjük.

### 5.3 Segédeszközök

Az etalon és a kalibrálandó mérőeszköz összekapcsolását annak saját mérővezetékeivel végezzük. Ilyenek hiányában a csatlakoztatásokat 1 m hosszúságú, 2 mm$^2$ keresztmetszetű, sodrott, mindkét végén banán csatlakozóval szerelt mérővezetékekkel végezzük el. Négy darab ilyen vezetéket az 5.1. pont szerinti etalon tartozékaként kezelünk.

## 6. Környezeti feltételek és stabilizálódási idő

A kalibrálás egyetlen lényeges befolyásoló mennyisége a laboratóriumi környezet hőmérséklete. A környezeti hőmérsékletnek az etalon és a kalibrálandó mérőeszköz bemelegítésének megkezdése előtt egy órával már, és a kalibrálás teljes tartama alatt az etalon specifikációjának megfelelő +(23 ± 5) $^o$C hőmérséklettartományban kell lennie. Ezt kalibrált hőmérővel ellenőrizzük, és ezen a hőmérséklettartományon kívül kalibrálást nem végzünk. Az etalon specifikációja szerint a hőmérsékletnek a fenti tartományon belüli változásai járulékos bizonytalanságot nem okoznak.

A metrológiai jellemzők stabilizálódásához az etalon és a kalibrálandó mérőeszköz gépkönyveiben megadott bemelegedési idők közül a hosszabbikat kell biztosítani. A kalibrátor – specifikáció szerint – a bekapcsolás után 90 percnyi bemelegedési időt igényel.

## 7. Átvétel és előkészítés

### 7.1 Átvételi feltételek (ellenőrzés)

Kalibrálandó mérőeszközt a laboratórium személyzetének olyan tagja veheti át kalibrálásra, akinek feladata az elektromos mérőeszközök kalibrálása, vagy a kalibrálás felügyelete, irányítása. Mivel a mérőeszköz szállítása csak a gépkönyvében vagy műszerkönyvében előírt módon történhet, ezért átvételkor ellenőrizni kell, hogy az előírt szállítási feltételek teljesültek-e (az előírt rövidzárakat, rögzítéseket, védőkupakot, korrózióvédelmet, stb. alkalmazták-e).

### 7.2 Jelölés (címkézés) és nyilvántartásba vétel

A megrendelés sorszámát az átvevő tünteti fel a műszerkísérő címkén, ő vezeti be (vagy ellenőrzése mellett vezetik be) a megrendelést a kalibrálási nyilvántartóba és ő igazolja az átvételt aláírásával. Az átvevő gondoskodik arról, hogy a mérőeszközt a kalibráló helyiségbe, vagy a beérkező műszerek raktárába szállítsák.

### 7.3 Előkészítés, beállítások és a működőképesség ellenőrzése

Az etalon kalibrátort és a kalibrálandó mérőeszközt összekapcsoljuk azok gépkönyveiben megadott szempontok szerint. Ezek speciális mérővezetékek alkalmazására, a guard- és a sense vezetékek kezelésére, két- és négyvezetékes ellenállásmérésre, a földhurkok elkerülésére, autozéró, szűrő stb. alkalmazására vonatkozhatnak.

Ha a kalibrálandó mérőeszköz telepes táplálású, úgy gondoskodunk az akkumulátor teljes feltöltéséről, vagy az elemeket új alkáli elemekre cseréljük ki. Ha a mérőeszköznek van elemállapot-figyelő opciója, annak információit a kalibrálás ideje alatt figyelemmel kísérjük.

Az etalon és a mérőeszköz kezelőszerveit az első kalibrálási műveletnek megfelelően beállítjuk. A kalibrálandó mérőeszköz elektromos és/vagy mechanikus nulláját szükség szerint beállítjuk.

A kalibrálás során használt etalonokat és a kalibrálandó mérőeszközt bemelegítjük a 6. pont szerint. Ezután a mérőeszköz minden kalibrálandó mérőképességének minden méréstartományában egy mérési ponton ellenőrző mérést végzünk a kalibrálással azonos módon, és a mérések eredményeit azonnal kiértékeljük. Ha durva mérési hibára utaló eredményt kapunk bármelyik ellenőrző mérés során, akkor az etalon működését ellenőrizzük. Ha az ellenőrzés a kalibrálandó mérőeszköz nem megfelelő működését, vagy működésképtelenségét mutatja ki, akkor jegyzőkönyvet veszünk fel. Ennek során a kalibrálással megbízott személyen kívül a laboratórium egy másik munkatársának is jelen kell lennie, aki független tanúként igazolja a jegyzőkönyvben foglaltakat.

Funkcionálisan hibás mérőeszköz kalibrálását nem kezdjük meg, hanem kezdeményezzük a megbízó értesítését.

### 7.4 Biztonsági intézkedések

Az etalon kalibrátor életveszélyes nagyságú elektromos feszültségek generálására képes. A balesetek elkerülése érdekében a gépkönyvben leírt kezelési eljárás maradéktalan betartását a laboratórium vezetőjének rendszeresen ellenőriznie kell. Nem szabad megengedni helytelen kezelési rutin kialakulását és rögzülését. Ezen felül a kalibráló személy(eke)t a megfelelő, körültekintő munkavégzés ide vonatkozó különös szabályairól rendszeres időközönként oktatni, és az oktatás megtörténtét naplózni kell. Ezt a legalább évenkénti rendszeres baleset-megelőzési oktatás keretében lehet elvégezni.

### 7.5 Jegyzőkönyv előkészítése

A bemelegítés alatt kell kitölteni a kalibrálási jegyzőkönyvnek a kalibrált eszközre, az etalonra és a kalibrálás körülményeire vonatkozó részét, valamint ellenőrizni és feljegyezni a környezeti hőmérsékletet, amint azokat az előnyomtatott jegyzőkönyv-űrlap tartalmazza.

## 8. Kalibrálás [2] [3] [4]

### 8.1 Kalibrálási műveletek

Digitális kijelzésű mérőeszköz kalibrálása során helyes értéknek a kalibrátoron beállított névleges értéket tekintjük korrekció nélkül, a mért értéket pedig a kalibrálandó mérőeszközről olvassuk le. A kalibrált mérőeszköz kijelzésének esetleges instabilitását a 8.2 pont szerint vesszük figyelembe.

Analóg kijelzésű mérőeszköz kalibrálásakor – a leolvasási bizonytalanság csökkentése érdekében – a kalibrátor kimeneti mennyiségének finom szabályozásával állunk rá adott ellenőrzési pontnak megfelelő skálaosztásra. A beállítást két irányból végezzük: monoton

növekvő, és monoton csökkenő kimeneti mennyiség-értékeken keresztül, a csapágysúrlódás miatti hiszterézis figyelembevételére. Ebben az esetben a helyes értéket a 8.2 pont szerint számítással határozzuk meg.

A metrológiai jellemzők mérése során alkalmazott ellenőrzési pontok (névleges értékek) meghatározása a következők szerint történik:

a) Linearitás ellenőrzése digitális kijelzés esetén

A teljes méréstartományt – ha a megrendelő másképp nem rendelkezik – legalább 5 és legfeljebb 9 egyenlő részre osztjuk, és az ellenőrzési pontokat ennek megfelelően tűzzük ki, majd a kalibrálást az aktív 0-nak[2] megfelelő névleges értékkel kezdjük. A mérőeszköz túlcsordulásának, vagy az automatikus méréshatár váltásnak elkerülése érdekében a helyes értéket a felső méréshatárra nem állíthatjuk be, ezért a legnagyobb értékű ellenőrzési pontot a felső méréshatár és annak 90 %-a között jelöljük ki.

Abban az esetben, ha a kalibrálandó mérőeszköz gyári specifikációja nem érvényes a teljes méréstartományban, úgy az ellenőrzési pontok kitűzését általában a specifikációnak megfelelően végezzük el kivéve, ha a megrendelő másképpen rendelkezik.

A linearitást a mérőeszköz alapfokozatának megfelelő méréstartományban ellenőrizzük. Alapfokozatban működik a mérőeszköz egyen- vagy váltakozó feszültségmérő üzemmódjának abban a méréstartományában, amelyben a legkisebb bemeneti osztó, és a legkisebb erősítés van bekapcsolva, ezért itt a legjobb a mérőeszköz specifikációja. Ez általában az 1…10 V-hoz legközelebbi méréstartomány.

Egyenfeszültség mérő üzemmódban a linearitás ellenőrzését mindkét polaritásban el kell végezni. Váltakozó feszültség mérő üzemmódban a linearitást a specifikált referencia frekvencián, specifikáció hiányában általában 1 kHz-en, kézi multiméterek esetében 50 Hz-en, vagy a specifikált frekvenciahatárok mértani közepének megfelelő frekvencián ellenőrizzük. Ha a mérőeszköznek csak áram üzemmódja van, akkor a 100 mA-hez legközelebbi egyen- és/vagy váltakozóáramú méréshatárban ellenőrizzük a linearitást.

Ellenállásmérő üzemmódban a linearitást az 1 kΩ-hoz legközelebbi méréstartományban ellenőrizzük.

Kapacitásmérő üzemmódban a linearitást az 1 μF-hoz legközelebbi méréstartományban ellenőrizzük.

Frekvenciamérő üzemmódban a linearitást az 1 kHz-hez legközelebbi méréstartományban ellenőrizzük.

b) Linearitás ellenőrzése analóg kijelzés esetén

A linearitást – ha a megrendelő másképp nem rendelkezik – a skála fő osztásvonalain ellenőrizzük. A kalibrálást a nulla skálaosztáson kezdjük, ahol csak mechanikai, és ha szükséges elektromos nullázást végzünk, rövidrezárt bemenet mellett.

A linearitás ellenőrzésének méréstartományait az a) pont szerintieknek megfelelően választjuk ki az analóg kijelzésű mérőeszközök sajátosságainak figyelembevételével.

Reciprok skálájú analóg mérőeszköz esetén a linearitást csak a megrendelő kívánságára ellenőrizzük, a skála 1-el megírt, és a tőle balra eső, 10-el megírt osztásai között.

c) Pontosság ellenőrzése

Digitális kijelzés esetén a pontosságot a felső méréshatár és annak 90 %-a között, egy ponton ellenőrizzük.

Analóg kijelzés esetén a pontosságot a skála legnagyobb értékű fő osztásvonalán ellenőrizzük.

Reciprok skálájú analóg mérőeszköz esetén – ha a megrendelő másképp nem igényli – minden méréstartományban a skála 1-el megírt osztásánál ellenőrizzük a pontosságot.

d) Frekvenciafüggés ellenőrzése

[2] 0-ra beállított kimenő mennyiség, bekapcsolt kimenet

A frekvenciafüggést a specifikált alsó- és felső határfrekvenciákon ellenőrizzük, minden méréstartománynak azon az ellenőrzési pontján, ahol a pontosságot ellenőriztük referencia frekvencián.

### 8.1.1 A kalibrálási műveletek sorrendje

Multiméterek esetében a kalibrálási műveletek sorrendje általában a következő:

- DC feszültség alapfokozat linearitása. A linearitás ellenőrzését mindkét polaritású bemeneti feszültséggel elvégezzük.
- DC feszültség méréstartományok pontosságának ellenőrzése mindkét polaritású bemeneti feszültséggel.
- DC áram méréstartományok pontosságának ellenőrzése mindkét polaritású bemeneti árammal.
- AC feszültség alapfokozat linearitásának ellenőrzése referencia frekvencián. A referencia frekvencia kézi multiméterek esetén általában 50 Hz, egyébként 1 kHz.
- AC feszültség méréstartományok pontosságának ellenőrzése referencia frekvencián.
- AC áram méréstartományok pontosságának ellenőrzése referencia frekvencián. A referencia frekvencia kézi multiméterek esetén általában 50 Hz, egyébként 1 kHz.
- AC feszültség méréstartományokban a frekvenciafüggés ellenőrzése.
- AC áram méréstartományokban a frekvenciafüggés ellenőrzése.
- Egyenáramú ellenállás mérés linearitásának ellenőrzése.
- Egyenáramú ellenállás méréstartományok pontosságának ellenőrzése.
- Kapacitás mérés linearitásának ellenőrzése.
- Kapacitás méréstartományok pontosságának ellenőrzése.
- Frekvencia mérés linearitásának ellenőrzése.
- Frekvencia méréstartományok pontosságának ellenőrzése.

Adott kalibrálandó mérőeszköz esetén ez a lista szűkülhet egészen az egyfunkciós mérőeszköz (pl. digitális DC feszültségmérő) kalibrálására is. Minden ilyen esetben a fentieket értelemszerűen kell alkalmazni.

A kalibrálási jegyzőkönyvben feljegyezzük az összes ellenőrzési ponton a kalibrátoron névlegesként beállított $X_h$ helyes értékeket és az ezekhez tartozó $X_m$ mért értékeket, vagy azokat az értékeket, amelyekből a mért- illetve helyes értékeket számoljuk.

Adott esetben minden kalibrálási mérésfajta, azon belül pedig egy-egy linearitásmérési sorozat elvégzése előtt – általában minden méréshatár váltás után, illetve szükség/előírás szerint – a kalibrálandó mérőeszközt nullázni kell. Ehhez esetleg a kábelezést meg kell bontani. A visszaállítás különös gonddal történjen.

## 8.2 A metrológiai jellemzők kiszámítása

A metrológiai jellemzők számításához szükséges mért- és helyes értékek meghatározásához a következőket vesszük figyelembe:

- Analóg kijelzésű mérőeszköz esetén a két irányból történő osztásra állás során a kalibrátorról leolvasott két érték számtani középértékét fogadjuk el helyes értéknek. Mért értéknek pedig az osztáshoz tartozó névleges értéket tekintjük
- Digitális kijelzés esetén mért értéknek a kalibrátor kapcsolási tranziensének lecsillapodása után kijelzett, stabilizálódott értéket vesszük figyelembe. Ha a kijelzés nem stabilizálódik egyetlen érték mutatására, úgy az instabilitást, vagy ismétlőképességet a 8.3.2.1 pont szerint vesszük figyelembe.

A kalibrálás során rögzített, vagy kiszámolt összetartozó mért- és helyes értékek különbségeként számítjuk ki a kalibrált műszer hibáját, vagy eltérését:

$$h = X_m - X_h \tag{8.1}$$

Ez a kalibrálás definíciószerű eredménye, annak a következő pontban tárgyalt bizonytalanságával együtt.

### 8.3 A kalibrálás bizonytalanságának meghatározása

A kalibrálás bizonytalanságát az EA-4/02 dokumentum szerint határozzuk meg. Az eredő mérési bizonytalanság általunk figyelembe vett tényezői a következők.

#### 8.3.1 Az etalon bizonytalanságának tényezői. Legjobb mérési képesség

a) Az etalon visszavezetésének standard bizonytalansága.

Az etalon visszavezetésének (kalibrálásának) $U_{ek}$ eredő kiterjesztett bizonytalanságát a kalibrálási bizonyítvány tartalmazza az etalon minden egyes funkciójára, k = 2 kiterjesztési tényezővel. Ebből az etalon kalibrálásának standard bizonytalansága:

$$u_{ek} = U_{ek}/2 \tag{8.2}$$

b) Az etalon stabilitása annak két kalibrálása között.

Az etalon két kalibrálás között (az adott etalon esetében legfeljebb egy évig) érvényes pontossági specifikációját annak gépkönyve tartalmazza. A szimmetrikus, $\pm\Delta_{es}$ alakú specifikáció két hibahatár, amelyek egy $2\cdot\Delta_{es}$ szélességű hibasávot vagy hibatartományt határoznak meg. A funkcionálisan hibátlan (valamint rendszeresen kalibrált és annak alapján szükség szerint beszabályozott) etalon hibája ebből a tartományból nem lép ki, ezen belül viszont az eloszlásról semmiféle információnk nincs.

Ha az etalon hibáját a fentiek alapján határaival megadott, zérus várható értékű, egyenletes eloszlású valószínűségi változónak tekintjük akkor annak standard bizonytalansága:

$$u_{es} = \frac{2\cdot\Delta_{es}}{\sqrt{12}} = \frac{\Delta_{es}}{\sqrt{3}} \tag{8.3}$$

c) Az etalonnal kapcsolatos egyéb bizonytalansági tényezők.

Az etalon gépkönyve szerint annak a +(23 ± 5) °C hőmérséklettartományban járulékos, hőmérsékletváltozás miatti hibája nincs.

Az etalon kalibrátoron a kalibrálandó mérőeszköz terhelési hibát nem okoz.

Tekintettel arra, hogy a fentieken kívül a kalibrálás bizonytalansági tényezői között már csak a kalibrálandó mérőeszköz véges felbontása miatti bizonytalanság szerepel, ezért a laboratórium $U_{LMK}$ legjobb mérési képességeit a (8.1) és (8.2) szerint kiszámított standard bizonytalanságok eredőjének a k = 2 kiterjesztési tényezővel való szorzataként határozzuk meg:

$$U_{LMK} = 2\cdot\sqrt{u_{ek}^2 + u_{es}^2} \tag{8.4}$$

A kalibrálási szolgáltatások táblázatának megfelelő oszlopában az így kiszámított értékek szerepelnek.

#### 8.3.2 A kalibrált mérőeszköz kijelzéséből eredő bizonytalanság

8.3.2.1 Digitális kijelzésnél a legkisebb helyi érték 1 digitjénél finomabb kijelzés nem lehetséges, azaz a digitális kijelzésnek rendszertechnikai okból van egy $\Delta_f$= 1 digit szélességű holt sávja. Ezzel a felbontásból eredő standard bizonytalanság:

$$u_f = \frac{d}{2\cdot\sqrt{3}} = 0{,}29\cdot d \tag{8.5}$$

ahol d a legkisebb kijelzett helyi érték 1 digitjének megfelelő mennyiség. A felbontási bizonytalanságnak az $X_m$ mért értékre vonatkozó %-os relatív értéke:

$$u_{fr}^{\%} = \frac{1}{2 \cdot \sqrt{3}} \cdot \frac{d}{X_m} \cdot 100 = 29 \cdot \frac{d}{X_m} \qquad (8.6)$$

Ha a kalibrálandó mérőeszköz kijelzése a tranziens lecsengése után a legkisebb helyi érték egy digitjénél nagyobb ingadozásokat mutat a zaj miatt, akkor a következők szerint járunk el:

a) Rövid ideig megfigyelve a mért értékeket, megállapítjuk és feljegyezzük a legkisebb $X_{mmin}$ és a legnagyobb $X_{mmax}$ mért értéket.

b) Meghatározzuk ezek különbségét és a (8.5)-ben d helyére ezt helyettesítjük:

$$d_{zaj} = X_{mmax} - X_{mmin}$$

c) Mért értéknek ebben az esetben az alábbi átlagot fogadjuk el:

$$X_{mátlag} = (X_{mmax} + X_{mmin})/2 \qquad (8.7)$$

A kiszámított átlagértéket a komponensek legkisebb helyi értékéig kerekítjük.

d) Relatív érték számításához (8.6)-ba $d_{zaj}$ és $X_{mátlag}$ értékeit helyettesítjük.

Az instabil kijelzés megfigyelt határai közötti tartomány nem lehet nagyobb, mint a legkisebb helyi értékű digit tízszerese. Ha a talált instabilitás nagyobb, úgy ezt a kalibrálási bizonyítvány megjegyzés rovatában közöljük.

8.3.2.2 Analóg kijelzés esetén a leolvasási hiba okoz bizonytalanságot. Ha a skála osztásértéke d, és a mutató helyzetét ennek tört, m-ed részényi leolvasási hibával tudjuk megbecsülni, akkor a leolvasásból eredő standard bizonytalanság:

$$u_{le} = \frac{d}{2 \cdot m \cdot \sqrt{3}} \qquad (8.8)$$

Ennek az $X_m$ mért értékre vonatkoztatott százalékos értéke:

$$u_{ler}^{\%} = \frac{1}{2 \cdot m \cdot \sqrt{3}} \cdot \frac{d}{X_m} \cdot 100 = \frac{29}{m} \cdot \frac{d}{X_m} \qquad (8.9)$$

Osztásközben álló mutató esetén m = 2 ... 5 lehet, osztásra állított mutató esetén – a jelen eljárás szerinti kalibrálásoknál minden esetben – pedig m = 10 ... 20 értéket lehet figyelembe venni a skálahossztól, az osztások számától, valamint a mérő személy gyakorlottságától függően. Ebben a kalibrálási eljárásban m = 10 értéket választunk a leolvasás standard bizonytalanságának becsléséhez. Ezzel:

$$u_{le} = 0{,}029 \cdot d \qquad (8.8.a)$$

illetve

$$u_{ler}^{\%} = 2{,}9 \cdot \frac{d}{X_m} \qquad (8.9.a)$$

### 8.3.3 A kalibrálás eredő bizonytalansága

A kalibrálás eredő standard bizonytalansága a 8.3.1 és 8.3.2 pontokban kiszámított standard bizonytalanságok eredője:

$$u_{kal} = \sqrt{u_{ek}^2 + u_{es}^2 + [u_f \text{ vagy } u_{le}]^2} \qquad (8.10)$$

A kalibrálás eredő kiterjesztett bizonytalansága k = 2 kiterjesztési tényező mellett:

$$U_{kal} = 2 \cdot u_{kal} \qquad (8.11)$$

Az alábbiakban táblázatos formában bemutatjuk a jelen eljárás szerinti kalibrálási mérések bizonytalansági járulékainak becslését tipikus esetekre vonatkozóan. A számításokat a 8.3.1, a 8.3.2 és a 8.3.3 pontok szerint végeztük el.

a) Egyenfeszültség mérő. Méréshatár: 20 V, kijelzés: $4\ ^1/_2$ digit, kalibrálás a mh-on.

| Bizonytalansági járulékot okozó mennyiség | Becslése | Standard bizonytalanság értelmezése | Értéke $u(x_i)$ | Érzékenységi együttható $c_i$ | $c_i \cdot u(x_i)$ |
|---|---|---|---|---|---|
| Etalon értéke kalibrálás után | $X_h$ | $u_{ek} = U_{ek}/2$ | 0,40mV | 1 | 0,40 mV |

| | | | | | |
|---|---|---|---|---|---|
| Etalon stabilitása két kalibrálás között | 0 | $u_{es} = \Delta_{es}/\sqrt{3}$ | 0,98 mV | 1 | 0,98 mV |
| Kalibrálandó műszerrel mért érték | $X_m$ | $u_f = d/(2\cdot\sqrt{3})$ | 0,29 mV | 1 | 0,29 mV |
| Hiba: | $h=X_m-X_h$ | Eredő standard bizonytalanság: | | | u(y)=1,1 mV |

A kalibrálás eredő kiterjesztett bizonytalansága k = 2 mellett: $\mathbf{U_{kal}}$ **= 2,2 mV**, ami relatív értékben megfelel **0,011 %**-nak a mért értékre vonatkoztatva.

b) Egyenáram mérő. Méréshatár: 20 mA, kijelzés: 4 $^1/_2$ digit, kalibrálás a mh-on.

| Bizonytalansági járulékot okozó mennyiség | Becslése | Standard bizonytalanság értelmezése | Értéke $u(x_i)$ | Érzékenységi együttható $c_i$ | $c_i \cdot u(x_i)$ |
|---|---|---|---|---|---|
| Etalon értéke kalibrálás után | $X_h$ | $u_{ek} = U_{ek}/2$ | 1,2 μA | 1 | 1,2 μA |
| Etalon stabilitása két kalibrálás között | 0 | $u_{es} = \Delta_{es}/\sqrt{3}$ | 2,1 μA | 1 | 2,1 μA |
| Kalibrálandó műszerrel mért érték | $X_m$ | $u_f = d/(2\cdot\sqrt{3})$ | 0,29 μA | 1 | 0,29 μA |
| Hiba: | $h=X_m-X_h$ | Eredő standard bizonytalanság: | | | u(y)=2,4 μA |

A kalibrálás eredő kiterjesztett bizonytalansága *k* = 2 mellett: $\mathbf{U_{kal}}$ **= 4,8 μA**, ami relatív értékben megfelel **0,024 %**-nak a mért értékre vonatkoztatva.

c) Váltakozó feszültség mérő. Méréshatár:200 V, kijelzés:3 $^1/_2$ digit, frekvencia: 1 kHz, kalibrálás a méréshatáron.

| Bizonytalansági járulékot okozó mennyiség | Becslése | Standard bizonytalanság értelmezése | Értéke $u(x_i)$ | Érzékenységi együttható $c_i$ | $c_i \cdot u(x_i)$ |
|---|---|---|---|---|---|
| Etalon értéke kalibrálás után | $X_h$ | $u_{ek} = U_{ek}/2$ | 13 mV | 1 | 13 mV |
| Etalon stabilitása két kalibrálás között | 0 | $u_{es} = \Delta_{es}/\sqrt{3}$ | 23 mV | 1 | 23 mV |
| Kalibrálandó műszerrel mért érték | $X_m$ | $u_f = d/(2\cdot\sqrt{3})$ | 29 mV | 1 | 29 mV |
| Hiba: | $h=X_m-X_h$ | Eredő standard bizonytalanság: | | | u(y)=39 mV |

A kalibrálás eredő kiterjesztett bizonytalansága k = 2 mellett: $\mathbf{U_{kal}}$ **= 78 mV**, ami relatív értékben megfelel **0,039 %**-nak a mért értékre vonatkoztatva.

d) Váltakozó áram mérő. Méréshatár: 2 A, kijelzés: 3 $^1/_2$ digit, frekvencia:50 Hz

| Bizonytalansági járulékot okozó mennyiség | Becslése | Standard bizonytalanság értelmezése | Értéke $u(x_i)$ | Érzékenységi együttható $c_i$ | $c_i \cdot u(x_i)$ |
|---|---|---|---|---|---|
| Etalon értéke kalibrálás után | $X_h$ | $u_{ek} = U_{ek}/2$ | 0,24 mA | 1 | 0,24 mA |

| | | | | | |
|---|---|---|---|---|---|
| Etalon stabilitása két kalibrálás között | 0 | $u_{es} = \Delta_{es}/\sqrt{3}$ | 1,4 mA | 1 | 1,4 mA |
| Kalibrálandó műszerrel mért érték | $X_m$ | $u_f = d/(2\cdot\sqrt{3})$ | 0,29 mA | 1 | 0,29 mA |
| Hiba: | $h=X_m-X_h$ | Eredő standard bizonytalanság: | | | u(y)=1,45mA |

A kalibrálás eredő kiterjesztett bizonytalansága k = 2 mellett: $\mathbf{U_{kal}}$ **= 2,9 mA**, ami relatív értékben megfelel **0,15 %**-nak a mért értékre vonatkoztatva.

e) Ellenállásmérő. Méréshatár: 1000 Ω, kijelzés: 5 $^1/_2$ digit, kalibrálás 1000 Ω-on

| Bizonytalansági járulékot okozó mennyiség | Becslése | Standard bizonytalanság értelmezése | Értéke $u(x_i)$ | Érzékenységi együttható $c_i$ | $c_i \cdot u(x_i)$ |
|---|---|---|---|---|---|
| Etalon értéke kalibrálás után | $X_h$ | $u_{ek} = U_{ek}/2$ | 140 mΩ | 1 | 140 mΩ |
| Etalon stabilitása két kalibrálás között | 0 | $u_{es} = \Delta_{es}/\sqrt{3}$ | 130 mΩ | 1 | 130 mΩ |
| Kalibrálandó műszerrel mért érték | $X_m$ | $u_f = d/(2\cdot\sqrt{3})$ | 2,9 mΩ | 1 | 2,9 mΩ |
| Hiba: | $h=X_m-X_h$ | Eredő standard bizonytalanság: | | | u(y)=190 mΩ |

A kalibrálás eredő kiterjesztett bizonytalansága k = 2 mellett: $\mathbf{U_{kal}}$ **= 380 mΩ**, ami relatív értékben megfelel **0,038 %**-nak a mért értékre vonatkoztatva.

### 8.4 Minősítés

Ha azt a megrendelő kéri, a kalibrálási bizonyítvány minősítés rovatában minősítjük a mérőeszközt. A minősítés alapjául szolgáló metrológiai jellemzők megengedett határértékeinek forrása lehet:

- a gyártó által kiadott gépkönyv,
- szabvány, vagy egyéb ágazati előírás,
- jogszabály, vagy
- a felhasználó által közölt, a szándékolt alkalmazásnak megfelelő hibahatár(ok).

A minősítés csak metrológiai jellemzőkre vonatkozhat, és meg kell adni, hogy a megfelelőségi/nemmegfelelőségi állítás a vonatkozó specifikáció mely pontjára (pontjaira) vonatkozik.

Megfelelőség csak akkor tanúsítható, ha a kalibrálás $U_{kal}$ eredő kiterjesztett bizonytalansága elég kicsi a specifikált $\Delta_s$ tűréshez, vagy hibahatárhoz képest. A laboratórium vállalt pontossági tartaléka (5.1 pont) ezt biztosítja.

A jelen kalibrálási eljárásban szereplő többfunkciós mérőeszköz esetén minden egyes üzemmódra külön-külön lehet minősítést adni. A minősítés megadásának feltételei:

a) A mérőeszköz megfelel az előírásnak, ha minden egyes ellenőrzési ponton

$$|h| + U_{kal} < \Delta_s$$

b) Sem a megfelelőség, sem a nemmegfelelőség nem igazolható, ha legalább egy ellenőrzési ponton

$$|h| + U_{kal} > \Delta_s \qquad \text{és} \qquad |h| - U_{kal} < \Delta_s$$

Ha ebben az esetben $|h| < \Delta_s$, úgy a mérőeszköz megfelelősége valószínűbb, míg ha $|h| \geq \Delta_s$, úgy a mérőeszköz nemmegfelelősége valószínűbb.

c) A mérőeszköz nem felel meg az előírásnak, ha legalább egy ellenőrzési ponton

$$|h| - U_{kal} > \Delta_s$$

ahol:

$|h|$ a mérőeszköz (8.1) képlettel definiált hibájának abszolút értéke adott ellenőrzési ponton,

$U_{kal}$ a kalibrálás eredő kiterjesztett bizonytalansága ugyanitt,

$\Delta_s$ a specifikált tűrés, vagy hibahatár.

A laboratórium által közölt minősítés megbízhatósága kb. 95 %, a kalibrálási bizonytalanság meghatározásának megfelelően.

## FELHASZNÁLT IRODALOM


[1] NAR-18-VIII Útmutató nem szabványos kalibrálási eljárások tartalmára és felépítésére Nemzeti Akkreditáló Testület, Budapest, 2002. január

[2] NAR-EA 4/02 A mérési bizonytalanság meghatározása kalibrálásnál, Nemzeti Akkreditáló Testület, Budapest, 2003. január

[3] Útmutató a mérési bizonytalanság kifejezéséhez (GUM), Országos Mérésügyi Hivatal, Budapest, 1995

[4] Guidelines on Assessment and Reporting of Compliance with Specification, ILAC G8, 1996

Reményi Tibor: Függ-e a kalibrálás bizonytalansága a kalibrált műszertől? (Mérésügyi Közlemények, 2000. június)

http://www.meter.hu/kalibralni_pedig_kell, 2007.05.06 (2008.08.13.)

MSZ EN ISO/IEC 17025:2005 Vizsgáló- és kalibrálólaboratóriumok felkészültségének általános követelményei, Magyar Szabványügyi Testület, Budapest, 2006. május 1.

NAR-22-VIII Segédlet mérési bizonytalanság számításához kalibrálásnál, Nemzeti Akkreditáló Testület, Budapest, 2002. január

Nemzetközi Metrológiai Értelmező Szótár (VIM), OMH - MTA-MMSZ, Budapest, 1998

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Báthy Sándor**
Zrínyi Miklós Nemzetvédelmi Egyetem
bathy.sandor@zmne.hu

# A HONVÉDELMI CÉLÚ TARTALÉKOK SZEREPE AZ ELLÁTÁSI LÁNCBAN

***Absztrakt***

*A cikk témaválasztását elsősorban az indokolta, hogy 2006. áprilisában NATO logisztikai konferencián ismertették a NATO műveleti támogatási lánc menedzsment koncepcióját (NATO Operations Support Chain Management Concept[1]), amely megítélésem szerint egy újabb lépés a NATO logisztikai integrációs folyamatában. Ezt azért integrációs kérdés, mert a katonai logisztika számára maga az ellátási lánc nem új jelenség. A katonai műveletek anyagi támogatásának megszervezésében mindig jelen volt az ellátási lánc alapgondolata, nevezetesen az, hogy honnan, milyen forrásból szerezzük be a harcolóknak szükséges fegyverzetet, ruházatot, élelmet, stb. és azt milyen ellátó-elosztó rendszeren keresztül juttassuk el a felhasználókhoz. Végül, de nem utolsó sorban, az ellátmány „megfelelőségéről" visszajelzést adjunk, és ezzel hatást gyakoroljunk a beszerzőn keresztül a gyártóra, illetve előállítóra.*
***Kulcsszavak:*** *logisztika, ellátási lánc, NATO*

A gazdaságban civil társadalomnak a piaci verseny kiéleződésére volt szüksége ahhoz, hogy a vevő minél tökéletesebb kiszolgálása érdekében a termék előállításában résztvevő valamennyi szereplőt érdekeltté tegye a „legmegfelelőbb" termék létrehozásában.

Mivel az anyagok eljuttatása a misszióban szolgálókhoz civil és katonai ellátási láncokon keresztül történik, amelyeknek más és más tulajdonságai vannak szükségesnek látom, hogy néhány elméleti kérdésre világítsak rá a NATO koncepció és a Magyar Honvédség anyagi támogatása összefüggésében.

Fontosnak tartok néhány gondolatot közre adni a polgári (civil) és katonai ellátási láncok azonos és eltérő vonásairól.

## A polgári (civil) ellátási lánc

Supply Chain Council meghatározása szerint: „Az ellátási lánc minden olyan tevékenységet magában foglal, amely a termék előállításával és kiszállításával kapcsolatos, a beszállító beszállítójától kezdve a végső fogyasztóig bezárólag. A négy fő folyamat – a tervezés, a beszerzés, a gyártás, a kiszállítás – , amely az ellátási láncot meghatározza, magában foglalja a kereslet-kínálat menedzselését, az alapanyagok és alkatrészek beszerzését, a gyártást, az

[1] NATO ACT 1 st Draft 5 April 2006

összeszerelést, a készletezést, a rendelésfeldolgozást, a disztribúciós és a végső fogyasztóhoz való kiszállítást."

Az Egyesült Államokbeli non-profit szervezet idézett megfogalmazása 1997-ből származik, és bár előtte és utána többen is leírták az ellátási láncot, lényegében csak más aspektust jelentenek a vizsgálatban, hiszen arra irányulnak valamennyien, hogy a végső fogyasztó igényeit minél tökéletesebben elégítsék ki.

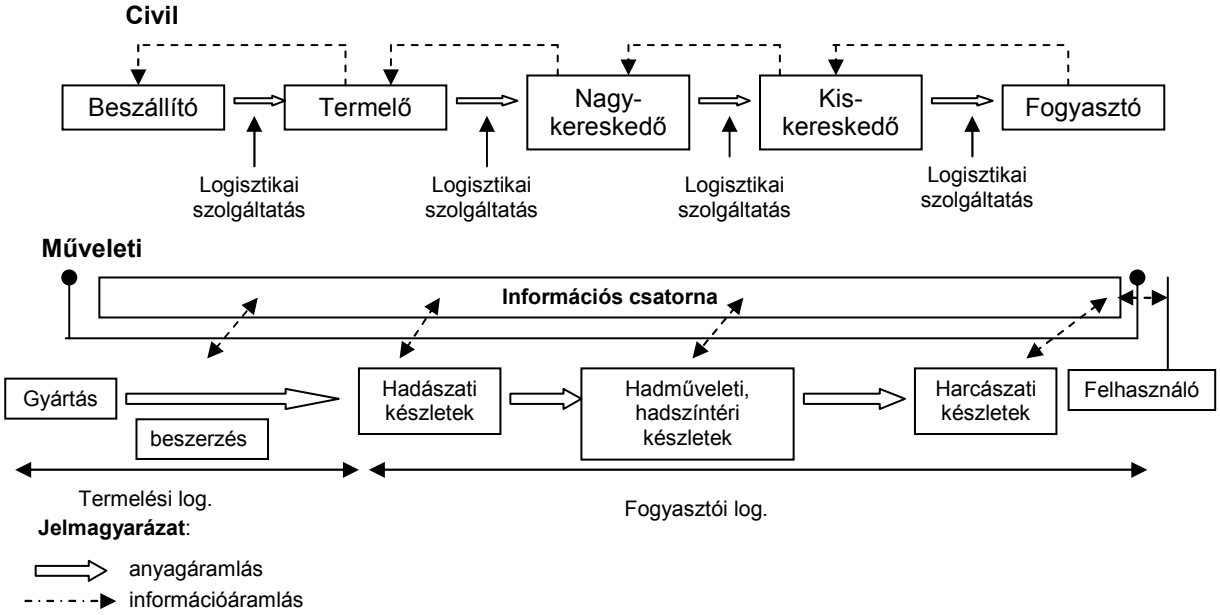
## A MŰVELETI ELLÁTÁSI LÁNC

„Az ellátási lánc lefedi a teljes teret az ellátó, gyártó és a vevő között, amelyben áruk, szolgáltatások és információk mennek keresztül mindkét irányba[2]."

2007-ben a Zrínyi Miklós Nemzetvédelmi Egyetemen tartott előadásában Keszthelyi Gyula dandártábornok már egy átfogóbb fogalommal dolgozott: „Műveleti Logisztikai Lánc (OLC): utánpótlási vonalakon együttműködő logisztikai intézmények és elosztó képességek hálózata, amely fogadja, szállítja, tárolja, elosztja, és újra elosztja a felszerelést, az anyagokat és az állományt a végfelhasználó részére".

A két, illetve három fogalomból kitűnik, hogy a katonai fogalmak csak együtt képezik azt a teljességet, amit a civil ellátási lánc felfogása tükröz. Időben az eltérést (1997-2006) valószínűleg az okozza, hogy a nemzeti logisztikák valamennyien evidenciaként, ellátási láncban működtették saját rendszerüket és csak a többnemzeti logisztika folyamatainak további integrálásához (információ, vezetés) volt szükség a NATO koncepció és program kidolgozására.

Néhány főbb jellemző[3] alapján összehasonlítva a civil és katonai ellátási láncokat a különbözőségek mellett fontos azonosságokat is találunk.




Az ábrákat figyelmesen elemezve szembetűnő, hogy mindkét lánc kezdő és végpontja, azok tartománya azonos és csomópontjai is beazonosíthatóak. Ugyanakkor a logisztika és persze az ellátási lánc célja eltér egymástól, hiszen a (katonai) fogyasztói logisztikának nem célja a profitszerzés, míg a civil ellátási lánc minden egyes eleme ebben érdekelt. Ezt jelzi az a különbség is, hogy míg a civil lánc végpontján fogyasztóként a **vevő** áll, addig a katonai

[2] Supply Chain Management (SCM) developments in NATO Nations and Recommendations for a NATO SCM Concept – Az ellátási lánc menedzsment (SCM) fejlesztései a NATO nemzetek körében és ajánlások a NATO ellátási lánc menedzsment koncepció részére. NATO Study Paper, 2006

[3] Szegedi Zoltán - Prezenszki József: Logisztika menedzsment Kossuth Kiadó 2003 360. oldal

lánc végpontján a **katona, a technika, illetve az objektum áll fogyasztóként,** nem pedig a vevő (vásárló). A termelői logisztika beszerző alrendszere azonban mégis piaci értelemben vett vevőt jelent a gyártó (előállító) felé, de új értéket a szolgáltatásai és a fogyasztói logisztika szolgáltatásai ellenére sem teremt és ezért ellenszolgáltatást sem kap.

Ez azt jelenti, hogy a katonai logisztika esetében a Porter-féle értéklánc csak két tagból áll és kapcsolódó folyamatainál az áru- és információáramlás teljesen, míg a pénzáramlás csak a hadsereg, mint egész és a gyártók, illetve szolgáltatók között működik.

Az ellátási lánc néhány jellemző, meghatározó tulajdonsága, illetve jegye alapján még mélyebb összefüggéseket találhatunk. Összehasonlításul alapul vettem a Szegedi Zoltán és Prezenszki József által készített „Az ellátási lánc főbb jellemzői[4]" táblázatot.

| | **Civil** | **Katonai** |
|---|---|---|
| Cél | az elsődleges cél a fogyasztói igények kiszolgálása; ezt kell egyensúlyba hozni a költségekkel és az eszközök megtérülésével | elsődleges cél a felhasználói igények kielégítése, amit költséghatékonyan kell teljesíteni<br>csak a termelői tag profitorientált |
| Kiterjedés | a teljes folyamatot átfogja, a termék vagy szolgáltatás előállításától a végső fogyasztóhoz történő eljuttatásig | megegyezik |
| Rendszerszemlélet | az összes szereplőt és folyamatot egy egységes rendszerbe integrálja | megegyezik |
| Együttműködés | szervezeti határokon ível át; mind a szervezeten belüli, mind a szervezetek közötti kapcsolatok kiemelkedően fontosak | megegyezik + többnemzeti |
| Megvalósítás eszköze | a kooperációt és koordinációt olyan információs rendszeren keresztül valósítja meg, amelyben a tagok addig titkosan kezelt információkat osztják meg. | megegyezik + együttműködés + NATO koncepció (megbízik a Szövetséges által működtetett láncban, átláthatóvá teszi a rendszert |
| Információ, mint mozgató és hatalmi tényező | az egész rendszer mozgatója, esetenként a dominancia eszköze | a műveleti és harcászati szint vezeti a rendszert (Pull elv működik) |

Amennyiben a két ellátási lánc értelmezés meghatározó jegyeiket nézzük, további fontos következtetésre juthatunk.

Van néhány meghatározó pont, amely a lényeges jegyek alapján eldönti hasonlóságukat és különbözőségüket:

- a fogyasztói igény kielégítésének problémája;
- az információ hozzáférésének problémája;
- a lánc rugalmassága és megbízhatósága;
- a lánc irányítása, csomópontjai,
- Push és Pull elv működése.

*A fogyasztói igény tekintetében* a civil logisztika, mondhatnánk egyszerű helyzetben van, hiszen a „megfelelőséget" a megvásárlás ténye dönti el és ez az értékítélet, valamint a vevőkkel készített interjúkból, felmérésekből pontosan orientálhatjuk a gyártást és az ellátási

[4] Szegedi Zoltán - Prezenszki József: Logisztika menedzsment Kossuth Kiadó 2003 160. oldal

lánc szereplőit a fogyasztói elégedettségről.

A katonai logisztika fogyasztói nem választanak, hanem készen kapják a „rendszeresítet" anyagokat és elégedettségüket vagy elégedetlenségüket sem tudják kifejezni a megvásárlás megismétlésével vagy elutasításával.

A felhasználói vélemény visszajelzésére a szolgálati hierarchia útjai és a felmérési rendszer szolgál, ami gyakran nem ad megfelelő támpontot az anyag vagy szolgáltatás megfelelősségére vonatkozóan, mert a rosszul értelmezett „regula", esetleg érdektelenség útját állja.

*Az információ hozzáférhetősége* mindkét rendszerben lehetőség szintjén jelen van, de míg a civileknél a láncot uraló domináns cég monopolizálhat információkat, addig a tapasztalatok szerint a műveleti szintű logisztikában inkább az információk – főleg negatív – kozmetikázásáról lehet beszélni.

*A lánc rugalmassága és megbízhatósága* tekintetében a megvásárlás ténye, illetve katonai vonatkozásban a fogyás és veszteség mennyiségének, idejének és helyének a bizonyossága vagy bizonytalansága a meghatározó. A civil ellátási láncban a vásárlói bizonytalanság oda vezethet, hogy a lánc szereplői tartalékolnak, növelik készleteiket és ezzel jelentős többlet költséget szenvednek el, esetenként többszörösére növelik a láncban lévő anyagok mennyiségét. („ostorcsapás effektus").

A katonai ellátási láncnak a művelet, a katonai működés természetéből adódik a bizonytalanság, ami a várható fogyás és veszteség mennyiségének, minőségének pontos helyének és keletkezése idejének tervezhetetlenségéből ered (legfeljebb prognosztizálható). Ez olyan kényszert eredményez, hogy elsősorban harcászati tagozatban nem lehet lemondani a szintenként képzett anyagi tartalékokról. A bizonytalanságot, összevetve a civil ellátás bizonytalansági tényezőjével, nyugodtan nevezhetjük „lórúgás" effektusnak.

A lánc irányítása, és csomóponti helyei vonatkozásában fontos eltérés, hogy amíg a civil rendszer egy természetes közös érdekek szintjén született együttműködésen alapszik, illetve ahol egyes dominanciát szerzett szereplők válnak a lánc működtetőivé, addig a katonai logisztika a katonai hierarchiának megfelelően épül fel műveleti szinten, és csak a termelői logisztika elemeit építi fel a gazdasági életben megszokott módon.

Ez a különbség azt is jelenti, hogy a hadműveleti-, hadszíntéri igények határozzák meg az ellátási lánc működését és a „felhasználói igények" birtokában szabályozzák a teljes lánc működését. A többnemzeti csapatcsoportosítások esetében ez természetesen hozza magával a NATO parancsnok hatáskörének kiszélesedését a nemzeti logisztikai támogatás szabályozásának és koordinációjának vonatkozásában.

## A RÉGI MÓDSZER ÚJ ARCA

Az ellátási lánc a katonai logisztikában tehát egyáltalán nem új jelenség. A háborús tevékenység és elsősorban a támadó műveletek mindig feltételezték, hogy hosszabb, rövidebb távolságon összekapcsolják a többnyire honi területen lévő ellátó bázist a frontvonallal. Ez az összekapcsolás soha nem volt közvetlen, mindig ellátási tagozatokon és szinteken keresztül valósult meg.

Ennek oka magában a műveletek sajátosságaiban, a harc dinamizmusában, a váratlanság állandó jelenlétében, a nagy műveleti mélységben és a hátország bizonytalanságában keresendő. Az ellátás biztonsága azt igényelte, hogy szintenként és tagozatonként megfelelő tartalékok álljanak rendelkezésre a folyamatos ellátás és az adott csoportosítás cselekvési autonómiájának biztosítása érdekében.

Az anyagok osztályozását a katonai logisztika az ellátási láncban betöltött szerepe, helyesebben áramlási tulajdonságai szerint határozta meg. Ennek megfelelően a magyar

osztályozás **harcanyagokról, fenntartási anyagokról és ellátási anyagokról** szól. Ezen belül nagyon jól érzékelhetők a termékpályák és ezek áramlási sajátosságai.

Távolabbi történelmi kitekintést nem igényel annak belátása, hogy az ellátást úgy kell megszervezni, hogy az megfeleljen a kombatáns állomány igényének, a különböző helyen beszerezhető eszközök időben eljussanak a felhasználókhoz és tartalék készleteivel képes legyen áthidalni a felhasználás kialakuló csúcsait.

Miben jelent mégis újat az idézett NATO koncepció? A kérdés feltevésére egy ok szolgál alapul. Ez nem más, mint a NATO legsajátosabb katonai megjelenési formája, nevezetesen a többnemzeti működés és az ezzel járó vezetési mechanizmus.

A többnemzeti működés kapcsán a logisztika nagyon sok, a különbözőségekből eredő problémával találkozik, különösen napjainkban, amikor a többnemzeti csoportosítások harcászati szinten is jelentkeznek. Ennek nem csak a fegyverrendszerek és eszközök eltérő volta az oka, hanem hozzájárul ezek eltérő logisztikai támogatási igényei és a kapcsolódó megvalósítási metodika különbözősége is.

Az ellátási lánc műveleti szinten esélyt ad az integráció kiszélesítésére és a nemzeti támogatás koordinálására és ezeken keresztül a vezetés nagyobb centralizálására a NATO parancsnok kezében. Ez várhatóan a logisztikai erők hatékonyabb alkalmazását, a nemzeti támogatás optimalizálását is jelenti.

Teljesen egyetértek a koncepció kiváltó okát illetően Baranyai Virgillel, aki 2006-ban TDK dolgozatában kifejtette:" A jelenlegi és az előző NATO műveleteket független és gyakran koordinálatlan nemzeti logisztikai rendszerben látták el, amelyek előtérbe helyezték a balkáni, az 1. öbölháború, az afganisztáni és a jelenlegi iraki műveletek tapasztalatait, és amelyek jelentős pénzügyi, felszerelési és emberi erőforrások nem hatékony felhasználását eredményezték. Hiány volt az előzetes átgondolásból a szállítási központok használatának a területén, sőt a felhasználók és műveleti parancsnokok korlátozták, és nem tették láthatóvá az ellátási erőforrások elérhetőségét. Ez elvesztegetett lehetőségeket vagy felesleges utánpótlási ellátásokat eredményezett. Az ellátási igények gyakran előre kalkuláltak voltak és pontatlan megállapításokon alapultak kevés korrigálási lehetőséggel, hogy azok megfeleljenek a folyamatban lévő valóságos helyzetnek. Mindezt összevetve az élőerő mozgatási rendszere, a felszerelés és az ellátás darabos és lassú volt a hatékony irányítás hiányában."

## A NATO HADMŰVELET TÁMOGATÁSI LÁNC FŐBB RENDEZŐ ELVEI

A NATO hadműveleti támogatási láncnak, mint a kiterjedést szemléltető ábrából kitűnik irányítania kell az ellátási források igénybevételét, a ki- és behajózási kikötőben (POD, POE) való érkezéstől egészen a frontvonali felhasználókig.

A rendszer komplexitást és átláthatóságot igényel és a lánccal szembeni alapelveket fogalmaz meg, amelyek a teljesség igénye nélkül az alábbiakra terjednek ki:

- a műveleti támogatási láncon belüli információknak láthatónak kell lenniük a műveletekben résztvevők számára,
- a műveleti támogatási lánc komplex és rugalmas,
- a műveleti támogatási láncot a műveleti és taktikai felhasználók követelményei vezetik,
- a műveleti támogatási lánc átfog minden biztosítási területet, beleértve a műszaki, egészségügyi és a civil szolgáltatói ellátást is,
- a műveleti támogatási lánc nem irányít és ír elő nemzeti rendszereket vagy folyamatokat,
- a műveleti támogatási lánc elég rugalmas, hogy összeegyeztesse a „tőlem" és „hozzám" módszert,
- a műveleti területen jelen lehet nem kifizetődő logisztikai tevékenység is,

- többnemzetiségű logisztikai struktúrákat és eljárásokat ott alkalmaznak, ahol annak előnye előre látható, illetve megfelelő feltételei vannak,
- minden résztvevő nemzet a műveleti támogatási láncba veti a bizalmát és hajlandó megbízni a Szövetségesek által működtetett ellátási láncban.

Az alapelvek közül, némileg önkényesen, a téma szempontjából fontosnak tartva kiemelem a *láthatóságot*, valamint azt a körülményt, hogy a műveleti támogatási láncot a *műveleti és taktikai felhasználó követelményei vezetik*. Ha együtt értelmezzük a két tényezőt, arra a következtetésre juthatunk, hogy a koncepció a lánc működtetésén keresztül a többnemzeti ellátási csatorna további integrációját is kimondatlanul magában rejti.

Összevetve ezt a civil ellátási láncokkal, érzékelhető hasonlóság látható a lánc vezetésében, amikor egy, a legtöbb információval bíró tag válik a lánc mozgatójává, irányítójává. Ez azzal összefüggésben figyelemre méltó, hogy lehetnek a láncnak erősebb tagjai is, mégis ahhoz kerül a domináns szerep, aki a legfontosabb információk birtokában van. Ezek az információk pedig a vásárlók elégedettségéről és szokásairól szóló információk. A mi esetünkben ezek az információk vitathatatlanul a hadszíntéren vannak, ezért tökéletesen egyet lehet érteni a NATO elképzeléssel a „pull" elv alkalmazásában a lánc működtetését illetően.

A honvédelmi célú tartalékok rendeltetése az, hogy a honvédelemben résztvevő erők működésének azonnali megkezdéséhez lehetőséget teremtsenek és biztosítsák a tevékenység folytatását mindaddig, amíg a hazai gyártás vagy külföldi beszerzés nem kapcsolható be az ellátás folyamatába.

Ebből a szempontból vizsgálva a Magyar Honvédség anyagainak osztályozását (harcanyagok, fenntartási anyagok, ellátási anyagok) azt láthatjuk, hogy nagyon kevés támpontot ad arra vonatkozóan, hogy az ellátási láncban milyen mozgási tulajdonságok kapcsolhatók egyes anyagcsoportokhoz. Valamivel több segítséget jelent a NATO öt + 1 anyagosztálya, illetve a tíz osztályos rendszer, mert ezek válaszolnak olyan kérdésekre, hogy vajon a szövetséges ellátási rendszerben mely anyagcsoportoknál támaszkodhatunk a Befogadó Nemzeti Támogatásra, illetve más Szövetséges ország támogatására.

Ugyanakkor az is látható, hogy több jelentős, sőt döntő anyagellátási terület csak a Nemzeti Támogatás rendszerében oldható meg.

Így vizsgálva készleteinket szembetűnő, hogy azok nem „egyenszilárdak".

Ez alatt azt értem, hogy a NATO ajánlás 30 napos készletei nem egységes metodika szerint kialakított közepes hazai napot takarnak. Mivel a NATO az üzemanyagra vonatkozóan pontos metodikát ad, célszerű lenne, „öntevékenyen" a többi anyagra is elkészíteni egy az alkalmazás intenzitásában ehhez konvergáló rendszert. Ebben a kérdésben teljesen egyetértek Szabó Árpád alezredes 2002-ben készült tanulmányában leírtakkal.

A másik kritikus kérdés a Magyar Honvédség technikai modernizációjával kapcsolatban vetődik fel. Amennyiben logisztikai vonatkozásban egyenszilárd rendszert szeretnénk kiépíteni, úgy kéne eljárnunk, hogy az új beszerzésekhez is annyi tartalék alkatrészt, illetve lőszert, stb. szereznénk be (harci napban számvetve) amennyi a rendszerben lévő régi eszközeink után van (remélem, van). Ez azonban azért lenne célszerűtlen, mert az új eszközök fenntartási rendszere és az MH csapatainak fenntartási (javítási) lehetősége gyökeresen megváltozott. Nincs is szükség arra, hogy a régi értelemben vett kis-, közép- és nagyjavítási lehetőséggel rendelkezzen a hadsereg. Arra azonban szükség lenne, hogy az új technikai eszközeinket a missziókban zavartalanul fenntarthassuk, szervizelésük, javításuk biztosított legyen, illetve a hadszíntéren a NATO parancsnok igénye szerinti készletek (pl. lőszer és fenntartási anyag) rendelkezésre álljanak.

Ennek biztosításához az eszközöket két gondolati csoportba kell sorolni. Egyrészt azokra, amelyek stacioner eszközök és kizárt az ország határain kívüli alkalmazásuk, másrészt

azokra, amelyek missziós, de inkább fogalmazzunk úgy, hogy a Szövetség határain túli alkalmazása lehetséges.

A készletek megalakítását és az ellátási lánc működtetését ennek figyelembevételével kell kialakítani.

A beszállítókkal olyan szerződéseket kell kötni, ami biztosítja a hazai szervízhálózat (lehetőleg HM RT-ben) létrehozását, a folyamatos időbeni pótlást és a hadszíntéri követelmények kielégítését is.

Befejező gondolatként ismét Szabó Árpád „A NATO készletképzés tervezési folyamata és annak hatása a MH készletképzés tervezési gyakorlatára" című 2002-ben készült tanulmányához nyúlok vissza, ahol a befejező részben így ír.

„Azoknak az információknak az ismerete nélkül, melyekkel egy adott katonai szervezet alkalmazása egyértelműen meghatározó, nem lehet kiszámítani a szükséges anyagi készletek nagyságát. Ezért az alkalmazóknak a feladatrendszer elemzését követően meg kell adniuk a (had)művelet típusára (V. cikkely szerinti, vagy válságreagáló), a harci tényezőkre (támadás, védelem, visszavonulás, halogatás), a külső körülményekre (hazai, külföldi, szélsőséges időjárási körülmények közötti, nehéz vagy könnyű terep), a kontingens kereteire (nemzeti, többnemzetű, szövetségen belüli vagy azon kívüli), volumenére (az adott kötelék nagysága, várható időtartama), stb. vonatkozó paramétereket. Ezen jellemző értékek birtokában, valamint a meglévő készletek, a raktározási, szállítási és anyagmozgatási kapacitásadatok felhasználásával kell a szükségleteket lefedő készletszinteket megállapítani. Ezért szakítani kell az eddigi gyakorlattal – ahol a mindenkori legfelsőbb logisztikai vezető saját maga határozta meg a készletképzési elveket – és az alkalmazók bevonásával kell kidolgozni az MH, illetve a szóban forgó, felajánlott szervezet készleteinek nagyságrendjét.

A következő, a hatékonyság problematikája. Ez alatt azt kell érteni, hogy nem járható az az út, ahol csupán a meglévő készletek mennyiségéből származtatják a készletképzésre vonatkozó adatokat. Egy rendkívül leegyszerűsített példával ez nem jelent mást, mint amikor egy 1000 hagyományos fegyverrel rendelkező katonai formációnak csak 2000 lőszert biztosítanak, mert annyi van raktáron. Így minden egyes fegyverre kettő lőszer út, amivel az ellenséges cél megsemmisítési valószínűsége meglehetősen alacsony. A találati arányt kétféleképpen növelhetjük:

a.) csökkenthetjük a fegyverek számát;

b.) vagy emelhetjük a készletek mennyiségét.

Ha az MH egészére vetítjük ki a megoldási változatokat, azok nyilván mindkét esetben politikai döntések meghozatalát generálják. Azonban az semmiképpen sem elfogadható, hogy egy szimpla osztási művelettel feldaraboljuk a meglévő anyagmennyiséget és azt elosztjuk a katonai szervezetek között. Ezért a második fejezetben tárgyal ACROSS szoftver filozófiájához hasonlóan meg kell találni azt az optimális lőszerösszetételt, ami adott költségszint mellett, az ellenséges célok megsemmisítéséhez minimálisan szükséges és az megegyezik a politikai vezetés elképzelésével is. …" „A készletképzés tervezése során nem szabad figyelmen kívül hagyni Magyarország NATO tagságának tényét. Ez a tény viszont azt jelenti, hogy a többi tagállammal hazánk politikai szolidaritást vállal, azokkal szorosan együttműködik, osztozik velük a felelősségekben és kötelezettségekben a közös, illetve egyéni érdekeink elérése érdekében. Következésképpen mindenkor szem előtt kell tartani a Szövetség által megfogalmazott követelményeket, a jóváhagyott terveket és a kitűzött célokat. Ezért ma már nem tömeghadseregekben, nehéz tüzérségben és autark megoldásokban kell gondolkodni, hanem gyorsan bevethető, mozgékony, multinacionális közegben működő és többnemzetű ellátásra épülő katonai szervezetek kialakítására, valamint ezek ellátására és készletszintjük kidolgozására kell összpontosítani."

Összességében úgy látom, hogy függetlenül attól, hogy az ellátási lánc civil, katonai vagy a kettő ötvözete csak előre tervezett egységes műveleti követelmény szerint szervezett ellátás lehet „megfelelő” a csapatoknak és a Szövetséges vezetésnek egyaránt.

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Vigh Attila**
HM Fejlesztési és Logisztikai Ügynökség

# A HONVÉDELMI MINISZTÉRIUM FEJLESZTÉSI ÉS LOGISZTIKAI ÜGYNÖKSÉG ANYAGI-TECHNIKAI ÉS KÖZLEKEDÉSI IGAZGATÓSÁG KÖZLEKEDÉSI OSZTÁLY HELYE, SZEREPE A MISSZIÓS LOGISZTIKAI TÁMOGATÁS RENDSZERÉBEN

***Absztrakt***

*A Honvédelmi Minisztérium Fejlesztési és Logisztikai Ügynökség Anyagi-technikai és Közlekedési Igazgatóság (továbbiakban HM FLÜ ATKI) Közlekedési osztálya feladatrendszerének missziós vetülete csak tágabb kontextusban érthető meg, szükséges mindenekelőtt röviden megvilágítani a HM FLÜ egészének tevékenységét a Magyar Honvédség nemzetközi szerepvállalásának támogatása során.*

***Kulcsszavak:*** *logisztika, HM FLÜ ATKI, Magyar Honvédség*

Ismeretes, hogy a logisztikai rendszer legutóbbi átalakításának vezérlő elve a termelői és fogyasztói logisztikai feladatok szétválasztása volt. A termelői logisztikai feladatokat a HM FLÜ végzi, emellett a honvédelmi miniszter közvetlen alárendeltségében irányítja a tárca felsőszintű logisztikai gazdálkodásának egészét, ide nem értve az egészségügyi és az infrastrukturális gazdálkodást. Az MH Összhaderőnemi Parancsnokság (MH ÖHP) felelősségi körébe tartozik a fogyasztói logisztikai feladatok végrehajtása, hiszen alárendeltségébe tartozik a csapatok mellett a központi ellátó szervek (MH LEK, MH VEK, MH KKK, MH TD, MH HEK) többsége is. Ez az alapvető megosztottság meghatároz egy sor hatásköri kérdést, ugyanakkor számosat hagyott megválaszolatlanul.

Tudom jól, hogy minden hasonlat sántít, de olyan a helyzet alakult ki, mint pl. amikor az apuka (jelen esetben a HM FLÜ) biciklit vesz a fiának. A beszerzés minden terhéért „cserébe" joga van szabályokat alkotni, úgymint: „Nem mehetsz a göröngyös útra, tartsd be a KRESZ-t, stb." Az esetleges garanciális ügyintézést és a nagyobb javításokat, felújítást vállalja, de napi ellenőrzést, karbantartást, pumpálást, izzócserét nem. Azt mondja; „kölcsönadhatod a barátaidnak is (ez az átcsoportosítás analógiája), de vigyázz rá, mert egyhamar nem kapsz másikat."

Ennél valamivel bővebben a HM FLÜ főbb feladatai:

- A logisztikai gazdálkodás irányítása, tervezése, irányelvek kidolgozása;
- Teljes élettartam szemléletű hadfelszerelési rendszer működtetése;
- Beszerzések tervezése, lebonyolítása;
- Technológiai és innovációs feladatok (K+F) végrehajtása;

•Nemzetközi támogatási és rendezvényszervezési feladatok végrehajtása;

Lényeges, hogy a HM FLÜ struktúrája tudatosan és tervszerűen **eszköz-független** (másképpen szakág-független) **tevékenységek** mentén lett kialakítva. A missziós támogatás azonban nem tartozott a rendező elvek közé, ezért ez a feladat a szervezeten belül megoszlik: Az Anyagi-technikai és Közlekedési Igazgatóság (ATKI) vállát nyomja a hadfelszerelési rendszer működtetése, a beszerzések indítása, felügyelete, szakmai kidolgozói munka stb. A Technológiai Igazgatóság feladata a K+F tevékenység, az innováció, a minőségbiztosítás. A Beszerzési Igazgatóság végrehajtja a „megrendelt" beszerzéseket, a Gazdasági Igazgatóság főként a költségvetés területén ígér és igényel, számol és elszámoltat. A Nemzetközi Szolgáltatási Igazgatóság feladata a határnyitás és a vámokmányok, NATO menetparancsok kiadása.

Az ATKI szervezeti egységében, illeszkedve annak általános feladataihoz, a Közlekedési Osztály az alábbi tevékenységeket végzi:

A szállítással, anyagmozgatással, rakodásgépesítéssel, csomagolással, egységrakomány-képzéssel, konténerizációval összefüggő **tervezés és fejlesztés** irányítása, a beszerzési kritériumok, üzemeltetési **követelmények**, alkalmazási **irányelvek meghatározása** és a beszerzések kezdeményezése, nyomonkövetése.

Beszerzéssel, illetve a K+F tevékenységgel költséghatékonyan nem beszerezhető **kapacitások** (pl. stratégiai tengeri és légi szállítás, speciális vasúti eszközök) két- vagy többoldalú (polgári vagy katonai) szerződésekkel, egyezményekkel történő **biztosítása**.

Anyagi és adminisztratív „Egységes NATO Előírások" (STANAG) követelményeinek érvényesítése a beszerzések és K+F során, aktív részvétel a szövetséges szabványosítási tevékenységben, valamint a hazai bevezetés biztosítása és a kapcsolódó feltételek megteremtése.

A szakmai irányítói, követelménytámasztói feladatok mellett kiemelést érdemel, hogy meg kell teremtenünk a megfelelő feltételeket, lehetőségeket, kapacitásokat a feladatok optimális végrehajtásához.

A legegyszerűbb az lenne, ha a jogos igényeknek megfelelően mindig beszereznénk mindent, ami kell, a targoncától a szállítóeszközökig. Mivel ez nem járható út (legalábbis az „Óperenciás-tenger" innenső felén), ezért a később részletezett nemzetközi együttműködések, egyezmények, szerződések kiszélesítésén törjük a fejünket. A hazánkhoz hasonló helyzetben lévő, kisebb országoknak ugyanis elemi érdeke az összefogás és a más országok által jutányos áron kínált kihasználatlan részkapacitások felhasználása. Egy valamit azonban nem szabad elfelejteni; bármennyire is támaszkodhatunk más országokra, a nemzeti felajánlásokban szereplő erők hadszíntérre történő kijuttatása **nemzeti felelősség**.

A missziókban részt vevő katonai szervezetek közlekedési támogatási feladatrendszerében **kiemelt helyet foglal el** az alkalmazási területre történő **kitelepülés, a visszatelepülés** valamint a személyi állomány **váltása, pihentetése, és az utánszállítások** megszervezése, illetve ezek végrehajtásához a szállítóeszközök biztosítása. A megalakítás, felkészítés közlekedési feladatai (az elhelyezési körlet és a központi raktárak, illetve a kiképzőbázisok között) manapság már veszítettek jelentőségükből, hiszen követelmény a békében meglévő, kiképzett, a szükséges hadfelszereléssel rendelkező szervezetek alkalmazása. Alkalmanként sor kerül áttelepítésre, szemlék, ellenőrzések végrehajtására és sajnos sérültek, betegek szállítására is.

A különféle anyagmozgató, egységrakományképző és rakományrögzítő eszközökkel kapcsolatosan számos ellátási, üzemeltetési feladatot is végre kell hajtani. A szakanyagok

biztosítása történhet raktárkészletről (központi vagy csapat), átcsoportosítással, vagy (köz)beszerzéssel (ideértve a helyszíni bérlést is). A szolgáltatások és eszközök helyszíni beszerzése részletes jogi, és szakmai szabályzást igényel, mert sürgető igény van rá. Előnye, hogy gyors, olcsó, nem igényel szállítást, a helyszíni alkalmazhatóság garantált. A pénzügyi, számviteli nyilvántartási (bevételezési), rendszeresítési problémák megoldhatóak.

A biztosítási, és technikai karbantartási tennivalók jellegüknél fogva hasonlítanak más szakágak feladatrendszeréhez, ezért e helyen nem kerülnek részletezésre. Emlékeztetek azonban arra, hogy gyakran igen szigorú hatósági előírásoknak kell megfelelni (pl. az emelőgépekre vonatkozóan). Ezen feladatok mellett, azokkal összefüggésben szakkiképzési feladatok (pl. rakodási gyakorlat, gépkezelői kiképzés) és közlekedési infrastrukturális feladatok is jelentkeznek.

Az imént felvázolt közlekedési feladatrendszer java részét természetesen az MH ÖHP hajtja végre. A tervezési és előkészítési folyamatokból azonban a HM FLÜ is jócskán kiveszi a részét.

A **tervezést** elsősorban a hadműveleti követelmények, a rendelkezésre álló szállító-, rakodó- és raktári kapacitás, a közlekedési infrastruktúra és végül, de nem utolsósorban a finanszírozási lehetőségek határozzák meg. Számos kisebb (nem elöljárói szintű, hanem „csak” munkatársi) konfliktus származik abból, hogy a védelmi tervezők joggal szeretnének 10 évre előre pontosan kalkulálni mindent, számítási normákat követelnek, inflációs rátával szorozgatnak, és bizony a közlekedéseik pedig általában válasz helyett folyton csak visszakérdezgetnek, végül gyanúsan kerek számot adnak meg hangsúlyozva, hogy pusztán becslésről van szó. A közlekedési támogatási igény ugyanis függvénye a többi szolgálati ág feladatainak, az aktualizált műveleti tervnek, parancsnoki döntéseknek, stb.

Előbb tudnunk kell ugyanis, hogy mi a pontos feladat, mi a rakomány, csak utána tudunk „dolgozni”. Nem csak a szállításszervezés nehéz konkrétumok nélkül, hanem az egységrakományképzés, és rakományrögzítés miatt a közlekedési szakanyagigényre is hatással van a „többiek” kiszállítandó anyagfélesége és anyagmennyisége. A többszörös visszacsatolás, a sokszoros „iterációs” tervezés rokonszenvessé teszi a modern tudományos világképnek azt a vonását, miszerint lehetetlen mindent kiszámolni, törvényszerűen létezik végső bizonytalanság.

## A missziós műveletek során várható szállítási igények

A korábban domináns vasúti szállítás mellett ma már a missziókban részt vevő katonai szervezetek kitelepülése és visszatelepülése végrehajtásakor a személyi állomány mozgatása általában légi úton, a hadfelszerelés mozgatása vasúti és tengeri szállítással történik.

A NATO stratégiai szállítási elveit követve a személyi állomány és a hadfelszerelés szállítása leggyakrabban több ütemben és több szállítási ágazat bevonásával történik, az alábbiak szerint:

- Vasúti szállítás végrehajtása a berakó tengeri kikötőbe, a hadfelszerelés berakása. Természetesen a berakó személyi állományt is el kell szállítani a berakó kikötőbe.
- A személyi állomány a berakó repülőtérről légi úton közvetlenül a Fogadó Nemzet területén (az alkalmazási területen) a bázis körletben elhelyezkedő kirakó repülőtérre kerül átcsoportosításra.
- A tengeri szállítási folyamat végén a kirakó kikötőben következik a hadfelszerelés kirakása. A kirakás után a hadfelszerelés közúti menettel jut el a bázis körletben kijelölt gyülekezési körletbe a kiképzés és az összekovácsolás végrehajtására.

- A gyülekezési körletben végrehajtott rövid idejű kiképzés, összekovácsolás, akklimatizálódás után következik az előrevonás műveleti területre általában közúti menettel. (Előfordulhat azonban, hogy fogadó nemzet nem lévén a kitelepülés közvetlenül az alkalmazási területre történik.)

A konkrét megvalósításnak természetesen számos katonai, földrajzi, politikai, gazdasági, stb., korlátja lehet, vagyis a rutin mellett felelősségteljes döntésekre és optimalizálásra is szükség van.

**A nagytávolságú szállításra rendelkezésre álló lehetőségek**

*Nemzeti katonai szállító kapacitás*
Szállító hajónk nincs, a meglévő 5 db AN-26 repülőgép kapacitása rendkívül intenzíven van kihasználva. Ez az eszköz elsősorban harcászati (kistávolságú) szállításokra alkalmas, nagyobb távolságra minimális teherrel is csak több fel és leszállással repül el.
*A kereskedelmi szabadpiacon* az árak tervezhetetlenül hektikusak, emellett a műveleti területre való eljutás is bizonytalan, diplomáciai és biztonsági okokból. Gondot okoz ugyanis, hogy sok polgári légitársaság nem repül közvetlenül a kockázatos alkalmazási területre, illetve a megkövetelt leszállító berendezések hiánya esetén nem vállalják a szállítást (pl. Bagdad, Kabul).
*Más nemzet kihasználatlan katonai kapacitásának igénybevétele* - bármilyen egyezmény legyen is a háttérben - szintén bizonytalan, nem garantált. Ha szakítani akarunk azzal a szomorú képpel, hogy „a légifolyosók mellett integető stopposok" vagyunk, akkor komolyan meg kell fontolni saját katonai szállítórepülőgép beszerzését, ennek vizsgálata egyébként szerepel is a védelmi tervezési irányelvekben (10/2006-os HM ut.). (A kisebb szállítórepülőgépek nagyon praktikusak, számos „kis" ország vásárolt már, emellett pl. a gyártás előtt álló Airbus A-400M-ből összesen 180 db van lekötve.)

A ki- és hazatelepülés, a technikai eszközök cseréje és a nagyobb segélyek esetében, tehát a *nagytömegű* szállításokra a többnemzeti megoldások optimálisak (pl. SALIS, MIA, C-17). Többnemzeti szerződésekhez történő csatlakozás lehetőséget ad az eszközök *garantált* biztosítására. Ha valamely ország nem csatlakozik az ilyen megoldásokhoz, lehet, hogy adott esetben (pl. válsághelyzetben) nem tud hozzájutni ilyen kapacitáshoz a szabadpiacon, bármennyit is fizetne érte.

A *többnemzeti megoldások* „menedzselése", bővítése elsősorban a HM FLÜ feladata. Az alábbi rövid ismertetés rávilágít a főbb együttműködések hátterére és az elérhető előnyökre.

A 17 tagállam által létrehozott Stratégiai Légi Szállítási Átmeneti Megoldás (Strategic Airlift Interim Solution - SALIS) által korlátozott mértékben, de előre rögzített áron, többek között hazánk részére is elérhetővé vált elsősorban a túlméretes technikai eszközök szállítására egy garantáltan rendelkezésre álló polgári légi szállítókapacitás. A lipcsei bázisrepülőtéren 72 órás készenlétben áll 2 db valamint további 4 db (6, illetve 9 napos készenlétű) AN-124-es típusú óriás szállító-repülőgép, NATO, EU, vagy nemzeti célokra. A jelenlegi szerződés 2008 végéig van érvényben, ezt követően évente meg lehet újítani 2012-ig. A szerződés jövője egyrészt bizonytalan a szállítórepülőgép-beszerzési programok miatt, másrészt stabilnak ígérkezik, mert a beszerzésre kerülő gépek egyike sem vetélytársa az AN-124-nek méretben, teherbírásban, hatótávolságban.

Az *Európai Mozgáskoordináló Központ* (MCCE) egy több szállítási módot (légi, vízi és szárazföldi) tömörítő koordináló központ, amely az egyes tagországok hadseregeiben meglévő vagy az adott ország által a polgári piacról lebiztosított szállító kapacitásokat ajánlja ki a többi tagországnak hasznosításra.Az MCCE tagságunkból adódóan eleinte a **tengeri** szállítások terén érhetőek el szállítási költségcsökkentések, de a későbbiek folyamán az együttműködésben való részvételünk alapja lehet a **légiszállítások** vonatkozásában is a megtakarítások elérésének, valamint a **szárazföldi** szállításoknál is különböző előnyök realizálhatóak pl. több nemzet azonos irányban közlekedő kisebb **vasúti** szállítmányainak összekapcsolásával a gyorsabb eljutási idő elérése. Fontos lehet továbbá az MCCE-ben résztvevő néhány tagállam **légiutántöltő** kapacitásának felhasználása is a magyar Gripen pilóták kiképzése és a gépek esetleges külföldi bevetése érdekében. A HM FLÜ 2008-ban 1 fő őrnagyot biztosít az MCCE-be, ezzel is szorosabbá fűzve a kapcsolatokat.

Míg az MCCE a meglévő stratégiai szállítókapacitások koordinálásán, azok jobb kihasználásán dolgozik, addig a *Többnemzeti Tengeri Szállítást Irányító Bizottság* (MSSC) a garantáltan rendelkezésre álló tengeri szállítókapacitások növelésén munkálkodik a résztvevő országok által biztosított Tengeri Szállítási Képességcsomag (SCP) bővítése útján. (Kissé magyarosan kisarkítva: az MSSC a termelői logisztika, az MCCE pedig a inkább a fogyasztói logisztika része.) Az MSSC soros elnöki teendőit 2008-ban Magyarország képviseletében a HM FLÜ ATKI közlekedési osztályvezetője, Szarvas László mk. ezredes látja el. Feladatunknak érezzük a szervezet jelentős bővítését, ugyanakkor látni kell, hogy új tagországok csatlakozása nemcsak a bevételeket növeli, hanem a szállítótérigényt is, ezzel alkalmanként felborítva a kényes egyensúlyt.

Mielőtt az a vád érne, hogy mindenhez csatlakozunk, megemlítem, hogy létezik egy görög vezetésű Athéni Többnemzeti Tengeri Szállítást Koordináló Központ (Athens Multinational Sealift Coordination Centre - AMSCC) is, amely nem a garantált rendelkezésre állásra, hanem a velük kapcsolatban álló nagyszámú görög hajóra alapozva fejt ki propagandát. A garantált rendelkezésre állást firtató kérdésekre a görög hajómágnások morális elkötelezettséget szokták emlegetni, ami a NATO berkeiben nem elegendő. A szolgáltatást ugyan ingyenesen biztosítja az AMSCC, viszont a görög közbeszerzési eljárás alapján bérelt hajó valamennyi költsége teljes egészében a bérlőt terheli. Bár ez a szervezet is bővül és korszerűsödik, összességében a garancia hiánya, a tenderkiírások szükségessége, és a korábbi kedvezőtlen tapasztalatok miatt nem javasoljuk Magyarország csatlakozását.

Svédország, Finnország valamint 14 NATO tagállam tárgyalásokat folytat 3 db C-17 típusú katonai szállító repülőgép közös beszerzése tárgyában, a Stratégiai Légiszállítási Képesség (Strategic Airlift Capability-SAC) program keretében. Magyarország előbb gépek állomásoztatását és nyilvántartásba vételét vállalta, majd a beszerzést és ellátást végző szervezet hazánkba költöztetését is. Az események kedvező előrehaladása a HM FLÜ ATKI közlekedési osztályvezető aktív szerepvállalásának is köszönhető. A program megvalósulása kibővíti a missziós szállítási lehetőségeinket és megteremti a feltételeit - egyelőre beláthatatlanul - az MH Pápa Bázisrepülőtér további fejlesztésének is.

A nagytávolságú légiszállítások terén összegzésképpen megállapítható, hogy a SALIS, a SAC C-17, az A-400M és a nemzeti programok megvalósulása után a jelenlegi szorító kapacitáshiány szövetségi szinten nagymértékben csökkenni fog. A tengeri szállítások terén azonban borúlátásra ad okot, hogy csökken a katonai felhasználásra leginkább alkalmas RO-RO hajók száma és kapacitása, valamint a meglévő hajók hosszútávú szerződésekkel vannak, illetve lesznek lekötve, így azok alkalmankénti, kampányszerű felhasználására egyre kevésbé nyílik mód.

Befejezésül ismertetem a HM FLÜ közlekedési vonatkozású technikai *fejlesztési programjait:*

**Az MH anyagmozgatási rendszerének korszerűsítése**
Célja a mozgatások, rakodások területén az élő munkaerő kiváltása, az anyagok és eszközök gépesített mozgatáshoz történő előkészítése, valamint szakszerű mozgatása. A legfontosabb eleme az MH egységes rakodási rendszerébe illeszkedő korszerű és megbízható anyagmozgató gépek beszerzése.

**Reptéri anyagmozgatás korszerűsítése**
Katonai és polgári szállító repülőgépek ki- és berakásának az előírások szerinti gyors és biztonságos végrehajtása. A szállításra tervezett anyagok készletezése légi szállításhoz történő előkészítése, a kirakott rakományok megbontása és a szállítási irányok szerinti készletezése. A repülőtéren kijelölt raktárakból az anyagok mozgatása, szállítása.

**MH egységes felépítmény program**
A stratégiai légi és tengeri szállításokra optimalizált, a NATO anyagmozgatási rendszerébe illeszkedő, korszerű mobil szakági felépítmények beszerzése, a felajánlott erők szakági követelményei szerint. (Kapcsolódó programok: haditechnikai konténerprogram, hadtáp ellátó konténerprogram, térképész szakfelépítmény program, egészségügyi szakfelépítmény program)

Ezek a programok nagyon fontosak lennének a missziós támogatás érdekében is, sajnos már hosszú évek óta nagyon fontosak. Cinikusan úgy lehet összefoglalni a közös jellemzőjét a fejlesztési programoknak, hogy a tényleges megvalósulásuk következetesen a 10 éves tervidőszak távolabbi végére esik.

A széleskörű közlekedési feladatrendszer terén tapasztalt összes tanulságot és következtetést nehéz összefoglalni. A logisztikát akár kettéosztjuk, akár nem, a közlekedési szolgálat csak akkor képes megfelelni az új kor által támasztott követelményeknek, ha a feladatok megfelelő finanszírozása mellett a szakállomány fenntartja a szoros hazai és nemzetközi együttműködést.

## Felhasznált irodalom:


1. AJP- 4.4 Szövetséges Összhaderőnemi Mozgatási és Szállítási Doktrína. A Magyar Honvédség Közlekedési Szolgálatfőnökség, Budapest 2004
2. MC 447. A NATO Reagáló Erők Katonai Koncepciója. A Magyar Honvédség Összhaderőnemi Logisztikai és Támogató Parancsnokság kiadványa. Budapest, 2005.
3. MC 0526 Az NRF Műveletek logisztikai támogatásának irányelvei. A Magyar Honvédség Összhaderőnemi Logisztikai és Támogató Parancsnokság kiadványa. Budapest, 2005.
4. Szarvas László: A Magyar Honvédség Közlekedési Szolgálat feladatrendszerének átalakulása a NATO tagság következében. Záródolgozat, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004.
5. Szarvas László: A Magyar Honvédség nagytávolságú szállítási lehetőségei. Katonai Logisztika. A Magyar Honvédség Logisztikai Folyóirata. Budapest, 2007. 2. szám pp. 9-11.
6. Horváth Attila: Terrorfenyegetettség: célpontok, nagyvárosok közlekedés. Nemzetvédelmi Egyetemi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja. 10. évfolyam 3. (tematikus) szám. Budapest, 2006. pp. 136-152.
7. Horváth Attila: A térszemlélet változása a magyar katonai stratégiában 1920-tól napjainkig. Tér és Társadalom. A Magyar Tudományos Akadémia Regionális Kutatások Központja folyóirata. Győr, XVIII. évfolyam 2004. 1. szám. 127-143. oldalak.

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Csuka Antal**
Zrínyi Miklós Nemzetvédelmi Egyetem
antal.csuka@hotmail.com

**Előházi János**
Zrínyi Miklós Nemzetvédelmi Egyetem
elohazi.janos@gmail.com

# IRÁNYÍTOTT ENERGIÁJÚ FEGYVEREK ÉS VESZÉLYEIK A SZÁMÍTÓGÉPES RENDSZEREKRE

***Absztrakt***

*A cikk célja összefoglalni a létező irányított energiájú fegyvereket azok hatásmechanizmusa szerint. Az ilyen típusú fegyverek komoly fenyegetettséget jelentenek az elektronikai eszközökre, hiszen azok teljes használhatatlanná tételére képesek. Az ilyen, akár otthon is legyártható fegyverek kis méretük miatt észrevétlenek, és a támadó komoly károkat tud okozni velük. Társadalmunk egyre nagyobb mértékben függ az elektronikai eszközöktől, fontos irányítási feladatokkal bízzuk meg őket. Sok területen nélkülözhetetlen alkalmazásuk. Az irányított energiájú fegyverek egy új fenyegetési forrást jelentenek, melyeket a közeljövőben komolyan számba kell venni.*

*The aim of this article is to summarize the existing directed energy weapon technologies based on their affect mechanism. This new type of weapons means serious threats for electronic equipments, since they are able to cause vital damages in such systems. Some types of these weapons can be assembled at home in a very small size, thus the attacker can achieve her goals undetected. Our society considerably depends on electronic devices, very important functions are provided by them. In many areas it is unable to substitute them. Directed energy weapons mean a brand new threat that has to be seriously managed in the near future.*

***Kulcsszavak:*** *irányított energiájú fegyver, elektronikus bomba, HERF – nagy energiájú rádiófrekvenciás fegyver, számítógépes rendszerek ~ directed energy weapons, electronics bomb, HERF – High Energy Radiofrequency Weapons, computer systems*

## BEVEZETÉS

Az irányított energiájú fegyverek sokáig csak a fantázia és a tudományos-fantasztikus történeket szüleményei voltak. A 20. század végi felgyorsult elektronikai fejlődés lehetővé tette, hogy néhány, addig csak elméletben létező irányított energiájú fegyver mégis a valóság része legyen.

Az ilyen fegyverek energiát sugároznak ki magukból egy meghatározott irányban egy célra, hogy azon egy bizonyos hatást fejtsenek ki. Napjaink legelterjedtebb irányított energiájú fegyverei a lézer alkalmazásához köthetőek. Számos híradás szól arról, hogy az Amerikai Egyesült Államokban lézer alapú rakétaelhárító rendszert fejlesztenek, de 2007. július 15-én egy sikeres kísérlet keretében egy vadászrepülőgépet voltak képesek megsemmisíteni nagy energiájú lézersugár alkalmazásával [1].

A felhasználható energia ezekben a fegyverekben számos forrású lehet: lehet elektromágneses alapú, mint a lézer és mikrohullámú fegyverek esetében; lehetnek részecske fegyverek, melyek elektronokat vagy atomokat sugároznak egy adott irányban; és lehetnek akusztikus fegyverek, melyek zavaró, elviselhetetlen hangot sugároznak, és ezáltal hatékonyan alkalmazhatóak tömegoszlatás vagy őrzés védelem megvalósítása során anélkül, hogy maradandó kárt tennének az élő szervezetben.

Az elektronikus eszközöktől napról napra jobban függ a modern társadalom. Alapvető funkciókat látnak el informatikai rendszerek, melyek elengedhetetlenek a politikai-, üzleti- és kormányzati rendszer működtetéséhez. Olyan veszélyes üzemek irányítását bízzuk informatikai eszközökre, mint például az erőművek, a közlekedés irányítása, az üzemek és nem utolsó sorban a haditechnikai rendszerek. A 21. századra viszont az olyan hétköznapi eszközeink, mint a személygépjármű vagy háztartási eszközök sem képesek működni a félvezetők által nyújtotta szolgáltatások nélkül. A mindennapi életben is számos kommunikációs vagy szórakoztató szolgáltatást nyújtó eszközt használunk. Ezek nélkül a modern üzletvitel elképzelhetetlen, és nehézségeket okoz, ha szolgáltatásuk akár csak időlegesen is kiesik. Ez a nagyfokú függőség vezetett olyan fegyverek kifejlesztéséhez, melyek célzottan ezeket a berendezéseket veszik célba anélkül, hogy látványos fizikai rombolást végeznének, vagy közvetlenül az élő erőben tennének kárt. Az ilyen fegyverek elektromágneses energiát használnak arra, hogy a céleszköz által nyújtott funkciókat megtámadják, azt átmenetileg vagy tartósan működésképtelenné tegyék. [5]

## IRÁNYÍTOTT ENERGIÁJÚ FEGYVEREK

Az irányított energiájú fegyverek meghatározására több definíció is született. Az Amerikai Védelmi Minisztérium fogalomtárában olyan rendszerként definiálják, amely az irányított energiát elsősorban az ellenséges eszközök, létesítmények vagy személyek ellen rombolás, roncsolás céljából alkalmazza. [4] De az irányított energiájú fegyvereket definiálhatóak olyan fegyverként is, melyek a kiválasztott irányba energiát bocsátanak ki, hogy a célon különböző hatásokat érjenek el. A kinetikus energiájú eszközöket nem sorolják ide. [1]

A hidegháború alatt kezdődött meg az irányított energiájú fegyverek fejlesztése. A nekik szánt szerep az ellenséges erők irányítási rendszereinek (Command Control and Communications) megbénítása egy nagyarányú nukleáris támadás megindítása előtt. A hidegháborús feszültségek elmúlásával a kifejlesztett technológia a hagyományos hadviselésben is jelentős sikerekkel alkalmazható, és hatékonyan vethető be terrorista, info-terrorista és speciális erők ellen. [5]

Az irányított energiájú fegyverek csoportosítását a kisugárzott energia alapján tehetjük meg, így léteznek akusztikus-, rádiófrekvenciás-, lézer- és részecskefegyverek. A kisugárzott energia egyben meghatározza ezen fegyverek felhasználási területeit is.

## Akusztikus fegyverek

A térben terjedő hang nem egyéb, mint mechanikai hullám, ami valamely folytonos, rugalmas közegben kialakuló mechanikai zavarállapot továbbterjedése. A hangoknak rendkívül nagy jelentőségük van az élővilágban. Kapcsolatot teremtenek az egyedek közt, frekvenciájának függvényében elriasztja, vagy éppen magához csalogatja a másik egyedet.

Az akusztikus fegyverek elsődleges feladata az ellenséges élőerő megbénítása, és megakadályozása céljai elérésében anélkül, hogy életeket áldoznánk fel. Ezt a célt idegi, pszichikai befolyásolással, zaklatással éri el, ezáltal az ellenséges erők harcképessége csökken, szervezett munkavégzésre és tájékozódásra való képessége átmenetileg megszűnik anélkül, hogy fizikai károsodást okoznánk.

Az akusztikus fegyverek legegyszerűbb fajtája az úgynevezett LRAD (Long Range Acoustic Device), melyek kiválóan alkalmazhatóak nagy hatótávolságú kommunikációs célokra, de főként figyelmeztetés közvetítésére. Ez a fegyver nagy energiájú hangot sugároz magából, melynek erőssége elviselhetetlen és fizikai fájdalmat okoz. Emellett visszaverődő és másodlagos forrású kisugárzásai csökkentik a célzott személyek koncentrálási és tájékozódási képességét. [7] Az LRAD rendszerek azon frekvencián fejtik ki hatásukat, melyen az emberi hallás a legérzékenyebb. [9] Számos kutatás kimutatta, hogy az úgynevezett fehérzaj túlterheli a hallórendszert, fájdalmat és szédülést okoz. Egyéb megoldások robbantással előidézett hang-örvénygyűrűket alkalmaznak. Ezen eszközök hatótávolsága több tíz méter, és eredményesen gátolják meg a célt annak cselekvésében. [11]

A hallható hang mellett közismert, hogy az emberi szervezet által nem hallható tartományban sugárzott hanghatások is jelentős mértékben negatív irányban befolyásolják az emberi teljesítőképességet. Az infrahangoknak az elbűvölő, megbabonázó hatása régóta ismert, vízió, azaz látomáskeltő tulajdonságaira nemrégiben derült fény. Ez sok olyan jelenséget megmagyaráz, amit korábban rejtély övezett. Mint újdonság , új lehetőségeket kínál és adott esetben fegyverként is szolgál. A hang hatása (hatalma) ősidők óta ismert, fegyverként is régóta alkalmazzák az élővilágban az élőlények. A kibocsátott hanghullám időegységre vonatkoztatott rezgésszámától függően, megkülönböztetünk infrahangokat, ultrahangokat vagy a hallható tartományba eső rezgéseket, amelyek a térben tovaterjedve, a természet adta érzékszervekkel, felfoghatók, érzékelhetők. A hanghullám információtovábbító szerepe megszokott és jól ismert. Az ember evolúciós fejlődése folyamán a fizikai képességei az előretörő intellektusának a javára elmaradtak, legalábbis megtorpant. Ezt pótolták minden időkben azok a kiegészítő és segédeszközök, amelyek hiányzó képességeit kiegészítették. Ha fegyverről beszélünk, hasonlóképpen ilyen kiegészítő eszközök alkalmazására kell gondolnunk. [22] Az infrahang alkalmazása mellett szól az a döntő érv, hogy az alacsony frekvenciájú hanghullámok terjedését nehéz kedvezőtlenül befolyásolni. Hatására a célszemély mentális képességei nagymértékben csökkenek: megnő reakcióideje, szűkül a látótere, nyugtalanságot és szédülést, fejfájást, émelygést és görcsöket okoz, de előidézhet légzési nehézségeket és szélsőséges esetben epilepsziás rohamot is. A 7Hz körüli infrahang az emberi test saját rezgésével egyezik meg, ezért akár belső sérüléseket is okozhat. Az infrahang alkalmazásának további előnyei, hogy nem hallható, ezért mire a cél észleli annak hatásait, addigra a támadás elérte a célját. Hátránya az infrahangot alkalmazó technológiának, hogy működtetéséhez nagy energia szükséges, és idáig nem sikerült a gyakorlatban is alkalmazható generátorokat kifejleszteni. [11]

Az információátvitelt szolgáló rendszer esetében, alapvető követelmény az, hogy az átviteli közegben terjedő hanghullám vétele és feldolgozása a vevő oldalon zavartalan legyen. Az akusztikus fegyver abban is különbözik az információs rendszerektől, hogy ennek a feltételnek nem kell teljesülnie, mi több az esetek többségében követelmény, hogy a hanghullám a nem hallható tartományba essen, és ott fejtse ki a hatását. Erre szükség lehet stratégiai, taktikai, de olyan okokból is, ami a hanghullám jellemzőire, terjedési

tulajdonságaira és élettani hatására vezethető vissza. Kérdésként merül fel, hogy akkor egyáltalán beszélhetünk vevőről, ha ennek a feltételnek nem kell teljesülnie. [23] Igen, vevőről beszélhetünk, attól függetlenül, hogy a célpont élő, vagy élettelen test. Minden élő és élettelen test rendelkezik úgynevezett hullámabszorbciós képességgel. Ahol a hullám elnyelődik, ott valamilyen hatást is ki fog fejteni. A várható hatás nyilvánvalóan eltérő az élő szervezet és a tárgyak esetében. Míg az élő szervezet esetében az enyhébb kimenetelű zaklatástól az elpusztításáig fokozatai jól elkülöníthetők, addig a tárgyak, jelen estben a számítógépes rendszerek, esetében egyedül a rezonancia jelenségétől várható hatás.

Amennyiben nem élő szervezetet éri a hanghullám, akkor kizárólag olyan fizikai tulajdonságok, jellemzők jöhetnek szóba, a kívánt hatás elérése érdekében, mint az adott test saját rezonanciája. A számítógépes rendszerek ma még viszonylag zárt, kompakt és az akusztikus fegyverekkel szemben jól védett, nehezen sebezhető rendszert alkotnak. Ennek csak extrém nagy kisugárzott teljesítmény esetén lehet realitása. Egyben felmerül, hogy mennyire tekinthető gazdaságosnak egy ilyen megoldás. A válasz egyszerű és nyilvánvaló. A levegő által kitöltött rugalmas, fizikai térben, ez a megoldás azért kerül le a palettáról, mert alacsony hatásfokú és gazdaságtalan. Egészen más a helyzet, abban az esetben, ha nem élettelen, hanem élő szervezet van kitéve az akusztikus hullámnak. Ennek vizsgálata nem képezi vizsgálatunk tárgyát, ezért érdemben ebben az esetben, ezzel nem kívánunk a továbbiakban foglalkozni.

A műszaki technológia és informatika rohamléptekben fejlődik. A további fejlesztés alapfeltétele, mint tudjuk a technológiaváltás, egyfajta reform megvalósítása a gyártástechnológiában. A további miniatürizálás az élő szervezet mintájára történik, onnan veszi mindazokat a megoldásokat, amelyek remélhetőleg tovább lendítik a fejlődés útján. Idő kérdése csupán, hogy organikus anyagok felhasználásával a biológiai rendszerek komplexitását közelítő, mesterségesen előállított, informatikai rendszer megvalósuljon. A méret, alkatelem szám és a sérülékenység, mint tudjuk szoros összefüggésben áll egymással. Arra alapozottan, hogy az élő szervezet akusztikus hullámokkal milyen hatékonyan támadható, az eszköz és hálózatfejlesztés tovább fokozza az elektronikai rendszerek sebezhetőségét. Akusztikus fegyverekkel ma még nehezen sebezhető informatikai rendszerek a közeljövőben várhatóan egyre kisebb teljesítménnyel és nagyobb hatásfokkal válnak támadhatókká. A „body lan” megoldásokkal a katonai infokommunikációs rendszerek fejlesztése ma olyan szakaszába kerültek, ahol az akusztikus fegyverekkel való támadás lehetősége mindinkább megteremtődik.

## Rádiófrekvenciás fegyverek

A rádiófrekvenciás irányított energiájú fegyverek elsősorban mikrohullámú energiákat használnak fel arra, hogy elérjék céljukat. A rádiófrekvenciás tartomány az akusztikus hullámoknál lényegesen nagyobb spektrumot fog át. Gyakorlati jelentősége leginkább a 80-100 kHz-nél nagyobb rezgésszámú elektromágneses hullámok esetében van. Minden alkalmazásnak megvan azonban a sajátos tartománya, amelyen belül használható és kihasználhatók mindazok a jelenségek, amelyek hozzátartoznak. A széles spektrumnak köszönhetően a lehetőségek csaknem korlátlanok. Fegyverként a teljes rádiófrekvenciás spektrumot mégsem kell és nem is lehet igénybe venni.

Az akusztikus fegyverekhez hasonlóan a rádiófrekvenciás fegyverek bevethetők személyek (élő erő) de még inkább technikai eszközök (elektronikus és villamos berendezések) ellen. Mindehhez a teljes rádiófrekvenciás tartomány egy meglehetősen szűk részét elegendő felhasználni. Technikai eszközök, számítógépes rendszerek, hálózatok támadása is csakúgy, mint a személyek ellen bevethető rádiófrekvenciás fegyverek pusztító, romboló hatása az energiatovábbításon alapul. Elektronikai, számítógépes rendszerek elleni támadáshoz szükséges továbbítandó energia nagyságrendekkel nagyobb, mint a biológiai rendszerek ellen

alkalmazandó fegyverek esetében éppúgy, mint a korábban tárgyalt akusztikus fegyverek esetében. A hasonlat csak felületes összehasonlításként állja meg a helyét, mivel a rádióhullámok terjedése és energiatovábbító képessége nagyságrendekkel jobb, mint a levegőben mechanikai rezgésekként terjedő akusztikus hullámoké. A nagyobb hatásfok következtében az elektronikai rendszerek támadását kereső megoldások éppen ezért a rádiófrekvenciás fegyvereket részesítik előnyben. Az energetikai viszonyok nem összehasonlíthatóak az akusztikus fegyverek esetében tapasztaltakkal, nevezetesen, hogy a nagyobb hullámhossz és az alacsonyabb frekvenciákon a kívánt hatás a hullámhosszal arányosan nagyobb kisugárzott teljesítménnyel érhető el. Ilyen elhamarkodott következtetéseket cáfol a rádiófrekvenciás energiatovábbítás egy különlegesen nagy hatásfokú, úgynevezett impulzusüzemű alkalmazása. Eszerint a rádióhullámok fegyvertechnikai alkalmazása esetén megkülönböztetünk:

- impulzusüzemű, és
- periodikusan folytonos rádióhullámokat sugárzó rádiófrekvenciás fegyvereket.

Az impulzusüzemű rádiófrekvenciás fegyverek körébe sorolhatók mindazok az eszközök, amelyek az energiahatás többszöri előállítására alkalmasak, tehát működésük közben nem roncsolódnak. Egyes impulzusfegyverek alapját képező magnetohidrodinamikai jelenségek több mint 60 éve ismertek.

Egyes kis energiájú rádiófrekvenciás fegyverek megfelelő méretezés esetén az élőerőre lehetnek hatással, ezáltal például a tömegoszlatásban is alkalmazhatóak. Hatásukra a célban fájdalom keletkezik, és így a hatása alá eső személy a területet minél hamarabb el akarja hagyni. Ezek a fegyverek a jelenlegi publikált teszteredmények alapján nem okoznak maradandó károsodást.

Működési elvük szerint 95 GHz-es frekvencián sugároznak, és a bőr alatti vízmolekulákat hevítik fel 55°C-ra, ezáltal égő érzetet keltenek anélkül, hogy valójában égetnének. A mikrohullámú sugarak áthatolnak a vastag ruházaton, megközelítőleg fél milliméter mélyen hatolnak a bőrszövetbe. Egy úgynevezett ADS (Active Denial System) berendezés körülbelül fél kilométeres hatótávolsággal rendelkezik, bár sugarai a környezet tereptárgyain nem képes áthatolni.

Egyes kritikák szerint az ADS rendszerek alkalmazása kimeríti a kínzás fogalmát és ezért alkalmazása nemzetközi konvenciókat sért. [10]

A nagy energiájú rádiófrekvenciás sugarak alkalmazásának célja a felvezetők károsítása, a mikroáramkörök túlterhelése, a villamos alkatrészek szigeteléseinek átütése és ezáltal az elektronikai eszközök tönkretétele.

Az ilyen fegyverek három részből állnak: egy energiaforrásból, melyek a mikrohullámok generálásához szükséges nagy mennyiségű energiát előállítják, tárolják, egy mikrohullámokat generáló eszközből, és egy antennából, mely a kívánt irányba sugározza a generált mikrohullámokat. [6] [1] A nagy energiájú fegyverek által jelentett fenyegetés igen komoly, mivel az élet számos – és köztük kritikus fontosságú – területén alkalmazunk elektronikus eszközöket. Számos televíziós híradás számol be arról, hogy ilyen típusú eszközöket boltokban kapható alkatrészekből összeállíthat bárki, aki ért az elektronikához, de léteznek készre gyártott és megvásárolható eszközök is, így akár terroristák is könnyedén felhasználhatják céljaik elérésében.

A nagy energiájú mikrohullámú fegyverek közül az elektromágneses impulzusbomba (EMP) a leghatékonyabb. Az elektromágneses impulzusfegyverek hatékonyan vethetőek be elektronikus hadviselésben és légitámadás során. [12] A másnéven E-bombaként is ismert eszköznek vannak nukleáris és nem nukleáris alapú implementációi is. Az EMP fegyver nukleáris változata a nagy magasságban felrobbantott nukleáris töltet által keltett intenzív, de rövid ideig tartó elektromágneses mező hatásait használja ki. A robbanáskor keletkező több

ezer voltos elektromágneses lökéshullám visszafordíthatatlan károsodást okoz a területen elhelyezkedő elektronikus eszközökben.[12]

A nem nukleáris elektromágneses impulzusfegyverek egyéb megoldásokat használnak a nagy energiájú elektromágneses lökéshullám előállítására. A tápenergiát előállító eszköz lehet a Marx generátor vagy a fluxus kompressziós generátor. [6] [5] A fluxus kompressziós generátor több MJ energiájú elektromos energiát képes előállítani rövid (10-100 μs) ideig. A viszonylag kisméretű eszköz több MW impulzusteljesítményű energiaforrásnak számít. Működési elve azon alapul, hogy egy induktív energiatárolóban tárolt elektromágneses energiát robbantással, a tekercs meneteinek rövidre zárásával áramimpulzussá alakítja. [5] A Marx generátor számos kondenzátort alkalmaz, melyek mindegyike párhuzamosan van kötve, és ugyanarra a feszültségre van feltöltve. A kondenzátorok szikraközökkel vannak elválasztva egymástól. A generátor elsütésekor a szikraközök begyújtanak és az addig párhuzamosan kapcsolt kapacitásokat sorba kapcsolják, így nagyfeszültséget generálnak ezzel. [6] [13]

Az E-bomba hatását vizsgálva, teljes bizonyossággal kijelenthető, hogy mai ismereteink szerint ez a fegyvertípus jelenti a legnagyobb veszélyt az elektronikai és az elektromos berendezésekre, beleértve a számítógépes és hálózati rendszereket is. Hatása röviden abban nyilvánul meg, hogy az elektromos szigetelések átütési szilárdságát meghaladó feszültségek, és áramokat indukál a vezetőkben. Az impulzus időtartama 4-100ns, de ez idő alatt több száz A nagyságú áramok folyhatnak az elektromágneses hullámnak kitett vezetőkben. Hatótávolsága, pusztító ereje nagyon sok mindentől függ. Egyrészt az eszköz felépítésétől, másrészt a robbantásának a helyétől, körülményeitől. Mivel az impulzusbombában alkalmazott fluxuskompressziós generátort a robbanótöltet hozza működésbe, ennek következtében az eszköz megsemmisül. Bevetése a bombák mintájára történik. Robbantása csakúgy, mint az atombomba esetében - ahol elsőként ezt a jelenséget is sikerült megfigyelni-, megadott magaságban történik. Pusztító hatást a besugárzott körzeten belül található elektronikai és számítógéprendszerekre gyakorol. Korábban említett indukált áramok és feszültségek mindenekelőtt a legérzékenyebb eszközök, és legnagyobb elemsűrűségű áramköri alkatelemeket teszi tönkre. Ilyenek a memóriák, mikrovezérlők és mikroprocesszorok. Ezek a manapság minden eszközben előfordulnak. A védelemmel kell és lehet is foglalkozni, de a tökéletesen zárt Faraday-kalitkán kívül kellően hatékony megoldás nem ismert. Egyrészt azért, mert rendkívül költséges ilyen védelmi megoldásokat eredményezne, másrészt az impulzusfegyver bevetésének gyakorisága még nem teszi indokolttá, hogy a fejlesztők ezen gondolkodjanak.

A folytonos, periodikus jel előállítására alkalmas eszközök közül megemlíthető a Vircator (Virtual Cathode Oscillator), amely a fedélzeti rádiófrekvenciás fegyverek abba a csoportjába tartozik, amely többször felhasználható és az E-bombával ellentétben, parabola és tölcsérsugárzó segítségével irányított nyaláb formájában közvetíti az energiát. Az eszköz leírásával foglalkozó ismeretanyag szintén megtalálható a világhálón. [3] A HERF eszközök tényleges felépítéséről, paramétereiről még viszonylag keveset tudunk. Hatása csakúgy, mint az E-bomba esetében az energiatovábbításon alapul. Az energiatovábbítás rádióhullámok segítségével, a fegyvertechnikai alkalmazásokon túlmenően, meglehetősen futurisztikus ötletnek számít, ami úgy tűnik szerencsére megragadt a fantázia szintjén. Számítógépes rendszerekre potenciális veszélyt jelentő rádiófrekvenciás fegyverek birtokában valószínűsíthetően a nagyhatalmak vannak. A fejlesztésekről szóló tudósítások nem tartoznak a nyílt forrásokban gyakran közölt hírek közé.

### Lézer fegyverek

Az elektronikus és számítógéprendszerek mára elválaszthatatlan egységgé fonódtak össze. Lehetetlen és értelmetlen egyikről vagy másikról külön beszélni. A rugalmas és egyszerűen programozható eszközök alkalmasak a legegyszerűbb programvezérelt feladatoktól kezdve

rendkívül komplex feladatok ellátására egyaránt. Nem nevezhető korszerű haditechnikai eszköznek az olyan, amiben ma nem található egy vagy több programvezérelt eszköz, mikroprocesszor. Az olyan kivételektől eltekintve, mint amilyen például egy egyszerű irányítás nélküli robbanótöltet, a legtöbb katonai eszköz önálló vagy valamilyen hálózat elemeként, számítógépes rendszerként működik.

Ilyen a cirkáló rakétafejbe építetett komplex elektronikai rendszer, ami a töltet nagypontosságú célba juttatását végzi, de ilyenek a levegő-levegő rakéták hőkövető irányító rendszere vagy éppen a közvetlen veszélyt nem jelentő kamerák és optikai rendszerek. Ballisztikus rakéták, fegyverek és számtalan komplex elektronikai rendszer, ami kis teljesítményű, úgynevezett vakító lézerekkel vagy több száz kW teljesítményű lézerfegyverekkel támadhatók. [24] A vakító lézerek a céltévesztést szolgálják, míg a nagyteljesítményű átégető lézerekkel a ballisztikus rakéta robbanótöltete robbantható fel a célba érése előtt. A lézerfegyverekkel kibővült fegyverarzenál nem áll messze attól, hogy a múlt század közepén és második felében született tudományos fantasztikus elképzeléseket valóra váltsa. Ennek köszönhetően a lézerfegyverek, függetlenül attól, hogy félrevezető vagy fizikailag megsemmisítő céllal kerülnek bevetésre a legkorszerűbb és talán a legígéretesebb eszközök egyike.

A lézer fegyvereknek három fajtája létezik:

- kis energiájú lézer fegyverek,
- lézer-indukált plazma fegyverek,
- nagy energiájú lézer fegyverek.

A kis energiájú lézer fegyverek (Laser Dazzler) élő erőn és optikai érzékelőkön alkalmazhatóak. Pár száz métertől pár kilométerig terjed a hatótávolságuk. Látható fény tartományban hatásukat az élő szervezetre fejtik ki, dezorientiációt és a látászavart okozva azáltal, hogy átmenetileg megvakítják a célszemélyt. Optikai érzékelők ellen alkalmazva képesek infravörös tartományban is működni. 2006-ban az iraki háborúban az amerikai erők sikerrel alkalmazták gépfegyverre szerelhető verzióját az ellenőrző pontokon, olyan célszemélyek ellen, melyek nem voltak hajlandóak megállni. Lehetséges védekezési mód az ilyen fegyverek ellen keskenysávú optikai szűrők alkalmazása, melyek a lézer frekvenciáján szűrik a fényt. Ennek kiküszöbölésére adaptív, több frekvencián is sugárzó lézerfegyvereket fejlesztettek ki. [14]

A lézer-indukált plazma fegyverek (LIPC) lézer fényt használnak fel arra, hogy a levegőt ionizálva egy elektromosságot vezető nyalábot hozzanak létre. Az így terjedő elektromos energia villámcsapás-szerű hatást fejt ki, ezáltal bénítja az emberi célpontot vagy rongálja meg az elektromos berendezéseket. Az elektromos energia skálázható úgy, hogy halálos vagy nem halálos hatást fejtsen ki. Védekezni ellene mágneses vagy elektrosztatikus mezővel, vagy Faraday-kalitka alkalmazásával lehetséges. [15]

A nagy energiájú lézer fegyverek alkalmazása elsősorban a védelem terén jelentős. A mostanában jelentős publicitást kapó Airborne Laser projekt is ebbe a csoportba tartozik. Az ilyen fegyverek gyakorlati alkalmazása elsősorban a ballisztikus rakéták elhárítására terjed ki. Az Airborne Laser projekt keretén belül az Amerikai Egyesült Államok légterében cirkáló módosított Boeing 747-es repülőgép, a fedélzetén elhelyezkedő lézerágyúval képes megsemmisíteni a becsapódást megelőzve az ellenséges rakétákat nagy távolságról. Az izraeli hadsereg által kifejlesztett MTHEL (Mobile Tactical High Energy Laser) rendszer hasonló célokat szolgál. Ez a mobil elhárító rendszer az ellenséges rakétákat képes érzékelni, és becsapódásukat megelőzve megsemmisíteni azokat. [6] [16] A nagy energiájú lézerek hatékonysága abban rejlik, hogy igen nagy energiát képesek kis területre sugározni. A területre érő energia egy része visszaverődik ugyan, de nagy része elnyelődik, felhevítve így a cél felszínét. Az égési folyamat során a lézersugár rövid időn belül átégeti a cél felszínét, és az a keletkező hő hatására megsemmisül. [17]

Egy másik rendező elv és szempont szerint a lézer technológia fizikai jellemzőket veszi figyelembe. Eszerint megkülönböztetünk:

- gáz
- folyadék
- szilárdtest lézereket.

A gázlézerek több száz KW teljesítményükkel a ma ismert legnagyobb teljesítményű lézer fegyverek. Átégető lézerekként tervezik a bevetésüket Az oxigén-jód gázlézer rendkívül nagy mérete (több 10m) miatt a mobilizálása speciális földi szállítójárművet igényel, vagy egy átalakított Boeing 747 teherszállító repülőgép fedélzetén helyezhető el. [24] Jellemzője, hogy az infra (1000-1200nm), hullámtartományban sugároz.

A folyadéklézereket szokás festéklézereknek is nevezni. Haditechnikai jelentősége nem annyira ismert, viszont mint különlegességet mégis érdemes megemlíteni. Jellemzője, hogy széles frekvenciatartományban hangolható, az ibolyántúli tartománytól egészen az infra tartományig. Bár teljesítménye messze elmarad a gázlézerekhez képest, mégis ez a tulajdonsága előnyösen kihasználható, minden olyan esetben, amikor a célfelületen tervezett hatás éppen ennek kihasználása révén érhető el.

A harmadik kategóriába tartozó lézer, a szilárdtest lézer. Fejlődésének üteme minden képzeletet felülmúlt. Teljesítménye ma meghaladja a 30 kW-ot. Nagy távolságú bemérő, követő, követő lézerként használható a $CO_2$ lézer helyett. Bemérő, rakétaelhárító vakító lézerként alkalmazható. Előnye a kis mérete, nagy hatásfoka. Teljesítménye alkalmassá teszi lövedék és rakétaelhárító feladatok végrehajtására.

## Részecske fegyverek

A részecske fegyverek nagy energiával rendelkező atomokat vagy elektronokat sugároznak a cél felé, hogy annak atomi vagy molekurális struktúráját roncsolják. Az elektron fegyver (Electron Particle Bean Weapon) működése során a cél elektromos áramköreiben visz végbe maradandó károsodást. Élő célt elérve a áramütés szerű hatással rendelkeznek. A céltárgy elektromos ellenállását kihasználva, az abban keletkező magas hőmérséklet okoz károsodást.

A részecskesugár kialakítására semleges töltésű hidrogén gázt ionizálnak, azáltal hogy megszabadítják egy elektronjuktól, vagy egyéb módon olyan állapotba gerjesztik, hogy egy szabad elektront megkötni legyenek képesek. Ha a hidrogén atom többlet elektronnal rendelkezik anionná, ha elektront vesztett, akkor pedig kationná alakul. A töltéssel rendelkező hidrogén atomokat részecskegyorsító berendezésben felgyorsítják. A pozitív és a negatív töltésű részecskék gyorsítására más-más típusú részecsekgyorsító berendezések szükségesek. A részecske fegyverek a nagy sebességű részecskék kinetikus energiáját felhasználva okoznak károsodást a célban. A részecske-sugár energiája akár egy GJ is lehet, sebessége megközelíti a fénysebességet [18]

A részecskefegyverek kifejlesztése a 20. század közepén kezdődött. Céljuk az interkontinentális ballisztikus rakéták elleni védelem megteremtése volt. A részecskesugár hasonló jelenség, mint a természetben előforduló villámcsapás: a villámcsapásban nagy sebességű elektronok vándorolnak a pozitív töltésű terület felé. A villámcsapásban áramló elektronok sebessége jóval kisebb, mint a részecske fegyver által generált sugárban áramló részecskék sebessége, de a jelenlévő részecskék száma nagyságrendekkel nagyobb. A részecskefegyver által kibocsátott sugár részecskéi a céllal ütközve átadják kinetikus energiájukat a cél atomjainak. Ennek hatására a cél részecskéi gerjesztett állapotba kerülnek, ami gyors hőmérsékletnövekedéssel jár, és a cél felrobban a sugár hatására. [19]

A részecskefegyvereknek két fajtája van: a töltéssel rendelkező részecskéket és a semleges töltés részecskéket felhasználó típus. A töltéssel rendelkező részecskesugár főleg földi környezetben (endoatmoszférikus), a semleges töltésű részecskesugár az űrben hasznosítható (exoatmoszférikus). Az endoatmoszférikus részecskefegyverek legnagyobb technológiai

kihívása a részecskék gyorsításához szükséges nagy energia előállítása, míg az exoatmoszférikus fegyvereknél a részecskesugár fókuszálása a több ezer km távolságra lévő céltárgyra jelent problémát. [19]

## SZÁMÍTÓGÉPES RENDSZEREK VÉDELME ÁRNYÉKOLÁSSAL

A számítógépes rendszerek igen érzékenyek a statikus energiákra. Minden eszköz fel van vértezve megoldásokkal, melyek a rendszerben fellépő felesleges zavaró energiát semlegesíteni képes. Ezért szükséges például a számítógépek házát megfelelő módon földelni. Abban az esetben, ha a földelés nem kielégítő a használat mértékétől függően pár nap vagy hét alatt a számítástechnikai berendezés meghibásodik, és a hardver elemek cseréje szükséges. A statikus töltések által hordozott energia viszont nagyságrendekkel kisebb, mint amit egy irányított energiájú fegyver képes a rendszerbe juttatni. Ahhoz, hogy elektronikai eszközeinket megvédjük, olyan speciális környezetbe kell juttatni őket, ahová a mikrohullámú energia nem képes bejutni. Megfelelő falvastagság, fémlapok alkalmazása vagy a Faraday kalitka sikeresen kivédi az ilyen típusú irányított fegyverek által jelentett fenyegetést, mivel ezeken a felületeken a mikrohullámú sugárzás nem képes áthatolni.

A Faraday kalitka egy zárt tért alkot. A teret határoló elemek elektromosságot vezető anyagból állnak. Faraday kalitkát alkalmaznak a mikrohullámú sütőkben is, hogy megakadályozzák, hogy az előállított energia ki tudjon lépni a készülékből megóvva ezzel a környezetet és javítva a berendezés hatékonyságát, de a speciális kutatólaborok is hasonló módon vannak védve a külső behatások ellen. Az alkalmazott Faraday kalitkával szemben támasztott követelmény csupán, hogy fala elegendő vastagságú legyen, és a rései kisebbek legyenek, mint az a hullámhossz, amelytől a kalitkán belül található teret meg akarjuk védeni.

A Faraday kalitka azon az elven alapul, melyet Michael Faraday fedezett fel, miszerint az elektromosan töltött részecskék a vezető külső felületén helyezkednek el, és annak belsejére semmilyen hatással nincsenek. Ennek megfelelően a kalitka belső oldalának potenciálja megegyezik a belső tér potenciáljával, míg a külső felület potenciálja a külső tér potenciáljával egyezik meg.

## ÖSSZEGZÉS

Az irányított fegyverek közül, mint látható, a mikrohullámú és a nagy energiájú rádiófrekvenciás fegyverek a legveszélyesebbek az elektromos berendezésekre nézve. Az elektronikai berendezésekre nézve visszafordíthatatlan károsodásokat okozó hatásuk, és viszonylag kis méretük, egyszerű felépítésük lehetővé teszi széleskörű alkalmazásukat és könnyű hozzáférésüket. Az ilyen fegyvert használó támadónak nincsen szüksége arra, hogy ismerje támadott rendszert, hatásuk visszafordíthatatlan, akkor is kárt okoznak a célrendszerben, ha azok nem működnek (kikapcsolt állapotban vannak, vagy áramtalanítottak). A védelem implementálása során az egész rendszert érintő változásokat kell bevezetni. [20]

Az elkövetkezendő pár évben az ilyen fegyverek nagy valószínűséggel jelentős fenyegetettséget fognak jelenteni. Paramétereik megfelelnek a különböző terrorista csoportok számára, hiszen egy igen hatékony eszköz áll a rendelkezésükre, mely kis méretben képes rendkívül eredményes támadást kivitelezni, társadalmunk pedig egyre nagyobb mértékben függ az elektronikai berendezésektől. A technológia fejlődésével egyre több megoldás lesz beszerezhető illegális forrásokból, mivel a megfelelő fegyver előállítási költségei egyre csökkennek. Ezek ismeretében a biztonsági szakembereinek fontos feladata lesz a jövőben a kritikus informatikai és egyéb elektronikai eszközök felvértezése a mikrohullámú és nagy energiájú fegyverek elleni védelemmel.

## IRODALOMJEGYZÉK


[1] http://en.wikipedia.org/wiki/Directed_energy_weapon

[2] http://en.wikipedia.org/wiki/Ebomb

[3] http://en.wikipedia.org/wiki/Herf

[4] JP 1-02, DOD Dictionary of Military and Associated Terms

[5] Carlo Kopp: An Introduction to the technical and operational aspects of the electronic bomb [1996 November, Air Powers Studies Centre, ISBN 0 642 26415 5]

[6] Dr. Ványa László: Irányított energiájú fegyverek [előadás]

[7] http://www.atcsd.com/site/content/view/37/50/

[8] http://en.wikipedia.org/wiki/Long_range_acoustic_device

[9] http://www.atcsd.com/pdf/LRAD-Tech-Backgrounder.pdf

[10] http://en.wikipedia.org/wiki/Active_Denial_System

[11] http://www.zmne.hu/kulso/mhtt/hadtudomany/2004/2/2004-2-10.html

[12] Carlo Kopp: A doctrine for the use of ElectroMagnetic Pulse Bombs [1993]

[13] http://en.wikipedia.org/wiki/Marx_generator

[14] http://en.wikipedia.org/wiki/Laser_dazzler

[15] http://en.wikipedia.org/wiki/Electrolaser

[16] http://www.israeli-weapons.com/weapons/missile_systems/systems/THEL.html

[17] http://www.ausairpower.net/AADR-HEL-Dec-81.html

[18] http://en.wikipedia.org/wiki/Particle_beam_weapon

[19] http://www.airpower.maxwell.af.mil/airchronicles/aureview/1984/jul-aug/roberds.html

[20] http://globalguerrillas.typepad.com/globalguerrillas/2004/05/journal_homemad.html

[21] http://en.wikipedia.org/wiki/Faraday_Cage

[22] Judy Muller: Sound and Fury: Sonic Bullets to Be Acoustic Weapon of the Future. http://www.hartford-hwp.com/archives/27a/115.html (2007. 02. 01.)

[23] Roxana Tiron: Acoustic-Energy Research Hits Sour Note http://www.nationaldefensemagazine.org/issues/2002/Mar/Acoustic-Energy.htm (2007. 02. 01.)

[24] Csuka Antal: Az irányított energiájú fegyverek perspektivikus alkalmazása az amerikai hadseregben, Repüléstudományi közlemények, Különszám 2007. Április 20.

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Farkas Imre**
Zrínyi Miklós Nemzetvédelmi Egyetem
farkas.imre@geodezia.hu

# HATÉKONY KIÉRTÉKELÉSI LEHETŐSÉGEK AZ MGCP PROJEKT SORÁN

***Absztrakt***

*A 90'-es években végbement világpolitikai, gazdasági, társadalmi változások következtében a katonai feladatok is nagy átalakuláson estek át. A globális terrorizmus elleni harc, a béketeremtő, illetve békefenntartó műveletek újabb kihívásokat támasztottak. Jelentősen megnőtt az igény a nagy méretarányú, megbízható pontosságú, részletgazdag, komoly információtartalommal bíró térinformatikai termékek iránt.*
*Az MGCP (Multinational Geospatial Co-production Program / Többnemzeti Térinformatikai Együttműködési Program) keretében, mintegy 28 NATO tagországgal egyetemben állítjuk elő a Föld, katonailag kiemelkedő jelentőséggel bíró részeiről, 1:50.000-es, illetve 1:100.000-es méretarányú 1° x 1°-os földrajzi koordinátákkal határolt cellákból álló digitális térinformatikai adatbázist. A nemzetközi szerepvállalással hazánk az expedíciós tevékenységhez szükséges térinformatikai, térképészeti adatforráshoz fog hozzájutni. E cikkben bemutatom az adatnyerés irányításom alatt kidolgozott, Magyarországon alkalmazott folyamatát, mellyel eleget tudtunk tenni a szigorú nemzetközi szakmai követelményeknek. Bemutatom a távérzékelési adatok interpretációjának e projekt keretein belül alkalmazott metodikáját.*

*The changes in world-politics, economics, and social changes during the nineties also caused significant transformations in military tasks. The war on global terrorism, peacemaking and peacekeeping operations raised new challenges. The demand for high resolution, high accuracy and detailed geographic information products has increased significantly.*
*During the course of the MGCP (Multinational Geospatial Co-production Program) in conjunction with 28 NATO member states we are producing an 1:50.000 or 1:100.000 scale digital geoinformatics database which is divided into 1° x 1° cells of the strategically important areas of Earth. With the international undertaking our country will acquire geographic and topographic information important for expeditionary agendas. Within this article I will present the procedures of data extraction used in Hungary, which was developed under my*

*management and can stand up to the strict international professional requirements. I will also present the methodology used in this project for interpreting the remote sensed data.*

***Kulcsszavak:*** *Többnemzeti Térinformatikai Együttműködési Program, digitális térinformatikai adatbázis, nemzetközi szerepvállalás, térinformatikai- térképészeti adatforrás, távérzékelési adatok interpretációja ~ Multinational Geospatial Co-production Program, digital geoinformatics database, international undertaking, geographic and topographic information, interpreting the remote sensed data*

## AZ MGCP PROJEKT

### 1.1 A projekt bemutatása

Az **MGCP** rövidítés a Multinational Geospatial Co-production Program angol kifejezésből ered és Többnemzeti Térinformatikai Együttműködési Program-ot jelent.

A projektet az USA Nemzeti Térképész Hírszerző Hivatala (USA NGA) kezdeményezte 2003 áprilisában. A nemzetközi katonai program célja, hogy a Föld felszínének minél nagyobb részéről nagy felbontású térinformatikai adatbázis készítése, és annak folyamatos frissítése. Az együttműködés eredményeként a világ területéről olyan vektoros térképek, téradatbázisok állnak majd a programban résztvevő kormányok rendelkezésére, melyeknél minden egyes kiértékelt elemhez tartozik egy attribútum tábla, mely leíró adatokat tartalmaz az adott objektumról. Az együttműködésben való részvétel arányában a kormányok betekintést nyernek az elkészült állományokba. A program végrehajtása során fontos tényező az idő- és költséghatékonyság, így papíralapú térképek csak a szükséges területekről és mennyiségben készülnek. E kiemelt fontosságú nemzetközi projektnek köszönhetően biztosítható, hogy mindig naprakész térinformatikai adatok álljanak a projektben résztvevő országok rendelkezésre és azok megfelelő formában, és időben jussanak el a közreműködőkhöz.

A jelenlegi magyarországi projekt célja mintegy 28 db, 1:50 000 illetve 1:100 0000 méretarányú topográfiai térkép adatsűrűségével megegyező, $1^o$ x $1^o$ –os méretű, egész értékű földrajzi koordinátákkal határolt cella.

Az elsődleges munkaterületek 2006-2008-ban európai jellegű, 2009-2011-ben pedig afrikai jellegű területek kerülnek feldolgozásra. A kiértékelést 1:50 000 méretarányú Nemzetközi Katonai Szelvényezési rendszer szerint kell végrehajtani, a vonatkoztatási rendszer WGS84.

### 1.2 Hivatalos alapanyagok

A téradatokat (pont, vonalas és felület objektumokat) a rendelkezésre álló források felhasználásával kell előállítani.

A Magyarországon végrehajtandó kiértékelés elsődleges alapadatai a 2,5m terepi felbontású digitális (SPOT - georeferált), és a kiemelt városoknál 0,5m terepi felbontású digitális űrfelvételek (Quickbird, Kompsat - georeferált), illetve az azokból generált ortofotók.

További (másodlagos) alapanyagok:

- 1:50 000 méretarányú katonai topográfiai térképek szkennelt, georeferált állományai;
- topográfiai jelkulcskészlet;
- országhatárokat tartalmazó adatállományok;
- GeoNames – Földrajzi nevek adatbázisa; településjegyzék;

- AAFIF – „Automatikus légi adatbázis információs fájl” (Automated Airfield Facilities Information File);
- DVOF – „DMA függőleges akadály adatok digitális nyilvántartása” (DMA Vertical Obstruction File);
- jelkulcs készlet a leadandó ellenőrző térképlaphoz (GeoSym);
- autósatlasz adott területre.

Egyéb alkalmazandó anyagok, szabályzatok:

- MGCP Műszaki Referencia Dokumentum (**T**echnical **R**eference **D**ocument, a továbbiakban **MGCP TRD**), melynek főbb részei:
  - MGCP objektum- és attribútum katalógus,
  - MGCP szemantikai értelmező modell,
  - MGCP kiértékelési útmutató,
  - Az MGCP metaadatok specifikációja,
  - MGCP csatlakoztatási folyamat.
- Az adatnyerést végrehajtó Geodézia Zrt. Belső utaításai.
- MGCP_FC_optional attributes.xls – objektumonként tartalmazza azokat az attribútumokat, amelyek TRD szerint opcionálisak, de kitöltésük jelen projekt szempontjából kötelező jellegű.
- MGCP fórum (megrendelői és kivitelezői hozzáféréssel).

### 1.3 Kiértékelés végrehajtásához alkalmazott szoftver

Az adatnyerési és ellenőrzési technológia szoftver környezetét az Intergraph Co. GeoMedia Pro termékre épülő GeoInformational Production System (GIPS) szoftver rendszer alkotja. Az adatállományok kezelése Oracle adatbázis-kezelő rendszerben történik.

## 2. MGCP PROJEKT ADATNYERÉSI IRÁNYELVEI, PROBLÉMAFELVETÉS

A projekt végrehajtásakor rendkívül szigorúan szabályozott szakmai követelmény rendszernek kell meg felelni a kiértékelés végrehajtóinak. A különleges műszaki elvárások egyedi kiértékelési technológia kidolgozására kényszerítették az irányításom alatt dolgozó szakembereket. Az alábbiakban ismertetésre kerülnek a műszaki keretek, elvárások, valamint az ezek betartására kidolgozott adatnyerési metodika.

### 2.1 Általános adatnyerési szabályok

Az objektumok csak abban az esetben kerülhetnek kiértékelésre, ha azok a digitális ortofotón, mint elsődleges alapanyagon azonosíthatóak. A kiértékelés során a digitális képanyagot mindig a legmegbízhatóbb forrásnak kell tekinteni, különösen a geometriai információk tekintetében. A kiegészítő anyagok olyan helyzetekben segíthetnek, amikor bizonyos információk nem jelennek meg a képanyagon.

A kiértékelés kiterjed:

- a felszíni topológiára (felület objektumok),
- az épületekre és építményekre,
- a természetes és mesterséges vízhálózatra,
- a légi közlekedésre,
- a közúti közlekedésre,

- a vasúti közlekedésre,
- a földfelszínre és növénytakaróra,
- a közművekre (pl. erőmű).

Az adatbázis ideális kialakítását nemzetközi szinten egy szabályrendszer határozza meg. Ez a szabályrendszer az MGCP műszaki dokumentációja, melyből a kiértékelő személy pontos útmutatás alapján köteles elvégezni az adatnyerési munkafolyamatot.
Tehát az űrfelvételen történő azonosítás után, a TRD szabályrendszer kiértékelési útmutatója alapján kategorizálni kell, amely alapján a kiválasztott objektum felvételre kerül.

Az MGCP TRD az objektumokra és attribútumokra „kötelező" (mandatory), „feltételes" (conditional) és „opcionális" (optional) besorolást alkalmaz. Minden olyan objektumot, amely a szabályzatban „kötelező" vagy „feltételes" besorolással szerepel, ki kell értékelni. Az opcionális besorolású objektumokat csak abban az esetben kell kiértékelni, ha digitális ortofotón egyértelműen azonosíthatók. [1]

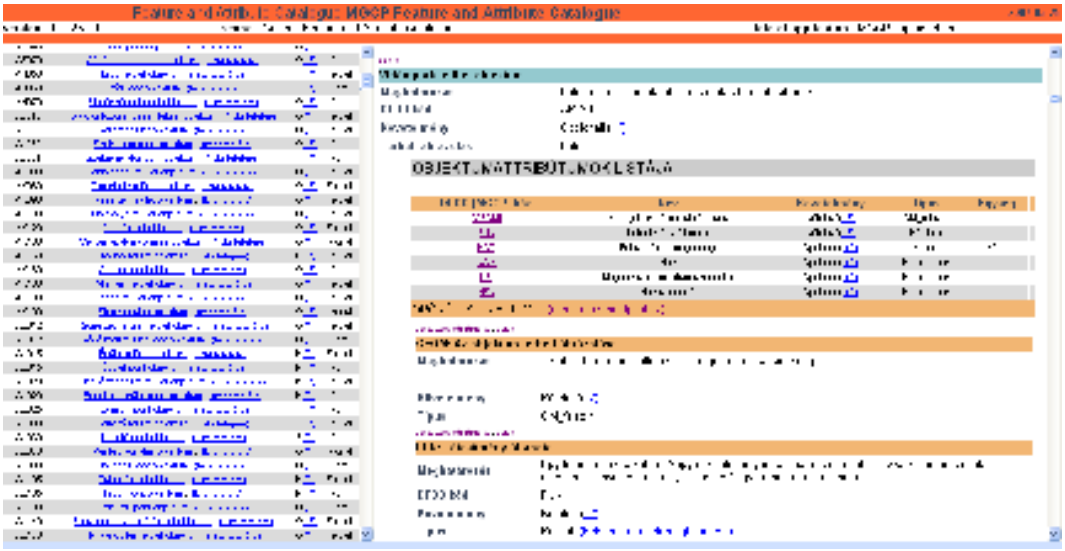
1. ábra: Példa egy objektum kiértékelésének meghatározására [1]

Az interpretáció feltételeit a TRD kiértékelési útmutatója tartalmazza, ezeket a szabályokat az adatnyerés során a kiértékelő személynek szigorúan be kell tartania. E szabályzat minden, a projektben szereplő objektumhoz tartozó pontos definíciót, útbaigazítást, képanyagon való megjelenési példát tartalmaz. Tartalmazza továbbá az adott objektum környezetében található jellemző objektumok listáját, alkalmazható geometriai típusait (pont, vonal vagy felület) és azokra vonatkozó kiértékelési feltételeket és kritériumokat. [2]

Minden kiértékelt objektumokhoz tartozik egy attribútum tábla, melynek mezői különböző alapanyagok alapján kerülnek feltöltésre. Az elsődleges alapanyag alapján meghatározásra kerül a geometriai helyzet, valamint az objektumok attribútum tábláinak a feltöltéséhez szükséges adatok. Az attribútum táblák pontos feltöltése érdekében a rendelkezésre álló segédanyagok

felhasználására is szükség van. A térinformatikai adatbázis naprakész állapotra hozása a vektoros kiértékeléssel egy időben történik, ezért a kiértékelőknek körültekintőnek kell lenniük, és fontos a TRD ismerete és alkalmazása.

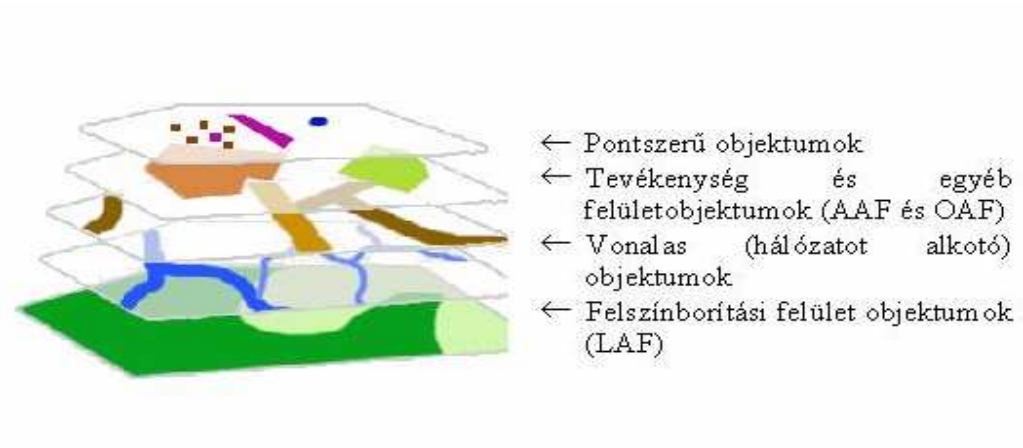
Az objektum- és attribútum katalógus tartalmazza az objektumok típusait és azok attribútumainak felsorolását pontos meghatározással, valamint az adott attribútumok lehetséges, felvehető értékeit és azok definícióit.



2. ábra: Példa egy objektum attribútumozására [2]

A „kötelező” besorolású attribútumokat minden esetben meg kell adni, a „feltételes” és „opcionális” besorolású attribútumok megadása nem kötelező, azonban ha bármilyen rendelkezésre álló forrásból származik adat ezen attribútumok valós értékének megállapítására, akkor tölteni kell a megfelelő attribútum értékekkel.

A szemantikai modell alapjai az objektumok, melyek meghatározott viszonyrendszerben helyezkednek el egymáshoz képest.




3. ábra: Topológiai modell [3]

Tapasztalataink alapján további kiértékelési nehézségeket okoz a topológiai modell előállítása, ugyanis az objektumok kapcsolata egymással nagyon szoros mind attribútum, mind geometriai értelemben. Szakmai irányításommal kollégáim részletes szoftveres és vizuális tematikus ellenőrzéseket dolgoztak ki e problémák feloldására.

### 2.2. A kiértékelés folyamata, jellemzői

Az adatnyerési folyamat szelvény szinten történik. A hibalehetőségek csökkentése céljából az adatnyerést különböző szakaszokra bontva hajtjuk végre.

A kiértékelés első szakaszában a vonalas hálózati elemek felvétele történik adott sorrendben: víz-, út- és vasúthálózat, valamint ezen objektumokhoz kapcsolódó objektumok.

A kiértékelendő objektumok a következők:

- **Vízhálózati elemek:** folyó (BH140), csatorna (BH020), öntözőcsatorna (BH030), vízvezeték (BH010), tó (BH080), víztározó (BH130)…; *kapcsolódó elemek:* kompátkelő (AQ070), zsilip (BI030), gát (BI020)…

Ez az objektumcsoport kiértékelhető mind vonalas objektumként, mind felületként. Kiértékelendők azok az objektumok, melyek a teljes hálózathoz szükségesek, illetve felépítendő a kapcsolatrendszer az elemek között. A terület jellegének pontos ábrázolása érdekében a vízelvezető objektumokat is ki kell értékelni. Az egyes szakaszok ne legyenek 300 méternél rövidebbek. Csatornának csak az olyan vízfolyás minősül, amely vízi közlekedésre alkalmas (hajózható), és egyáltalán nem, vagy csak ellenőrzött mértékben áramlik. A vízellátást segítő, termőföld öntözésére vagy vízelvezetésére szolgáló mesterséges vízfolyások az öntözőcsatornák. Ha az öntözőcsatorna hossza 300 méternél kisebb, de mindkét végén vízelvezető objektumhoz kapcsolódva nagyobb vízelvezető hálózat részét képezi, akkor hálózati összekötőként lehet kiértékelni.

A fent felsorolt típusok közül az egymással érintkezők összefüggő topológiai vízrajzi hálózatot alkotnak. Ez azt jelenti, hogy ha a felület, vonalas és pont szerű objektumok a valóságban csatlakoznak, akkor az ábrázolás során is csatlakoztatni kell azokat. [3]

- **Úthálózati elemek:** út (AP030), földút (AP010), ösvény (AP050); *kapcsolódó elemek:* csomópont (AP020); híd (AQ040); töltésút (AQ064); töltés (DB090), alagút (AQ130), alagút (DB070)…

Az utakat úgy kell kiértékelni, hogy az úthálózat teljes legyen, és a lakott vagy használatban lévő területek össze legyenek kötve. Minden utat fel kell venni, egészen a javasolt minimális 300m hosszúságig és 300m-enként, és teljes összekapcsolt elemek hálózatát kell kialakítani. Az utcahálózatot azok az utak alkotják, melyek teljes egészükben lakott területeken belül vannak, vagy annak határát alkotják, és a helyi úthálózat keretére vannak építve. Az utcamintákat úgy kell kiértékelni, hogy az megfelelően képezze le az egyes lakott területek sűrűségét, visszaadja a település szerkezetét. Az utak helyes szerkezeti áttekinthetőségének érdekében a kiértékelés során a szoftver segítségével tematikus megjelenítés segít az utak kategorizálásában. Az érintkező közúti objektumok összefüggő topológiai hálózatot alkotnak. A közutakkal összefüggő vonalas objektumoknak van egybeeső geometriájuk azokkal a közúti objektumokkal, amelyeket kiszolgálnak. [4]

- **Vasúthálózati elemek:** vasút (AN010), vasúti mellékvágány (AN050); *kapcsolódó elemek:* mozdonyfordító (AN075)…

A felszínborítást, illetve az egyéb terület felületek határvonalait össze kell hangolni a vonalas objektumok által alkotott hálózattal, a keletkező szilánkok és egyéb topológiai hibák elkerülése végett. Amennyire lehetséges – az alapanyagot figyelembe véve – egy adott felszínborítási felület határán futó vonalas objektum töréspontjainak egybe kell, hogy essenek a felület töréspontjaival.

A felületek és vonalak töréspontjainak meghatározása során a két pont közötti minimális távolság 5m lehet. A vonalas objektumoknál figyelni kell arra, hogy elemei egységes hálózatot alkossanak és tükrözzék az adott kiértékelt terület jellegét hálózat szempontjából (Pl. települések utcahálózata). A vonalas objektumokat csak akkor törjük meg, ha azt a hálózat megkívánja és változik valamely attribútuma. Az egymással érintkező vasúti objektumok összefüggő topológiai hálózatot alkotnak.

A hálózati elemek kiértékelése után sor kerülhet a **felszínborítás**t alkotó felület objektumok (továbbiakban LAF-ok) kiértékelésére. A elkészült, műtárgyak nélküli hálózatokat célszerű felhasználni a 100 %-os területlefedést meghatározó felszínborítási felületek felvételekor. Minden LAF-ot ábrázolni kell, függetlenül attól, hogy a felületek határán halad-e valamely hálózat objektuma vagy sem. [5]

A kiértékelendő objektumok a következők:

- Bánya (AA010), kőfejtő (AA012), beépített terület (AL020), sósivatag (BH160), sziget (BA030), tundra (BJ110), talajborítás (DA010), mezőgazdasági terület (EA010), füves terület (EB010), bozótos (EB020), fás terület (EC0030)…

A területfedés után kerül sor a **tevékenység** felületszerű objektumok (AAF) kiértékelésére. A tevékenység felületek teljes egészében vagy részben átfedhetnek a felszínborítási felületekkel. Ezek mutatják meg, hogy az adott területen milyen tevékenység zajlik. A tevékenység felület-objektumok általában átfedhetik egymást, valamint átfedésben lehetnek az „egyéb" felület (OAF) objektumokkal is.

A listában szereplő minden objektum átfedésben van egy vagy több felszínborítás objektummal. A felületek átfedhetőségi szabályait egy xls fájl tartalmazza, amely szerves része a TRD-nek. Előfordulhatnak olyan helyzetek, amelyek kivételt képeznek az egymást átfedő felületekre vonatkozó általános szabály alól. Például néhány emberi tevékenységet jelölő objektum soha nincs átfedésben árapály zónával (BA040), más tevékenység felület objektum pedig pl. temető (AL030), soha nincs átfedésben vasúti teleppel (AN060).

A kiértékelendő objektumok a következők:

- Hulladéklerakó (AB000), erőmű (AD010), gyár (AC000), karám (AJ030), park (AK120), temető (AL030), tábor (AL105), országúti pihenőhely (AQ135), kikötő (BB005), ártér (BH090), irtás (EC060), repülőtér (GB005)…

Az **egyéb felület**szerű objektumokat kell az utolsó lépésben kiértékelni, ezek az objektumok átfedhetik egymást, valamint tevékenység és felszínborítás felület objektumokkal is. A listában szereplő objektumok mindig átfedésben vannak egy vagy több felszínborítási objektumokkal és/vagy tevékenység objektumokkal.

A kiértékelendő objektumok a következők:

- Ülepítő tó (AC030), stadion (AK160), épület (AL015), gabonasiló (AM020), stég (AK190), rom (AL200), hullámtörő (BB041), nádas (EC010), hangárelőtér (GB015)…

Az egyéb objektumok kiértékelése során a legtöbb gondot az épületek felvétele okoz a kiértékelőnek, ugyanis az épületek attribútumok alapján való kategorizálása nagyon nehéz. A munkát továbbra nehezíti az űrfelvételekről történő adatnyerés, ezért kellő figyelemmel és óvatossággal kell a kiértékelőnek kezelni az épületek attribútum értékeinek megválasztását, továbbá figyelnie kell az attribútum értékek összeférhetetlenségeire is. Például, nem lehet egy épületnek terméke, ha korábban beállítottuk hogy ez egy temetőépület.

Eddigi munkánk során nagyon sok kellemetlenségeket okozott számunkra cella szinten az attribútumok ellenőrzése és javítása, hiszen az épület objektum (AL015) az, amelyiknek a

legtöbb attribútumot kell tölteni, valamint ez az objektum rendelkezik a legnagyobb elemszámmal.

Az **épület** objektumcsoport kiértékelhető mind pontként, mind felületként, a geometriai területének nagyságától függ, hogy melyik objektumtípussal digitalizáljuk. Az épülethatárokat úgy kell létrehozni, hogy az épületekhez csatlakozó, 25m-nél kisebb „beugrásokat" vagy „kiszökelléseket" nem kell leképezni.

Ha az épület alakja meghatározó (pl. **L**-alakú), akkor egyes oldalak hosszától függetlenül kell kiértékelni. Amennyiben az épület fő körvonalain belül 25m x 25m-nél nagyobb lyukak találhatók, akkor ezek a területek lyukként ábrázolandók. Fontos, hogy a jellegzetes alakú épületek felületként kell kiértékelni, még akkor is, ha a területük nem éri el pontosan a TRD-ben meghatározott területhatár.

Az épületek kiértékelése megfelelő sűrűséggel végzendő, hogy helyes információt közvetítsenek a kiértékelt területről. A jellemző minta definíciója szerint a hasonló objektumok sűrű csoportjának legmeghatározóbb objektumainak kiválasztását és ábrázolását jelenti, az objektum tényleges helyét kell ábrázolni, nem pedig a „legjobb illeszkedés" szabályát kell követni az objektumok között.

A szelvény szintű kiértékelés legutolsó fázisában kell az előbbiekben még fel nem vett vonalas és pontszerű objektumokat kiértékelni.

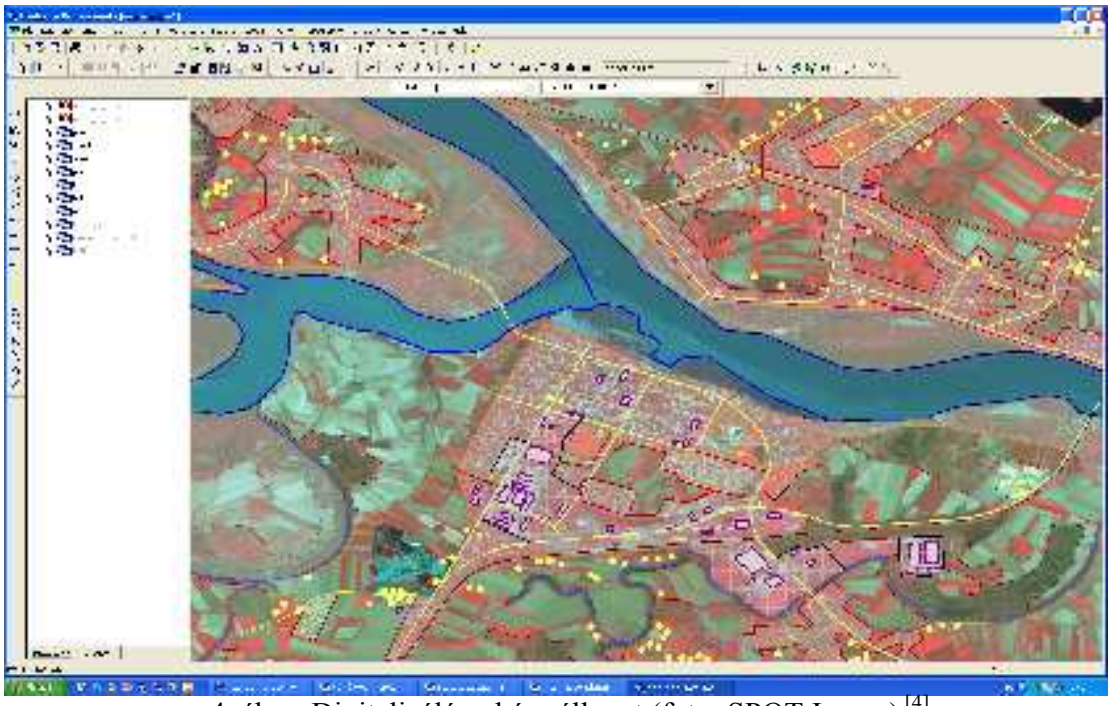
A kiértékelendő objektumok a következők:

- **Vonalas objektumok**:

  Szállítószalag (AF020), csővezeték (AQ113), nagyfeszültségű vezeték (AT030), telefon/távíró vezeték (AT060)…

- **Pontszerű objektumok**:

  Irányítótorony (AQ060), kút (AA050), daru (AF040), gyár (AC000), kémény (AF010), szélmalom (AJ050), beépített terület (AL020), emlékmű (AL130)…

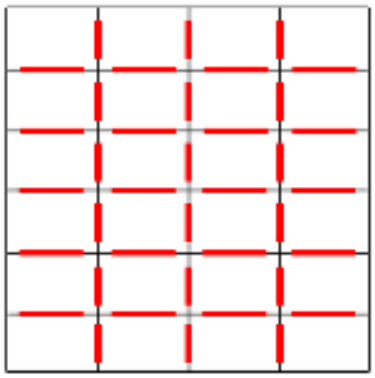


4. ábra: Digitalizálás - kész állapot (foto: SPOT Image) [4]

A csatlakoztatás során a szomszédos szelvény alegységek határán jelen lévő folytatólagos objektumok kerülnek egyesítésre (merge). Ügyelni kell az attribútumok helyességének meglétére, mely után az adott több „darabból” álló objektumot egyesíteni kell. Olyan esetben, ha adott objektum az alapanyag szerint folytatódik a szomszédos szelvényen, de az ott még nem került felvételre, akkor azt pótolni kell.

A csatlakoztatás a szelvények közötti éleken történik. A sorrend kötetlensége idő- és erőforrás kihasználtság szempontjából előnyös. Figyelni kell arra, hogy ha egy szelvény egy élén épp csatlakozás folyik, akkor egy időben ugyanazon a szelvényen más munka nem folyhat.

A csatlakoztatás ellenőrzése szintén élenként történik.



5. ábra: Szelvények csatlakoztatása [5]

## ÖSSZEFOGLALÁS

A Többnemzeti Térinformatikai Együttműködési Programban résztvevő országok szakembereinek meg kell felelniük a legszigorúbb szalmai elvárásoknak a téradatbázis elkészítése során. Az egységes Műszaki Referencia Dokumentum ellenére minden ország maga határozta meg kellett a saját adatnyerési, ellenőrzési és adatmigrációs technológiáját. A bemutatott interpretációs technológia a vezetésemmel kidolgozott adatnyerési sor, mely tapasztalatok bővülésével, az elvárások módosulásával folyamatosan változik, finomodik. A különböző országok eltérő szoftveres támogatást, más kiértékelési metodikát választottak, de végleges adataik ugyanannak a globális térinformatikai adatbázisnak a struktúráját, adatkapcsolatát, adatsűrűségét tartalmazzák. Az általunk kidolgozott adatnyerési eljárással már feldolgozásra került mintegy 35.000km$^2$ területet lefedő távérzékelési alapanyag.

## IRODALOMJEGYZÉK


[1] Ellenőri utasítás v2.0 2007.10.30. , 10-11.o ( Geodézia Zrt. belső dokumentum)

[2] MGCP Műszaki Referencia Dokumentum (Technical Reference Documentation -TRD) TRD2.0\DataContent\Extraction_Guide\MGCP Extraction Guide TRD2 v2.0 20070330.htm

[3] Operátori utasítás v1.4 2007.10.30. , 12-14.o (Geodézia Zrt. belső dokumentum)

[4] Operátori utasítás v1.4 2007.10.30. , 15.o (Geodézia Zrt. belső dokumentum)

[5] Operátori utasítás v1.4 2007.10.30. , 20.o (Geodézia Zrt. belső dokumentum)


## ÁBRAJEGYZÉK


[1] MGCP TRD2 v2.0 - Kiértékelési útmutató TRD2.0\DataContent\Extraction_Guide\MGCP Extraction Guide Features\MGCP EG AK030.htm

[2] MGCP TRD2 v2.0 -Attribútum katalógus TRD2.0\DataContent\Feature_Attribute_Catalogue\MGCP Feature Catalogue TRD2.0 20070328\htmlMGCPCatalogueBrowser_TRD2.0_20070328.html

[3] Brunbauer_Otto_MGCP.ppt http://www.geodezia.networldtrading.com/main.php?module=geo&bid=6&PHPSESSID=1772540c84480c8a9bdd8cca151f561d

[4] Munkaterület állapota Intergraph Co. GeoMedia Pro környezetben

[5] Ellenőri utasítás v2.0 2007.10.30. , 33.o (Geodézia Zrt. belső dokumentum)

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Farkas Imre**
Zrínyi Miklós Nemzetvédelmi Egyetem
farkas.imre@geodezia.hu

# TECHNOLÓGIAI MÉRFÖLDKÖVEK AZ MGCP TÉRADATBÁZIS ELŐÁLLÍTÁSA ÉS ELLENŐRZÉSE SORÁN

***Absztrakt***

*Az Többnemzeti Térinformatikai Együttműködési Programban Magyarország vállalásaként jelentkező mintegy 250.000 km$^2$ területet lefedő térinformatikai adatbázis elkészítése, a magyar térinformatikai szakmában példa nélküli kihívást jelent. Ez nem csak a körülbelül két és fél Magyarországnyi méretből, hanem az adatbázis részletességéből, az objektumtípusok és azok attribútumai között fennálló bonyolult kapcsolatrendszerből, a sok leíró adatból, valamint a projekt különféle dokumentumainak, szabályzatainak bonyolultságából is adódik. Az adatnyerésben és ellenőrzésben résztvevő cégek, a HM Térképészeti Kht-ban létrehozott MGCP Koordinációs Irodával az élen elkötelezték magukat az adatbázisok kifogástalan minőségű előállítása mellett. A célkitűzés azt az összetett követelményrendszert kielégítve, amelyet az MGCP, mint nemzetközi program megkövetel csak akkor érhető el, ha a különböző folyamatokat, technológiákat folyamatosan elemezzük, majd elegendő tapasztalatgyűjtés után a megfelelő fejlesztéseket, módosításokat megtesszük. Jelen cikkben, mint az adatnyerést végrehajtó Geodéziai és Térképészeti Zrt. műszaki vezetője az MGCP téradatbázis adat-előállítása, belső ellenőrzése, hibajavítása során tapasztalt jellemző hibákat, valamint nem a kielégítő hatékonysággal folyó műveleteket, és azok megoldásának, hatékonyabbá tételének mikéntjét ismertetem.*

*The preparation of a geoinformation database covering an area of 250.000 km2 within the Multinational Geospatial Co-production Program is an unprecedented challenge within the Hungarian geoinformatics profession. This is not just because of the area that roughly equals two and half times of the area of Hungary, but because the detail of the database, the complicacy of the object types and their attributes hierarchy, the amount of descriptive data, and due to the complicacy of the various regulations and documentations of the project. The companies involved in the data extraction and monitoring are determined to produce the database flawlessly, with the leading of the MGCP Co-ordination Office formed under the Defense Ministry Topographic Public Company This goal can only be achieved with the satisfaction of the complicated requirements, that the MGCP as an international program demands, if we constantly monitor the procedures and technologies, and if enough experience is accumulated the necessary improvements and changes are implemented. In this article I will present the typical errors, and procedures that are not working with the necessary*

*efficiency during the production and verification of the MGCP geodatabase, and the solutions to these problems, as the technical director of Geodéziai és Térképészeti Zrt. (Geodesic and Topographic Closed Incorporated Company)*

***Kulcsszavak:*** *Többnemzeti Térinformatikai Együttműködési Program, hatékonyság, adatnyerés, MGCP téradatbázis ~ Multinational Geospatial Co-production Program, efficiency, data extraction, MGCP geodatabase*

## RÖVIDÍTÉSEK

| | |
|---|---|
| AAF | Activity Area Feature (Tevékenység felület objektum) |
| AAFIF | Automated Airfield Facilities Information File (Automatikus légi bázis információs fájl) |
| DVOF | Digital Vertical Obstruction File (Függőleges adatok digitális nyilvántartása) |
| Geodézia Zrt. | Geodéziai és Térképészeti Zrt. |
| GeoNames | GeoNames DataBase (Földrajzi nevek adatbázisa) |
| GIPS | Geospatial Intelligence Production System |
| IGW | International Geospatial Warehouse (Nemzetközi Téradattár) |
| KI | Koordinációs Iroda (HM Térképészeti Kht. KI) |
| Komunálinfó Zrt. | Komunálinfó Információs Szolgáltató Zrt. |
| LAF | Landcover Area Feature (Felszínborítás felület objektum) |
| MDNYR | Munkafolyamat és Dokumentum Nyilvántartó Rendszer |
| MGCP | Multinational Geospatial Co-production Program (Többnemzeti Térinformatikai Együttműködési Program) |
| MH GEOSZ | Magyar Honvédség Geoinformációs Szolgálat |
| OAF | Other Area Feature (Egyéb felület objektum) |
| TRD | Technical Reference Documentation (Műszaki referencia dokument) |
| USA NGA | USA National Geospatial Intelligence Agency (USA Nemzeti Térképész Hírszerző Hivatal |
| VaCWG | VMap Level1 Coproduction Working Group |

## ELŐZMÉNYEK

A ’80-as évek végén indította el az Egyesült Államok Védelmi Térképész Szolgálata egy olyan digitális térinformatikai adatállomány létrehozását, amely a Föld teljes egészét lefedi. Az elképzelés, annak gigantikus volta miatt, csak több állam összefogása útján valósulhatott meg. A kezdeményezés, 1:250.000 méretarányban (VMap Level 1) mára megvalósult 18 NATO tagállam, valamint Ausztrália, és Új-Zéland együttműködésének eredményeképpen. Magyarország nem volt tagja a társulásnak, így a digitális állomány részeihez csak valamely résztvevővel kötött kétoldalú megállapodások útján juthat hozzá, annak felelősségi keretein belül.

Napjainkban jelentős az igény, mind a civil, mind a védelmi szféra irányából a pontos, nagy részletességű, megbízható információ tartalommal rendelkező térinformatikai termékek iránt. Rendelkezésünkre áll az a technológia, azon információhalmaz, amelyből felépíthetőek a térinformatikai adatbázisok. A nagytömegű téradatnyerés manapság legelterjedtebb, költség hatékony módja a távérzékelési anyagok (légi- és űrfelvételek) interpretációja és adatbázisba rendezése. A közelmúltban lezajlott társadalomi-, világpolitikai-, valamint gazdasági

változások jelentősen átformálták a földrajzi információs rendszerekkel szemben támasztott követelményeket. A katonai oldalon ezek a változások talán még jelentősebbek, mivel az információs- és informatikai technológia mai lehetőségit kihasználva a megnövekedett béketeremtő és békefenntartó műveleteket, valamint a globálissá váló terrorizmus elleni harcot, a védelmi térképész szolgálatok fokozottam kívánják térinformatikai adatbázisokkal támogatni.

A VaWCG-ban (a VMap Level1-et létrehozó országok munkacsoportja) vezérszerepet betöltő USA Nemzeti Térképész Hírszerző Hivatala (USA NGIA) tudatában volt, hogy a VMap Level1 (a Föld teljes egészének digitális térképe, téradatbázisa 1:250.000-es méretarányban) nem elégíti ki az USA, illetve a NATO haderejének szükségleteit. Ezen okból a VaWCG 2003. áprilisi, Vancouver-ben megtartott konferenciáján kezdeményezte, a NATO szövetséges, illetve a NATO tagállamokhoz „közel" álló védelmi térképész szolgálatok szélesebb körű együttműködése keretében egy, a megváltozott kritériumoknak megfelelő térinformatikai adatbázis megalkotását biztosító program, az MGCP (Multinational Geospatial Co-production Program / Többnemzeti Térinformatikai Együttműködési Program) létrehozását. A program célja a Föld, a társult nemzetek számára kiemelkedő jelentőséggel rendelkező részeiről, 1:50.000-es, illetve 1:100.000-es méretaránynak megfelelő adatsűrűségű, 1° x 1°-os földrajzi koordinátákkal határolt cellákból álló digitális térinformatikai adatbázis elkészítése. A programhoz, 26 másik országgal egyetemben Magyarország is csatlakozott.[1] A nemzetközi szerepvállalással hazánk az expedíciós tevékenységhez szükséges térinformatikai, térképészeti adatforráshoz fog hozzájutni, melynek mértéke minden résztvevő tekintetében a részvétel mértékétől függ. A Magyar Honvédség Geoinformációs Szolgálata mintegy 250.000 $km^2$ terület elkészítésére vállalt kötelezettséget.

## BEVEZETÉS

Magyarország kötelezettségvállalása, nemzetközi viszonylatban, mennyiségi értelemben nem kimagasló. A projektben vezető nemzeti tisztet betöltő országok (Amerikai Egyesült Államok, Ausztrália, Dánia, Franciaország, Kanada, Nagy-Britannia, Németország, Olaszország, Norvégia, Spanyolország, Svédország), minimum 400 darab cella előállításával járulnak hozzá a projekthez. Cserébe ők teljes hozzáférést kapnak a téradattárhoz. A társult nemzetek (Belgium, Bulgária, Csehország, Észtország, Finnország, Görögország, Hollandia, Lengyelország, Lettország, Litvánia, Portugália, Románia, Szlovákia, Törökország, Új-Zéland) hozzájárulásuk súlyozott mértéke szerint hívhatnak le adatokat.

Bár hazánk felajánlása alapján nincs az elsők között (ez sem gazdaságilag, sem katonai szempontból nem lenne indokolt), mindent megtesz, hogy nemzetközi elismerést vívjon ki magának. Egyrészt azzal, hogy az elsők között tölt fel adatot a Nemzetközi Téradattárba (IGW), másrészt azzal, hogy a feltöltött térinformatikai adatbázisok minőségileg kifogástalanok. A magyar programot szervező Koordinációs Iroda elszántan törekszik ezen akarat kivitelezésére, a programban résztvevő cégek (az adatnyerést végrehajtó Geodéziai és Térképészeti Zrt. és az ellenőrző Komunálinfó Információs Szolgáltató Zrt.) pedig elkötelezték magukat e szándék mellett. Minőségi termék a gondos előállítás mellett fokozott, és alapos ellenőrzés útján állítható elő. Fontos, hogy a résztvevő vállalkozások elemezzék a teszt cella előállítása során összegyűlt tapasztalatokat, majd a levont konzekvenciák után lépéseket tegyenek az adat-előállítási és az ellenőrzési technológia minél hatékonyabbá tétele céljából.

Jelen műben ismertetem mely pontokon és miért változott az adatnyerés, a belső ellenőrzés, valamint a hibajavítás technológiája korábbi elképzeléseim és a teszt cella elkészítésének módszeréhez képest.

# ADATBÁZIS LÉTREHOZÁS, TECHNOLÓGIAI MÉRFÖLDKÖVEK

**Humán- és eszköz erőforrás változások**

A leglátványosabb változások a projektben a humán- és eszközerőforrás tekintetében történtek, aminek a fő oka az adatelőállítás volumenének fokozódása.

Az adatnyerést végző cég az MGCP projektet hat fő operátor, és egy fő projektvezető bevonásával kezdte el. A projektvezetőre, mint műszaki vezetőre hárultak a belső ellenőrzési feladatok is. Hamarosan többszörösére növekedett ez a létszám, lépést tartva az egyidejűleg előállított cellák mennyiségével. Módosítani kellett a végrehajtók beosztások szerinti arányszámát is. A műszaki irányító, vezetői feladatai mellett, képtelen volt elvégezni a belső ellenőrzési munkálatokat. A teszt cella előállításának idején az adatnyerés szűk keresztmetszetét a belső ellenőrzés jelentette. Miközben több munkarésznyi adatbázis az ellenőrzés lefuttatására várt, az operátorok munka nélkül maradtak, hiszen nem kapták időben vissza a hibalistákat. Ma már leginkább négy, de maximum öt operátorra jut egy belső ellenőr. A program közvetlen irányítása is megváltozott. Az egyrészt a többszörösére nőtt létszámból, másrészt a sokszorosára gyarapodott munkamennyiségből adódó bonyolultabb, és felelősebb, nagyobb kihívást jelentő irányítói tevékenységet, egy döntéshelyzetben lévő vezető látja el a projekt élén, kinek a munkavégzését egy műszaki csoportvezető támogatja. Eddigi tapasztalataink szerint ebben a felállásban (a technológiában történt később ismertetett módosításokat alkalmazva) már zökkenőmentesen zajlik a termelés, egyik folyamat sem lassítja a munkavégzést.

A Geodézia Zrt. az adatbázisok előállítására az Intergraph Corporation fejlesztette GeoMedia Professional szoftvert, valamint az erre épülő Geospatial Intelligence Production System-t (GIPS) állította rendszerbe. A GeoMedia beváltotta a hozzá fűzött reményeket és alkalmasnak bizonyult az MGCP követelte bonyolult térinformatikai adatbázis megalkotására. A GeoMedia adatszerver technológiája támogatja a nyílt szabványokat, így hozzáférést biztosít az összes számottevő térbeli és CAD adatformátumhoz, és a piaci szabvány relációs adatbázisokhoz is, így a termékbe könnyen integrálhatóak az MGCP adatbázisokhoz a különböző segédadatbázisok, mint például a kötelezően beépítendő GeoNames (Földrajzi nevek adatbázisa), AAFIF (Automatikus légi bázis információs fájl), és DVOF (Függőleges adatok digitális nyilvántartása). A GeoMedia az elemző eszközök teljes skáláját biztosítja, mind az attribútum, mind a térbeli lekérdezéseket tekintve. Lehetőség van buffer zónák létrehozására, térbeli fedés vizsgálatra. Az unikális adatszerver technológiának köszönhetően könnyedén készíthetőek elemzések különböző adatformátumban tárolt adatok összehasonlításával is. A GeoMedia-nak egyedülálló képessége, hogy egy lépésben végrehajthatóak vele „what-if” típusú elemzések, a GeoMedia ugyanis képes egyidejűleg több elemzési műveletet elvégezni az egymásra épülő lekérdezések végeredményének azonnali, dinamikus megjelenítésével. Ez azt jelenti, hogy a folyamatban bármely ponton megváltozó adatok azonnal megváltoztatják a végeredményt is. Az online futó query-k segítségével, egyrészt az adat-előállítással egyidejűleg kontrolálható annak hibamentessége, másrészt a hibajavítással azonos időben ellenőrizhető annak sikeres volta. Elmondható, hogy a GeoMedia Professional teljes eszköztárral rendelkezik a belső ellenőrzések végrehajtásához.[2]

A teszt időszakban az első megalkotott cella térinformatikai adatbázisa, a GeoMedia natív formátumában, azaz mdb (Access) adatbázisban lett előállítva. Ez, amikor önmagában a teszt cella elkészítése volt folyamatban, kielégítő megoldás volt. A későbbiekben, amikor már több cella egyidejű létrehozása zajlott, nem biztosította a kellő hatékonyságot. Ezt belátva a az adatnyerést végrehajtók egy jelentősnek mondható beruházás után, áttértek Oracle adatbázis alkalmazására. Azon túl, hogy jelentősen csökkent a különböző adatbázison elvégzett

műveletek gépigénye, rengeteg nehezen, és költségesen kezelhető nyilvántartási és adattárolási problémát megoldott.

Sok gondot jelentett a cella egységességének biztosítása. Az okozta ezt, hogy az előállítás 1:50.000-es méretarányú topográfiai szelvényeknek megfelelő méretű területegységekben történt, majd miután a rész-adatbázisok minősége kielégítő volt, azok csatlakoztatásával állt elő a leadandó cella méretű adatállomány. A csatlakoztatott szelvények azonban nem voltak tökéletesen egységesek! A technológiai folyamat részletes elemzése után megállapítottam, hogy a probléma oka két dologban keresendő:

1. a távérzékelt alapanyagból történő adatnyerés, a fotóinterpretáció bizonyos mértékig szubjektív folyamat,
2. az 1:50.000-es méretaránynak megfelelő térképkészítés néhány objektumtípus esetében túlságosan nagyfokú szabadságot biztosít az operátoroknak.

Oracle-ben definiálhatóak különböző hozzáférési jogosultságok. Ezt kihasználva a termelés ma már úgy zajlik, hogy minden operátor a saját szelvényére vonatkozóan rendelkezik editálási joggal, míg a cella többi szelvényét mindenki csak olvasni tudja. Az operátorok kontrolálhatják a cella teljes egészét, így a végeredmény sokkal homogénebb. Az Oracle ugyanezen lehetőségét kihasználva, a szelvények csatlakoztatási folyamata (amikor a szelvényhatárra kifutó objektumokat egyesíteni kell), sokkal egyszerűbb és gyorsabb. A határon találkozó objektumok, egyrészt geometriailag már eleve egy pontban találkoznak (pl., ha az egyik szelvényben már ábrázolva van egy, a szelvényhatárra kifutó út, akkor a szomszéd szelvényt készítő operátor már a szelvény előállításakor ehhez csatlakozni fog, és fordítva), másrészt az objektumok attribútumai is megegyeznek.

Az Oracle adatbázis kezelő többek között tökéletes megoldást biztosít a projektben résztvevő kollégák munkájának értékelésére is. Viszonylag egyszerűen vizsgálható például, hogy adott időegység alatt mely operátor milyen mennyiségű adatbázist hozott létre, hatékonyan támogatva az esetleges premizálásokat, vagy retorziókat.

Oracle-t alkalmazva az archiválási fegyelem megsértéséből adódó károk sem jelentkeznek, mert nem az operátorokra van bízva, hogy az adatállományokat a megfelelően strukturált tárhelyre mentsék, vagy hogy az esetleges javításokat az aktuális, ne pedig valamely korábbi fájlban eszközöljék.

**Az adatnyerés, a belső ellenőrzés, és a hibajavítás technológiájának változásai**

Az MGCP során 174 különböző objektumtípus felhasználásával jellemezhetjük a térképezendő tájat. Minden objektumtípus leíró adatokkal rendelkezik, melyek számossága objektumfüggő, de a 16 szupertípuson (olyan attribútum, melyet minden objektumtípus tartalmaz) felül, a néhánytól a több tízig terjed. [3] Az objektumtípusok felvételének, az attribútumok kitöltésének, a különböző segédadatbázisok felhasználásának szabályait a Technical Reference Documentation, röviden a TRD tartalmazza. A szabályzatban az objektumtípusok, és azok attribútumai között egy rendkívül bonyolult összefüggésrendszer van lefektetve.

Azon hibák, melyek a szabályzat hiányosságaiból, annak félreértelmezéséből, vagy esetleg nem kellő mélységű ismeretéből adódtak, a Koordinációs Iroda hathatós segítségével, először gyakori konzultációkkal, majd egy fórum rendszerbe állítása után, az azon zajló folyamatos kommunikációval megoldódtak.

Az adatnyerés, belső ellenőrzés, hibajavítás technológiája is gyökeres átalakuláson ment keresztül. Gyakorlatilag csak a munkaszervezés azon része maradt változatlanul, hogy a kiértékelés alapvetően a cella szelvényegységeiben történik, majd a cella e részadatbázisok egyesítése útján áll elő. A projekt elején a belső ellenőrzés az operátorok által késznek tekintett szelvényeken futott le. A belső ellenőrzés által felderített hibák javítását követően az adatbázis leadásra került az ellenőrzést végző cégnek, hogy az elvégezhesse a külső

ellenőrzési feladatokat. A hibák javításának minőségét, illetve eredményességét a külső ellenőr cég visszaellenőrizte egészen addig, amíg az összes szabálytalanság helyesbítve nem lett. [4] GAIT (az MGCP-ben nemzetközileg használt ellenőrző, konzisztencia vizsgáló szoftver) vizsgálat csak cellaszinten zajlott. Sajnálatos módon a feladat világviszonylatban való újszerűségét jól szemlélteti, hogy ez a szoftver a folyamatos korrigálások ellenére sem fut hibamentesen, így nem valós hibák ezreit generálja egy-egy futtatás során. Az Ellenőr a hibajavítást azzal támogatta (és támogatja GAIT futtatás esetén a mai napig), hogy a GAIT hibalistát minősíti, a nem valós hibákat kiszűri. A két cég közötti hibajavítás-visszaellenőrzés addig folytatódik, amíg a GAIT vizsgálat eredménye már csak nem valós hibákat tartalmaz.

Ez a metódus az MGCP szigorú követelményrendszerének nem felelt meg. A különböző ellenőrzési lépcsők nagy számú hibát tártak fel, igaz ezt részben indokolta a projekt újszerűsége, valamint a kezdeti tapasztalatlanság is. A belső ellenőrzés kapacitása egyértelműen nem volt elegendő feladatai megfelelő szintű ellátásához. A helyzet különösen akkor vált kritikussá, amikor a belső ellenőrzésre leadott szelvények mellett visszaellenőrzésre vártak a javított fájlok, valamint felügyelni kellett a külső ellenőr cég által jelzett hibák kijavításának eredményességét is. A belső ellenőrzés túlterheltségének folyományaként a tervezettnél több hibával terhelten kerültek adatállományok átadásra az ellenőrzést végző Komunálinfó Zrt-nek. A javítások minőségi hiányosságai következtében (az újra és újra történő visszaellenőrzések miatt) a külső ellenőr cég is kapacitása határán működött. A viszonylagos magas hibaszámnak tagadhatatlanul az is oka volt, hogy a pályáztatás elhúzódása következtében a külső ellenőrzés akkor kezdődött el, amikor az adatnyerés már csaknem lezárult, ergó a Geodézia Zrt. nem rendelkezett megfelelő visszajelzésekkel azokról a típushibákról, TRD értelmezési problémákról, melyeket egyébként egyszerűen orvosolhatott volna. Mire ezek világossá váltak, ezeket a hibákat majdhogynem a teljes adatállomány hordozta.

A technológián módosítani kellett, mielőtt a résztvevők a teszt cella lezárása után belevágtak volna a nagytömegű termelésbe. A mostani technológia jóval strukturáltabb (1. sz. kép). Az egy fő belső ellenőr által kontrolált operátorok számának csökkenéséről már volt szó. Ez fontos lépés volt a belső ellenőrzés hatékonyabbá tétele érdekében.

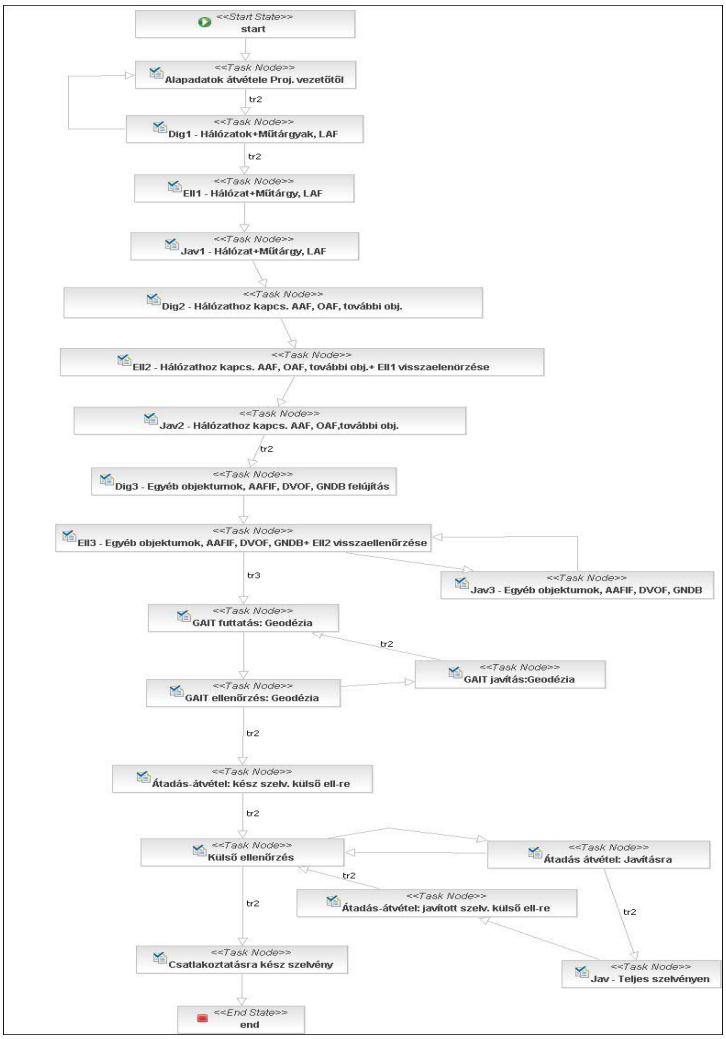
Kiemelkedő jelentőséggel bír továbbá, hogy az operátorok az adatnyerést nem egy lépésben végzik, saját maguk meghatározva a különböző objektumok felvételének sorrendjét. A kiértékelést objektumosztályokra bontottuk, meghatározva ezzel a digitalizálás egymásutániságát is. Az első adat-előállítási lépcsőben az út- vasút-, és vízhálózat, valamint az ezekhez szervesen kapcsolódó objektumok, majd a felszínborítást (LAF-ok) alkotó felületek kerülnek felvételre. A különböző hálózatok már jó alapot adnak a felszínborítás létrehozásához, a felszínborítással együtt, pedig már egyszerűbben felépíthető a későbbiekben minden egyéb objektumtípus.[5] A kiértékelést egy belső ellenőrzés, majd egy hibajavítás követi. A második adat-előállítási ütemben kerülnek felvételre a tevékenység felületek (AAF-ok), az egyéb felületek (OAF-ok), majd ezek után az összes maradék vonalas és pontszerű elem. A most következő belső ellenőrzés során visszaellenőrzésre kerülnek az előző hibák javításai, valamint az újonnan felvett elemek. Az adat-előállítás harmadik fázisában az AAFIF, DVOF, és GNDB bedolgozása történik. Ismételt belső ellenőrzés után hibajavítás, majd visszaellenőrzés folyik.

Jelentősen változott a technológia abból a szempontból is, hogy a nagyszámú GAIT hibák csökkentése érdekében a tesztcellával ellentétben, igaz csak csökkentett ellenőrzési módban, de fut egy GAIT ellenőrzés is. Annak érdekében, hogy ez az MGCP KI munkaidején kívül, vagy esetleges egyéb elfoglaltságai mellett is megtörténhessen, a Koordinációs Iroda megoldotta, egy *ftp* szerver segítségével, hogy az oda feltöltött fájlokon a GAIT lefusson, majd a hibalista automatikusan feltöltésre kerüljön az említet *ftp* szerver egy másik

mappájába. Így a termelés folyamatossága biztosított. A hibalista elbírálása utáni javítás után kerül csak átadásra a részadatbázis a külső ellenőr cégnek.

Az adatnyerés, belső ellenőrzés, hibajavítás minőségének javítása érdekében rendszerbe állítottunk néhány olyan lekérdezést, melyek folyamatosan futnak a felsorolt munkafázisok alatt. Ezzel a lépéssel elértük, hogy az elkövetett hibák egy részére már azok keletkezésének idejében fény derül.

A csatlakoztatási, és cellaszintű folyamatok nem változtak ilyen jelentős mértékben.




1.sz. ábra: Az MGCP szelvényszintű technológiájának sémája[6]

Fokozottan ügyelnünk kell viszont a külső ellenőr cég hibalistáinak kezelésére. Nem megengedhetőek azok a többletmunkák, illetve az ezekből adódó késések, melyeket a hibalisták nem hibamentes bedolgozása jelent. Ez a presztízsveszteségen túl mindenekelőtt időveszteséget, másodsorban Komunálinfó Zrt. fölösleges terhelését okozza, ami abból adódik, hogy ugyanazon területre eső adatbázison több visszaellenőrzést is el kell végezniük.

## ÖSSZEGZÉS

A Geodéziai és Térképészeti Zrt. fontos lépéseket tett meg, jelentős beruházások és technológia változtatások árán az ugrásszerű minőségjavítás, és gördülékenyebb termék-előállítás érdekében. Nem szabad ezzel megelégednünk. A változó szabályzatokat

folyamatosan figyelemmel kell kísérnünk, a változások miatt szükséges lépéseket meg kell tenni állandóan aktualizálva módszereinket. Meg kell találnunk a cellánként, vagy területenként változó alapanyagok értelmezésének, kezelésének leghatékonyabb módját. Munkatársaink légifénykép, illetve űrfelvétel értelmezési képességét folyamatosan fejlesztenünk kell, különös tekintettel arra a tényre, hogy a magyar szakmai életben megszokott Közép-európai területektől merőben eltérő jellegű területeken is dolgozni fogunk.

## IRODALOMJEGYZÉK


[1] Szabó Gyula: A Többnemzetiségi Térinformációs Együttműködési Program szerepe és feladatai egy egységes térinformációs világrendszer létrehozásában http://www.otk.hu/cd05/3szek/Szab%C3%B3%20Gyula.htm

[2] Tekiré Kft.: GeoMedia Professional Oktatási Segédanyag (v.1.2 2007.08.22.) 8-13 o.

[3] MGCP TRD2 v2.0 (Multinational Geospatial Coproduction Program Technical Reference Document) (2007.04.25.) - Kiértékelési útmutató TRD2.0\DataContent\Extraction_Guide\MGCP Extraction Guide Features\MGCP EG AK030.htm

[4] Ellenőri utasítás (v2.0 2007.10.30.) , 24-32.o ( Geodézia Zrt. belső dokumentum)

[5] MGCP Operátori Utasítás (v2.3, 2007.10.30.) - Szelvényszintű folyamatok, adatnyerés, 12-15. o. (Geodézia Zrt. belső dokumentum)

[6] Munkafolyamat és Dokumentum Nyilvántartó Rendszer (2008.03.20.) (HM Térképészeti Kht. MGCP KI belső dokumentum)

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Munk Sándor**
Zrínyi Miklós Nemzetvédelmi Egyetem
munk.sandor@zmne.hu

# KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁKHOZ KAPCSOLÓDÓ, SAJÁTOS KATONAI (VÉDELMI SZFÉRABELI) KÉPESSÉGEKET IGÉNYLŐ FELADATOK

***Absztrakt***

*Az információs szolgáltatásokat nyújtó és más, hagyományos infrastruktúráknak is hátteréül szolgáló információs infrastruktúrák biztonságának szerepe napjainkban folyamatosan növekszik. A kritikus információs infrastruktúrák védelme a kritikus infrastruktúra védelem egyik alapvető összetevőjévé vált. Mivel a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, a katonai, illetve védelmi szféra – saját kritikus infrastruktúrái védelmén túl – sajátos képességeire támaszkodva bővebb feladatokkal is rendelkezik. Jelen publikáció elemzi a sajátos képességek iránti igény okait és rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos katonai (védelmi szférabeli) képességeket.*

*Role of the security of information infrastructures providing information services, and support for other kinds of traditional infrastructures, in our days continuously grows. Protection of critical information infrastructures became one of the basic components of critical infrastructure protection. Since security of critical infrastructures is a basic component of national security, military, and defense sphere – beyond their duties regarding protection of their own critical infrastructures – based on their special capabilities, have additional tasks, and responsibilities. This publication analyses the roots of the demands for special capabilities, and describes special military (defense) capabilities, necessary for critical information infrastructure protection.*

***Kulcsszavak**: kritikus információs infrastruktúra védelem, katonai/védelmi képességek, informatikai felderítés, informatikai ellentevékenység, informatikai bűnügyi eljárások ~ critical information infrastructure protection, military/defence capabilities, cyber intelligence, cyber counteractivities, cyber forensics.*

# BEVEZETÉS

A távközlés és az Internet forradalma az emberek előtt az együttműködés, az összekapcsolódás és a különböző szolgáltatások igénybevételének rendkívüli távlatait nyitotta meg. A világ társadalmai ma már egyre növekvő mértékben függnek a tágabb értelemben vett informatika eszközeitől és szolgáltatásaitól, az információs technológiáktól. Ez a növekvő függőség ok-okozati módon vonta maga után az információs szolgáltatásokat nyújtó és más, hagyományos infrastruktúráknak is hátteréül szolgáló információs infrastruktúrák biztonságának megnövekvő szerepét. A kritikus információs infrastruktúrák védelme a kritikus infrastruktúra védelem egyik alapvető összetevőjévé vált.

A kritikus infrastruktúra általános értelemben mindazon infrastruktúrák (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége), melyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár. A kritikus információs infrastruktúra pedig információs tevékenységeket támogató rendszerek, eszközök olyan összessége, amely önmagában kritikus infrastruktúra, vagy lényeges szerepet játszik más kritikus infrastruktúrák működésében. A kritikus információs infrastruktúra fogalma értelmezhető nemzeti, védelmi, illetve regionális és szervezeti keretek között is.

A nemzeti kritikus infrastruktúrák és ezen belül a kritikus információs infrastruktúrák védelme jellemzően többszereplős feladatrendszer. Napjainkban a kritikus információs infrastruktúrák jelentős része – piacgazdaságra épülő államokban mintegy 80-90%-uk – az adott államtól teljes egészében, vagy részben független magánvállalkozások kezelésében van. Így a védelem megvalósításában egyaránt érintettek a kormányzati szervek és intézmények, az egyes infrastruktúrák tulajdonosai és üzemeltetői, sőt az informatikai ipar szereplői, bizonyos vonatkozásokban pedig még az információs szolgáltatásokat igénybevevő felhasználók is.

Bár az ezzel kapcsolatos vélemények esetenként eltérőek, véleményem szerint a fogalom alapvető elemeiből kiindulva a nemzeti kritikus információs infrastruktúrának mindenképpen részét képezi az adott állam védelmi és ezen belül katonai kritikus információs infrastruktúrája is. Ennek megfelelően a katonai, illetve a védelmi szféra szervezetei saját infrastruktúrájuk védelméhez kapcsolódóan szerepet játszanak a nemzeti kritikus információs infrastruktúrák védelmében.

Néhány megállapításra alapozva – mint azt egy korábbi publikációmban [1] már összegeztem – előzetes hipotézisként az is megfogalmazható, hogy a katonai, illetve védelmi szféra az előzőekben megfogalmazottnál bővebb feladatokkal rendelkezik, jelentősebb szerepet játszik a kritikus információs infrastruktúra védelemben. Az első megállapítás azt hangsúlyozza, hogy a kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, így megvalósításában érintett (lehet) a katonai, a rendvédelmi, a katasztrófavédelmi és nemzetbiztonsági szakterület is. A második – nemzetközi tapasztalatokra épülő – megállapítás szerint a kritikus infrastruktúrákhoz hasonló, összetett rendszerek informatikai védelmében leginkább a többnemzeti műveletekben résztvevő katonai erőknek vannak tapasztalatai. Végül a harmadik megállapítás szerint a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, a támadók elleni fellépés, de legalábbis e feladatok nagyobb része és egészének koordinációja a védelmi szféra feladata.

Mindezek alapján jelen publikáció alapvető célja a kritikus – elsősorban nemzeti – információs infrastruktúrák védelme sajátos katonai, illetve más védelmi szférabeli képességeket igénylő feladatainak feltárása, elemzése. Ennek érdekében:

- elemzi a sajátos képességek iránti igények alapvető típusait;

- rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos katonai képességeket és az ezekkel szemben támasztott követelményeket;
- rendszerezi, meghatározza a kritikus információs infrastruktúrák védelméhez szükséges sajátos más, védelmi szférabeli képességeket és az ezekkel szemben támasztott követelményeket.

## SAJÁTOS KÉPESSÉGEK IRÁNTI IGÉNYEK OKAI

A **kritikus infrastruktúra védelem feladatrendszere** a szakirodalomban, a vonatkozó szabályozókban és dokumentumokban különbözőféleképpen jelenik meg. A feladatrendszer leírására általában a feladatok jellegére épülő, jellemzően a biztonságot megsértő eseményhez viszonyított időrendet is tükröző osztályozást használnak. Az egyes feladatcsoportok – a kritikus infrastruktúra védelem lényegéből következően – jelentős hasonlóságokat mutatnak a válságkezelés, szükséghelyzet-kezelés, incidens-kezelés, illetve kockázatkezelés feladatrendszereinek összetevőivel.

Egy ITU kutatási anyag [2, 1-4.o.] a kritikus információs infrastruktúra védelem lényegi feladatait a következő négy csoportba sorolja: megelőzés és korai figyelmeztetés, észlelés, reagálás és válságkezelés . Ezeket az anyag a kritikus információs infrastruktúra védelem négy "tartóoszlopának" nevezi. Az első feladatcsoport alapvető rendeltetése, hogy a védekezésben érintettek fel legyenek készülve a bekövetkező incidensekre, megkapják az időbeni figyelmeztetést a várható fenyegetésekről. A második csoport lényege az új fenyegetések minél gyorsabb felfedezése. Ebbe az új technikai fenyegetési formák mellett bele kell érteni az általános kockázati helyzet változásait is (pld. új bűnözői, vagy terrorista csoportok). A reagálás magában foglalja a működés, szolgáltatás megszakadása okainak azonosítását és megszüntetését. Az incidensre adott válasz szintén nem csak technikai, létfontosságú része lehet a támadók megbüntetése. Ebbe a csoportba tartozik az incidens elemzése és a tapasztalatok közreadása is. Végül a válságkezelés feladatcsoportba az incidens bekövetkezését követő döntéshozatali, irányítási és koordinációs feladatok tartoznak.

Az Európai Kritikus Infrastruktúra Védelmi Program a védelem feladataira vonatkozó elképzeléseket a fogalomjegyzékben körvonalazza. [3, 19-23.o.] A kritikus infrastruktúra védelem feladatai a fogalom leírásában öt csoportot alkotnak: felkészülés, védekezés, mérséklés, reagálás és helyreállítás. Külön meghatározás írja le a megelőzés, a reagálás tartalmát. A megelőzés rendeltetése a veszélyeztetésnek kitettség, a veszélyeztetés bekövetkezési valószínűsége, illetve a bekövetkezés esetén fellépő károk csökkentése. A reagálás fogalma a dokumentum szerint a biztonságot megsértő esemény rövidtávú közvetlen hatásaihoz kapcsolódik.

Az Egyesült Államok Védelmi Minisztériuma első kritikus infrastruktúra védelmi tervében [4] a tevékenységeket hat fázisba csoportosítja: elemzés és értékelés, javítás/kiküszöbölés, figyelés és tájékoztatás, mérséklés, reagálás és helyreállítás/újraszervezés. A dokumentum következő változata [5] már nem tartalmaz ilyen felsorolást, de az egyes összetevők ebben is megjelennek. A javítás/kiküszöbölés a felismert sebezhetőségek (gyengeségek, hiányosságok) megszüntetésére irányuló tevékenységeket foglalja magában. A figyelés és tájékoztatás a felderítéstől származó figyelmeztetések összegyűjtése, szintetizálása és elosztása. A mérséklés a figyelmeztetések, vagy az incidens bekövetkezése után a potenciális káros hatások csökkentésére irányuló tevékenységek összessége. A dokumentum a kritikus infrastruktúra védelmet összekapcsolja a műveletbiztonság olyan más területeivel, mint: az erők megóvása; terrorizmus elleni harc; információvédelem; műveletfolytonosság; vegyi, biológiai, radiológiai, nukleáris és nagy erejű robbanás elleni védelem.

Összességében tehát megállapítható, hogy a kritikus információs infrastruktúra védelem főbb feladatcsoportjai közé a következőket sorolhatjuk: elemzés és értékelés (fenyegetések és

sebezhetőségek); kiküszöbölés (sebezhetőségek); felkészülés és felkészítés; figyelés, észlelés és tájékoztatás; mérséklés; reagálás; és helyreállítás.

A **kritikus információs infrastruktúra védelem szereplői** széleskörű áttekintését adja a 2002 óta kétévente megjelenő Nemzetközi Kritikus Információs Infrastruktúra Védelmi Kézikönyv. A kézikönyv 2006-os kiadása [6] már 20 ország és 6 nemzetközi szervezet kritikus információs infrastruktúra védelmi politikáját és megvalósításának helyzetét összegzi. A következőkben a kézikönyv országonkénti 'Szervezeti áttekintés' pontjaiban foglaltak alapján tekintjük át röviden és rendszerezzük a védelemben érintett szereplőket.

A kézikönyvben megfogalmazott összegzés [6, Vol I. 394-398.o.] alapján megállapítható, hogy a különböző országokban a kritikus információs infrastruktúra védelem feladatai megvalósításának szervezetrendszere rendkívül heterogén, számos szervezetet, intézményt, hatóságot foglal magában. A kormányzati szereplők között vannak minisztériumok, ágazatközi szervezetek, minisztériumokon belüli szervezeti egységek (hivatalok, bizottságok) és minisztériumok alárendeltségébe tartozó szervezetek. Az érintett szereplők között szinte minden országban találkozunk a köz- és magánszféra partnerségére épülő szervezetekkel is. Az érintett szereplők körét, helyét és feladatrendszerét különböző tényezők befolyásolják: hagyományok, történelmi tapasztalatok, az erőforrások elosztása, valamint az aktuális fenyegetésekkel kapcsolatos politikai elképzelések.

A különböző országoknál a tágabb értelemben vett védelmi szféra szervezetei közül találkozhatunk katonai (honvédelmi), rendvédelmi, katasztrófavédelmi és nemzetbiztonsági szereplőkkel. Ezek köre és jelentősége alapvetően az információs infrastruktúra szerepére vonatkozó elképzelésektől függ.

A kritikus információs infrastruktúra védelemmel kapcsolatos alapvető megközelítések négy csoportba sorolhatóak. [6. Vol II. 60-62.o.] Az első szerint ez egy technikai szintű, információ-, illetve informatikai biztonsági kérdés kiemelt tekintettel az Internet-biztonságra. A második megközelítés lényege az e-gazdasághoz kapcsolódó működésfolytonossági (üzletmenet-folytonossági) szemlélet. A harmadik a rendvédelmi megközelítés, amely az informatikai bűnözés elleni tevékenységre összpontosít. Végül a negyedik a kritikus információs infrastruktúra védelmet nemzetbiztonsági megközelítésben, annak lényeges összetevőjeként szemléli.

Az első két elképzelést valló országok esetében az információs infrastruktúra alapvetően az információs társadalom, az információgazdaság, az információs szolgáltatások bázisa, így a kritikus információs infrastruktúra védelem alapvető felelősei az e-kormányzatért, valamint az informatikáért és távközlésért felelős szervezetek, illetve a katasztrófavédelmi (veszélyhelyzet-kezelési) szervezetek. Többségében ezen országok esetében is megemlítésre kerül a rendőrség, mint az informatikai bűnözés elleni harc megvalósítója, azonban ez erőteljesebben a harmadik megközelítés esetében jelenik meg. Az informatikai bűnözésnek azonban minden esetben csak egy elemét alkotják a kritikus információs infrastruktúrák elleni támadások.

A védelmi szféra szervezeteinek jelentősebb szerep azon országokban jut, amelyek megfogalmazzák az információs infrastruktúrák nemzetbiztonsági jelentőségét és ehhez kapcsolódóan reális veszélynek tartják a terrorfenyegetettséget, sőt egyes esetekben már az államilag támogatott/megvalósított információs támadásokat. Ezen országokban így kiemelt szerepet kapnak katonai szervezetek és a nemzetbiztonsági szolgálatok is.

A **sajátos – adott szereplőhöz kötött – képességek iránti igények** mögött általános értelemben több különböző indok is állhat, amelyeket jelen publikációban két nagy csoportba sorolunk. Az első csoportot azok az esetek alkotják, amelyekben a kritikus információs infrastruktúra védelemhez szükséges, vagy ahhoz nagymértékben hasonló képességek sajátos eszköz- és eljárásrendszere, valamint az ezek alkalmazására való felkészültség egy adott

szereplőhöz kapcsolódik. A második csoportba pedig azok az esetek tartoznak, amikor egy adott tevékenység végrehajtását, illetve végrehajtóját jogszabályok írják elő, korlátozzák.

A feladatvégrehajtáshoz szükséges sajátos eszköz- és eljárásrendszer, illetve alkalmazási képesség önmagában nem feltétlenül jelenti azt, hogy az ezekkel rendelkező – például katonai, vagy védelmi szférabeli – szereplő mellett ugyanilyen képesség más, új szereplőknél nem építhető ki, de ez utóbbi legalábbis az erőforrások gazdaságos felhasználása szempontjából mindenképpen megfontolásra érdemes. Egy új képesség kialakítása az állami – és benne a katonai, védelmi – szférában alapvetően központi akarat alapján történik, a civil szférában pedig a törvények határai között különböző (gazdasági, stb.) szempontok alapján szabadon. A sajátos katonai, védelmi képességek nagyobb csoportjának egy alcsoportját alkotják azok a képességek is, amelyek hasonló – esetünkben civil (állami és magán-) – képességek szükséghelyzetben történő kiegészítésére/megerősítésére, kiváltására, ideiglenes helyettesítésére irányulnak.

A jogszabályok által korlátozott ('állami monopóliumként' kezelt) tevékenységekre irányuló képességek esetében nincs mód ezek más forrásokból történő helyettesítésére, sőt ezen tevékenységek más szereplők által történő megvalósítása egyenesen illegális. Ebbe a csoportba számos – például nemzetbiztonsági, bűnüldözési, stb. – tevékenység tartozik. Az ebbe a csoportba sorolható általános feladatköröknek a kritikus információs infrastruktúrák védelme során szükséges sajátos, a tömegkommunikációban informatikai, számítógépes, vagy hálózati minősítő jelzőkkel ellátott változatai (például 'számítógépes törvényszéki szakértés ) napjainkban is még csak kialakulóban vannak.

A kritikus információs infrastruktúrák védelme az információs társadalom kiépülésével, az információs szolgáltatások széleskörű elterjedésével és a tágabb értelemben vett informatika eszközrendszerének egyre kiterjedtebb alkalmazásával párhuzamosan egyre nagyobb jelentőségre tesz szert. Ezzel egyidőben fokozatosan bővülő mértékben fognak jelentkezni a különböző sajátos védelmi képességekkel szembeni igények, követelmények is. Mindez minden bizonnyal vonatkozni fog a sajátos katonai és más védelmi szférabeli képességekre is, amelynek egyes jeleivel már ma is találkozhatunk.

A következőkben sorra vesszük a kritikus információs infrastruktúra védelem főbb feladatcsoportjait és külön-külön megvizsgáljuk, hogy ezek közül melyekben van (lehet) szükség speciális katonai, illetve tágabb értelemben vett védelmi szférabeli képességekre.

## SAJÁTOS VÉDELMI KÉPESSÉGEKET IGÉNYLŐ FELADATOK

Egy állam haderejének a kritikus infrastruktúra védelemmel és ezen belül a kritikus információs infrastruktúra védelemmel kapcsolatos feladatai, valamint a feladatok végrehajtásához szükséges képességek általános értelemben három nagy csoportba sorolhatóak. Az első csoportot a haderő saját kezelésében lévő kritikus (információs) infrastruktúrák védelmére irányuló feladatok alkotják. A második – az előzővel szoros kapcsolatban álló – csoportba a haderő számára közvetlenül, vagy a saját kritikus infrastruktúráján keresztül kritikus szolgáltatást nyújtó, más szereplők, szervezetek kezelésében álló infrastruktúra összetevőkkel kapcsolatos tevékenységek tartoznak. Végül a harmadik csoport az adott állam más kritikus infrastruktúrái védelmére irányuló, támogató feladatokat foglalja magában. Jelen publikációban a továbbiakban alapvetően ez utóbbi csoport feladataira összpontosítunk.

A **kritikus információs infrastruktúrákat fenyegető támadások** általános értelemben lehetnek anyagi (fizikai), információs, vagy szellemi jellegűek. Az első csoportba többek között a következőek tartoznak: fizikai behatás; elektromágneses, vagy radioaktív besugárzás; illetve anyagi (fizikai) jellemzők megfigyelése, érzékelése, lehallgatása. A második csoportba pedig azokat a fenyegetéseket sorolhatjuk, amelyek az adott rendszer által értelmezhető,

feldolgozható információt juttatnak be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosítanak, törölnek, vagy szereznek, figyelnek meg az adott (hagyományos információfeldolgozási, vagy informatikai) rendszer saját folyamatai, résztevékenységei útján. Végül a harmadik – a továbbiakban részletesebben nem tárgyalt – csoportot az emberi tudatban érvényesülő szellemi kölcsönhatások (pld. megtévesztő propaganda, pánik-, vagy félelemkeltés, stb.) alkotják.

A kritikus információs infrastruktúrákat érintő veszélyek csoportosíthatóak forrásaik, kiváltóik szerint is: megkülönböztethetünk tudatos szereplőkhöz köthető fenyegetéseket, valamint gondatlanságból származó és természeti, vagy ipari eredetű veszélyeztetéseket. A katonai és rendvédelmi szervezeteknek mindenekelőtt az első csoport esetében lehetnek feladatai, a megelőzés a második csoport esetében alapvetően a katasztrófavédelem feladata.

A **kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplők**, egyben az adott állam (esetleg együttműködő államok szervezete) biztonságát is fenyegetik. Ezek között napjaink megváltozott biztonságpolitikai környezetében a hagyományos nemzetállami szereplők mellett egyre nagyobb szerephez jutnak az úgynevezett nem állami szereplők: államon belüli, az adott állammal szemben álló szereplők (pld. nemzeti, etnikai, vallási, vagy törzsi alapon szerveződő politikai-katonai szervezetek, vagy bűnszervezetek); valamint terrorista szervezetek, csoportok és nemzetközi bűnszövetkezetek. [7]

A biztonságpolitikai szereplők körében bekövetkezett változásoknál is jelentősebb a biztonsági kockázatok körének a biztonság átfogó értelmezéséhez kapcsolódó kibővülése. Az új típusú – köztük pld. információs jellegű – veszélyek, kockázatok és fenyegetések elméleti szinten számos dokumentumban megfogalmazásra kerültek, azonban az államok túlnyomó többségében teljeskörűen még ma sem érvényesül az újszerű biztonságfelfogás és nem alakult ki az ehhez kapcsolódó rendszerszemléletű felelősségi rend és cselekvési programok.

A Magyar Köztársaság esetében Szenes Zoltán megállapítása szerint is "a külső biztonság kezelése többé-kevésbé a helyén van (Külügyminisztérium, Honvédelmi Minisztérium, Miniszterelnöki Hivatal), a belső biztonság komplex értelmezése és gyakorlata kezd kialakulni (Belügyminisztérium[1]), a biztonság 'puha' aspektusai (gazdasági biztonság, információs biztonság stb.) teljesen esetlegesen jelennek meg az elméleti és gyakorlati szférában." [7]

Egy adott szervezet esetében az informatikai védelem tevékenységrendszere mintegy a szervezet 'határain belül' valósul meg. Egy szervezetnek ugyanis általában jogszerűen nincs lehetősége és többnyire nincs is megfelelő képessége közvetlen (pld. képességcsökkentést eredményező, elrettentő) ráhatást gyakorolni a fenyegetést megvalósító szereplőkre és korlátozottak a fenyegető szereplőkről történő információszerzésre irányuló lehetőségek is. Ezzel szemben a kritikus infrastruktúrák védelme egy adott állam biztonsága megőrzésének része, így megvalósítása során felhasználhatóak, sőt felhasználandóak az állam jogilag és materiálisan rendelkezésre álló képességei, lehetőségei.

Jelenleg jellemzően nincs egységesen elfogadott elgondolás az új típusú fenyegetésekhez kapcsolódó egyes feladatok különböző szervezetekhez rendelésére. **A védelmi szféra különböző szervezeteinek hagyományos rendeltetése** szerinti feladatmegosztás az információs színtéren nem minden esetben és általában csak kiegészítő értelmezésekkel, megfontolásokkal valósítható meg. Tekintsük át először kivonatosan a védelmi szféra főbb összetevői feladatainak jelenleg érvényben lévő törvényi szabályozását.

A katonai erő feladata az adott állam függetlenségének, területének, légterének, lakosságának és anyagi javainak külső támadással szembeni fegyveres védelme [8, 70.§. a)]. A rendőrség feladata a közbiztonság és a közrend védelme, valamint az államhatár őrzése, a határforgalom ellenőrzése és az államhatár rendjének fenntartása [9, 1.§. (1)]. A

[1] Napjainkban már Igazságügyi és Rendészeti Minisztérium.

nemzetbiztonsági szolgálatok feladata pedig a külföldre vonatkozó, illetve külföldi eredetű, a nemzet biztonsága érdekében hasznosítható információk megszerzése [10, 4.§ a) és 6.§ a)], valamint a Magyar Köztársaság szuverenitását, érdekeit veszélyeztető tevékenységek felderítése és elhárítása [10, 5.§ a)-d) és 7.§ a)-d)].

A katonai erő esetében a rendeltetés megfogalmazásának lényegi elemei közé a 'külső' és a 'fegyveres' jelzők tartoznak. Az előbbi értelmezése viszonylag egyértelmű, az utóbbié viszont ma már egyre kevésbé. Fegyver alatt általánosságban támadás vagy védekezés megvalósítására, vagy ezek hatásfokának, hatótávolságának megnövelésére alkalmas eszközt értünk. Átvitt értelemben minden, ami képes másban (tárgyban, élőlényben) kárt tenni, fegyvernek tekinthető. A hagyományos fegyverek mellett így jelentek meg a haderők haditechnikai arzenáljában az elektronikai hadviselés eszközei.

A kritikus infrastruktúra védelem feladatai közül a **sajátos katonai/védelmi képességek** vonatkozásában első lépésben kizárhatóak az olyan általános jellegű feladatok, mint a fenyegetések és sebezhetőségek elemzése és értékelése, a felkészülés és felkészítés, valamint a felismert sebezhetőségek megszüntetésére, illetve a szükségtelen kockázatok elkerülésére irányuló tevékenységek túlnyomó többsége.

A fennmaradó feladatok, illetve az ehhez szükséges sajátos képességek célszerűen időrendi csoportosításban vizsgálhatóak, amelynek alapvető határpontjait a kritikus információs infrastruktúrák biztonságát fenyegető esemény bekövetkezése, a veszélyeztető hatások megszüntetése/megszűnése, illetve az eredeti állapot helyreállása képezheti. A következőkben sorra vesszük az egyes időszakok fő feladatait és az ezek során felhasználható sajátos képességeket.

A **biztonságot fenyegető esemény bekövetkezése előtti időszak** fő feladata a fenyegetés bekövetkezésének megelőzése, illetve a biztonság megsértésének folyamatos figyelése, észlelése és a bekövetkezés esetén a szükséges riasztások, tájékoztatások megtétele.

A kritikus információs infrastruktúrák biztonságát tudatosan fenyegető (támadó) szereplőkhöz kapcsolódó megelőzési feladatok – más, ellenséges környezetben zajló tevékenység-rendszerekhez hasonlóan – magukban foglalják a potenciális támadók körének naprakész meghatározását; tevékenységük folyamatos figyelemmel kísérését; a fenyegetés megvalósítására irányuló képességeik csökkentését; a támadás végrehajtásától történő elrettentésüket; valamint a potenciális fenyegetéseik elleni védelmi képességek kialakítását. Ezek között az információs színtéren két nagyobb, a védelmi szférához kapcsolódó feladatcsoport azonosítható. Az első a 'passzív' felderítés/hírszerzés, a második pedig az 'aktív' ellentevékenység (zavarás, lefogás, pusztítás). Ezek részletesebb elemzésére a továbbiakban kerül majd sor.

A kritikus információs infrastruktúrák biztonságát fenyegető események figyelése és észlelése, a szükséges riasztások, tájékoztatások megtétele egy összetett szervezet- és eszközrendszer feladata, amelynek szervezeti összetevőit a különböző megnevezésű egységek (számítógépes vészhelyzeti reagáló csoport, számítógépes biztonsági esemény kezelő központ, számítógépes biztonsági esemény reagáló csoport, stb.[2]), speciális eszközrendszerét pedig többek között a különböző behatolás érzékelő és megelőző rendszerek[3] képezik. A biztonsági központok infrastruktúra összetevőkhöz, területi egységekhez köthetőek, fenntartásuk és működtetésük speciális katonai/védelmi képességeket tulajdonképpen nem igényel. Működésük folytonosságának biztosítása azonban szükségessé teheti védett – állami, katonai, vagy védelmi szféra – objektumokban történő elhelyezésüket.

A **biztonságot fenyegető esemény bekövetkezése utáni időszak** fő feladata a káros hatások érvényesülésének csökkentése, mérséklése, majd – amennyiben lehetséges – e

[2] Computer Emergency Response Team (CERT), Computer Security Incident Response Center (CSIRC), Computer Security Incident Response Team (CSIRT).

[3] Intrusion Detection/Prevention System (IDS/IDP).

hatások megszüntetése, végül az okozott károk elhárításának, a működés helyreállításának megkezdése. Az első feladatcsoport tevékenységei alapvetően a veszélyeztetett információs infrastruktúra védelmének általános és célorientált megerősítésére irányulnak, azonban a káros hatások csökkentésére, megszüntetésére mód van – az előzőekben már említett – a támadók ellen irányuló, a védelmi szférához kapcsolódó ellentevékenység segítségével is.

A kritikus információs infrastruktúrák esetében – egyes esetekben, megfelelő eszközrendszer birtokában – más szereplők mellett a védelmi szféra szervezetei, ezen belül is kiemelten az érintett katonai (híradó és informatikai) szervezetek átmenetileg képesek lehetnek a megtámadott infrastruktúrák kieső, vagy csökkentett szolgáltatásai pótlására, kiegészítésére. Erre telepítés után alapvetően a tábori híradó és informatikai rendszer erői és eszközei alkalmasak. Ennek megfelelően a kritikus információs infrastruktúrák védelmének keretében például célszerű meghatározni, hogy a Magyar Honvédségnek e célra milyen képességeket és kapacitásokat kell kialakítania és fenntartania.

A **veszélyeztető hatások megszüntetését/megszűnését követő időszak** fő feladata a kritikus információs infrastruktúrák teljeskörű működésének helyreállítása, az okozott károk következményeinek felszámolása, valamint a bekövetkezett támadás, veszélyeztetés elemzése, a biztonság fenntartásához szükséges védelmi intézkedések megtétele. E tevékenységek túlnyomó többsége első ránézésre nem igényel sajátos katonai, védelmi képességeket. Van azonban egy olyan szakterület, amelyik napjainkban általános értelemben is egyre növekvő jelentőséggel bír és ezen belül a kritikus információs infrastruktúrák védelmében is számottevő szerepet játszik.

Az előzőekben említett szakterület a bűnügyi (igazságügyi) nyomrögzítés, szakértés[4] az információs színtéren. Az igazságügyi nyomrögzítés, szakértés kezdetei a törvényszéki orvostanhoz köthetőek, amely speciális szakterületként a 19. század végén jelent meg, majd jelentős bővülés után alakult ki az igazságszolgáltatási rendszer számára érdekes kérdéseket megválaszoló tudományok rendszere[5]. Az információs színtéri szakértés, nyomrögzítés alapvető rendeltetése leegyszerűsítve az, hogy – más szakterületekkel együttműködésben – biztosítsa a jogellenes cselekedeteket elkövetők azonosítását és tevékenységük bizonyítását. A kritikus információs infrastruktúrák védelme esetében ez pedig hozzájárulhat a biztonságot szándékosan fenyegető szereplők elrettentéséhez, illetve felfedésükhöz és megbüntetésükhöz.

A következőkben sorra vesszük az előzőekben említett, katonai (védelmi) szférához köthető, speciális képességeket igénylő feladatokat, tevékenységeket.

### *Felderítés/hírszerzés az információs színtéren*

Az információs színtérnek a kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplőivel kapcsolatos információk megszerzése – a potenciális támadók körének naprakész meghatározása, tevékenységük figyelemmel kísérése – céljában, funkcióiban és feladataiban lényegében nem különbözik a nemzetbiztonsági szolgálatok, a katonai és a rendvédelmi szervezetek hírszerző, felderítő tevékenységétől, annak integráns részét képezi. Ebből – valamint a kapcsolódó törvényi szabályozásból – kifolyólag e tevékenység, illetve az ehhez szükséges képességek kiépítése és felhasználása szinte kizárólagosan a védelmi szféra feladata.

A kritikus információs infrastruktúrák biztonságát fenyegető szereplőkre vonatkozó információk megszerzése több szempontból is szorosan kapcsolódik a felderítés/hírszerzés 'hagyományos' területeihez. Egyrészt a potenciális veszélyt jelentő szereplők nem feltétlenül csak információs infrastruktúrákat fenyegetnek, hanem más, biztonsági szempontból lényeges célpontokat, másrészt az információs infrastruktúrákat nem feltétlenül [csak] információs támadásokkal, hanem hagyományos (pld. fizikai) módon is veszélyeztetik, így a rájuk

[4] Cyber forensics.
[5] Forensic sciences (forensics) = bírósági, bűnügyi tudományok.

vonatkozó egyes információk 'hagyományos' felderítési forrásokból, eszközökkel is – esetenként csak onnan – beszerezhetőek és ezeket más területek is felhasználhatják.

A kritikus információs infrastruktúrák védelméhez, egyben az informatikai biztonsághoz kapcsolódó felderítés/hírszerzés kialakulóban lévő speciális szakterülete az informatikai eszközökben megtalálható és az informatikai hálózatokon áramló információk megszerzése, összegyűjtése, elemzése és értékelése. E terület megnevezésére az angol nyelvű szakirodalomban különböző kifejezésekkel találkozhatunk: 'computer network exploitation', 'cyber intelligence', 'cyber surveillance'.

Az Egyesült Államok haderejében a számítógép-hálózati hadviselés[6] kifejezés az információs műveletek legújabb, ötödik területeként jelent meg [11, II-4 – II-5.o.]. A számítógép-hálózati hadviselés három összetevőjét a számítógép-hálózati támadás, a számítógép-hálózati védelem és a számítógép-hálózati felderítés képezi.[7] A **számítógép-hálózati felderítés** – szószerinti fordításban inkább számítógép-hálózati 'kihasználás' – "számítógépes hálózatok segítségével végrehajtott támogató műveletek és felderítési információszerző képességek, amelyek rendeltetése adatgyűjtés célpontot képező, vagy szembenálló felekhez tartozó informatikai rendszerekből és hálózatokból" [11, Glossary GL-6.o.] Ugyanezen kifejezés NATO értelmezése már közvetlenül nem tartalmaz a felderítésre utaló összetevőt, közelebb áll a 'kihasználás' tartalmához: "számítógép, vagy számítógép-hálózat, illetve a bennük rendelkezésre álló információk felhasználása előny megszerzése céljából" [12, 2-C-12.o.]

A számítógép-hálózati hadviselés hármas tagolása és ezen belül a számítógép-hálózati felderítés helye, szerepe tulajdonképpen az elektronikai hadviselés hármas felosztását – elektronikai ellentevékenység, elektronikai védelem és elektronikai támogató tevékenység – követi, ami egyben átvezet a rádióelektronikai felderítés szakterületéhez: "az elektronikai támogató tevékenységnek gyakorlatilag azonosak a feladatai a jelfelderítéssel (Signal Intelligence, SIGINT), de …" [13, 3.o.].

A **rádióelektronikai** (másnéven jel-) **felderítés**[8] a felderítés egyik információszerzési eljárása (módja), amely "passzív eszközökkel az elektromágneses kisugárzások gyűjtéséből, értékeléséből, analizálásából, feldolgozásából szerzi információit" [14, 37.o.]. A rádióelektronikai felderítés eljárásainak további osztályozására a szakirodalomban nem alakult ki közmegegyezés, a SIGINT technológiák köre a technológiai fejlődéssel együtt bővült, változott (kommunikációs felderítés, rádiótechnikai felderítés, stb.[9]). A NATO értelmezés szerint a rádióelektronikai felderítés a kommunikációs és rádiótechnikai felderítést összefoglaló fogalom. [12, 2-S-7.o.]

A rádió-, fax-, telex-, vagy radareszközök közötti kommunikáció lehallgatása a kommunikációs hálózatok struktúrájának, forgalmi viszonyainak, az egyes csomópontok szerepének felderítése mellett – az esetleges rejtjelfejtés után – többnyire a továbbított információk (üzenetek) megismerését is biztosította. Mindez azonban jelentősen megváltozott a számítógépek közötti csomagkapcsolt információcsere megjelenésével. Napjainkban – a 'minden IP felett' korszakában – már egyre kevésbé kerülhető meg az IP-alapú kommunikáció lehallgatása, elemzése és az ebből származó felderítési információk előállítása.

Az új felderítési információszerzési eljárás, amelynek megnevezésére egyes szakirodalmakban megjelent a '**számítógépek közötti jelfelderítés**'[10] kifejezés, még csak kialakulóban lévő technológia, azonban szerepe és jelentősége már elvitathatatlan. A

[6] Computer Network Operations (CNO).
[7] Computer Network Attack (CNA), Computer Network Defense (CND) és Computer Network Exploitation (CNE).
[8] Signals Intelligence (SIGINT).
[9] Communications Intelligence (COMINT), Electronic Intelligence (ELINT).
[10] Computer-to-computer SIGINT (C2C SIGINT).

szakterület számára "a következő időszak legfontosabb technológiai kihívása a számítógép-hálózatok felderítése, elemzése, illetve az adatforgalom lehallgatása, vagyis a C2C-SIGINT" [15, 160. o.] "A hír-szerző közösség évtizedes elutasítása után a korszerű technológiák megváltoztatják a hálózatok megfigyelésének régi megoldásait. Számos új technológia biztosítja a számítógépek között (C2C) áramló adatok elfogását, elemzését és hasznosítását ellenséges környezetben." [16, *.o.]

A számítógépek, illetve tágabb értelemben az információs tevékenységeket megvalósító informatikai eszközökre, valamint a bennük tárolt és köztük – adatok formájában – áramló információk megszerzésére irányuló **újszerű felderítési eljárások és módszerek** alapját az elsődleges adatszerzés képezi. Az informatikai eszközökben feldolgozott, tárolt információkhoz hozzá lehet jutni az eszközök, vagy adathordozóik fizikai megszerzésével; az eszközök működés közbeni elektronikus lehallgatásával; valamint rosszindulatú programok bejuttatásával. Az informatikai eszközöket összekapcsoló hálózatokon áramló információk megszerezhetőek a hálózati útvonalak fizikai megcsapolásával, vagy elektronikus lehallgatásával; valamint a hálózati kapcsolóelemekből (központok, kapcsolók, átjárók, útvonalválasztók, stb.).

A felsoroltak közül a fizikai és az elektronikus felderítési módszerek gyakorlatilag napjainkban is rendelkezésre állnak, bár a korszerű kommunikációs eljárások (pld. frekvenciaugratásos, vagy szórt spektrumú módszerek) megnehezítik a felderítést és az adatszerzést. Az újszerű megoldások közé így a rosszindulatú programokra (tulajdonképpen informatikai támadásokra) épülő, illetve a hálózati kapcsolóelemekhez kapcsolódó adatszerzés tartoznak. Az előbbivel, a 'passzív támadásokkal' más vonatkozásokban részletesebben a következő alpont foglalkozik majd, amelynek alapvető megállapításai érvényesek a kritikus információs infrastruktúrákat fenyegetők felderítésére is.

A hálózati kapcsolóelemekből történő információszerzés vizsgálatához már meg kell különböztetnünk a **belső ('hazai') és** a **külső ('külföldi') szereplők**, pontosabban az államon belüli és az azon kívüli informatikai infrastruktúrához kapcsolódó szereplők körét. Ettől függnek ugyanis az alkalmazható eljárások és módszerek és ettől függ, hogy kihez – melyik szervezethez – célszerű telepíteni az adott (felderítő) képességet.

Egy adott államon belül – megfelelő felhatalmazás birtokában – általában törvények biztosítják a nemzetbiztonsági és rendvédelmi szervek számára, hogy információkat szerezzenek be és megfigyeljék, lehallgassák a kommunikációs és/vagy informatikai hálózatokon zajló információcserét. Ez utóbbi technikai feltételeit az adott államon belül az érintett szolgáltatók (távközlési, internet, stb.) kötelesek biztosítani, így az arra felhatalmazott szervek az adott államon belül kiterjedt felderítési lehetőségekkel rendelkeznek.

Az információs színtér 'határok felettiségéből' következően a kritikus információs infrastruktúrákat fenyegető szereplők a világon szinte bárhol lehetnek, bárhonnan elérhetik, veszélyeztethetik a védendő infrastruktúrákat. Egy adott államnak a saját területén kívül két lehetősége van az információkhoz, információforgalomhoz, vagy ezek egy részéhez hozzáférni: együttműködés (uniós, szövetségi, vagy kétoldalú) révén, vagy titkos, hírszerzési információszerzési módszerekkel.

### *Ellentevékenység az információs színtéren*

Az információs színtérnek a kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplői ellen irányuló tevékenység rendeltetése, hogy csökkentse a fenyegetés megvalósítására irányuló képességeiket, elrettentse őket a támadás végrehajtásától. Az ellentevékenység katonai értelmezés szerint eszközök és módszerek alkalmazása az ellenséges tevékenység hatékonyságának csökkentésére [17, 129.o.]. Ennek megfelelően az ellentevékenység irányulhat a fenyegetést kiváltó szereplőre, az általa felhasznált eszközre, a védendő objektumot érő fenyegető hatásra, valamint épülhet a megtévesztésre is. Az

ellentevékenység módszereinek és eszközeinek többsége lényegét tekintve csak kevésbé, de céljaiban, esetleg mértékében különbözik a támadásoktól.

Az információs infrastruktúrák védelmét szolgáló ellentevékenység jellegét tekintve lehet adminisztratív (jogi), fizikai és információs. Az első csoportba tartozik például a joghátránnyal fenyegetés, illetve annak megvalósítása (büntető intézkedések), amelynek végrehajtói a törvényhozás, az igazságszolgáltatás és a rendvédelem szereplői. A második csoportot meghatározott feltételek fennállása esetén a fizikai megsemmisítés, pusztítás, rombolás alkotják és végrehajtói a katonai erők. A továbbiakban azonban részletesen csak a harmadik csoportba tartozó információs jellegű ellentevékenységgel foglalkozunk.

Az Egyesült Államok haderejében már a 2000-es évek elején megfogalmazódott **a számítógép-hálózati védelem aktív összetevőinek** szükségessége. Egy légierő akadémiai tanulmány aktív védelemnek azon rendszabályok összességét tartja, amelyek meghiúsítják a folyamatban lévő támadásokat, vagy a további támadásokat megnehezítik. Ezek közé sorolja, az ellentámadást, a megelőző támadást és az aktív megtévesztést[11]. Az ellentámadás a támadó informatikai rendszerei elleni számítógép-hálózati támadás az eredeti támadás során, vagy közvetlenül azt követően. A megelőző támadás a szembenálló fél (potenciális fenyegető) informatikai rendszerei elleni támadás abból a célból, hogy megakadályozza hatékony támadás indítását a saját rendszereink ellen. Végül az aktív megtévesztés a támadás eltérítése a saját rendszerekről azok virtuális helyettesítőire, ezzel abban a hitben hagyva a támadót, hogy sikerrel járt, de tevékenysége valójában semlegesítésre került. [18; 3-4.o.]

Az információs jellegű **megelőző támadás és ellentámadás** gyakorlatilag információs támadás a potenciális, vagy aktuális támadó ellen. Ennek eszköze lehet bármilyen támadó eszköz vagy módszer: a támadó fél rendszerébe bejuttatott rosszindulatú program, túlterheléses támadás, vagy megtévesztő üzenet. Mivel az ellentevékenység célja lehet a fenyegető szándékról történő lemondatás is, a megelőző, vagy ellentámadás lehet akár aszimetrikus is. Vagyis a fenyegetést közvetlenül megvalósító rendszer helyett irányulhat a fenyegetést kiváltó szereplő más rendszereire, eszközeire, vagy értékeire.

A kritikus információs infrastruktúrák védelmét, mint az adott állam biztonságának fenntartását szolgáló megelőző és ellentámadások megvalósítása funkcionális szempontból – mivel túlnyomó többségében a biztonságot kívülről fenyegető szereplők ellen irányul – a katonai erők feladata. Erre a megállapításra jut például egy 2008-ban kibocsátott tanulmány is. [19]

A **megfelelő képességgel rendelkező katonai szervezetek** kialakítása a nagyobb haderőkben már a 2000-es évek elején megkezdődött. A szakirodalomban ezek közé sorolják mindenekelőtt az Egyesült Államokat, Oroszországot és Kínát, de egy 2007-es McAfee jelentés szerint már körülbelül 120 állam használja az Internetet politikai, katonai, vagy gazdasági kémkedésre és támadásokra, épít ki informatikai támadási képességeket. [20, 12.o.]

Napjaink informatikai támadásainak egyik sajátos eszköze a rosszindulatú programok segítségével saját ellenőrzés alá vont számítógépek– akár több milliós – összessége (botnetek). Ennek megfelelően merült fel az Egyesült Államok hadseregében az informatikai megelőző és ellentámadások egyik eszközeként a **katonai botnetek** alkalmazása. A katonai botnet nem rosszindulatú programok segítségével, szándékuk ellenére felhasznált zombi gépek segítségével, hanem a végrehajtó kód saját eszközökre történő telepítésével lehetne kialakítható. A szerző elgondolása szerint bázisául felhasználhatók lennének például behatolás ellenőrző eszközök, a nem minősített hálózathoz csatlakozó számítógépek, sőt az elavulásuk miatt leváltásra kerülő eszközök is. [21]

Az informatikai megelőző és ellentámadások legnagyobb problémái közé a **'célmegjelölés'**, a **hatások célzottsága** és a **jogi kérdések** tartoznak. Számos szakmai anyag,

[11] Counterattack, preemptive attack, active deception.

publikáció foglalkozik ezekkel a kérdésekkel, amelyek között az első lényegét az képezi, hogy az információs színtéren – nagyrészt az Internet sajátosságai következtében – nem könnyen azonosítható a fenyegetést közvetlenül megvalósító informatikai rendszer, vagy eszköz és a mögötte álló szereplő. Közismert tény, hogy az azonosítás alapját képező IP cím egyrészt könnyen hamisítható[12], másrészt a fenyegetés kiváltható más, gyanútlan szereplő informatikai eszközének felügyelet alá vonásával és felhasználásával. Emellett ma már szolgáltatásként állnak rendelkezésre olyan 'anonimizáló' hálózatok, amelyek segítségével a hálózaton áramló információk (ezzel együtt műveletek) forrása visszakövethetetlenné tehető.[13]

Problémát jelent az informatikai támadások célzottsága is, ugyanis napjaink alapvetően csomagkapcsolt technológiára épülő hálózatai esetében egy adott, a fenyegetés megvalósításában résztvevő eszköz, vagy összetevő (végberendezés, hálózati csatolóelem, hálózati vonalszakasz, hálózati szegmens, stb.) támadása általában nem csak a megcélzott szereplőre, hanem számos más, vétlen szereplőre is hatással lehet.

Végül az informatikai megelőző és ellentámadások – tekintettel arra, hogy a jelenleg kialakulóban lévő gyakorlat szerint ezek a haderők feladatai között jelennek meg – jelentős jogi problémákat is felvetnek. Ezek közül az első, hogy a nemzetközi hadijog, vagy a humanitárius jog milyen módon vonatkozik az informatikai támadásokra. A kérdés megválaszolása többek között attól függ, hogy az informatikai támadások fegyveres konfliktust jelentenek-e; alkalmazásuk mennyiben okoz sebesülést, sérülést, halált, stb.; vagy hogy mennyiben különböztethetőek meg a katonai és civil célpontok. Ezt elemzi például részletesen [22] is.

További jogi problémát jelenthet a katonai erő hazai alkalmazásának viszonylag általánosan alkalmazott korlátozása, ugyanis az információs színtéren nem mindig különíthető el könnyen a hazai és a nem hazai jelleg. Ez utóbbira nincs még igazán kialakult jogi gyakorlat, vagyis hogy mi dönt: a fenyegető szereplő, a felhasznált eszközök, vagy például a közreműködő szolgáltatók honossága. Ez szintén az informatikai megelőző, vagy ellentámadások elrendelése során jelent problémát.

A bemutatott problémák könnyen belátható módon megnehezítik a védelmi célú, informatikai megelőző, vagy ellentámadások eredményes megvalósítását, sőt már a végrehajtásukkal kapcsolatos vezetői döntések meghozatalát is.

Az **aktív megtévesztés** tulajdonképpen átmeneti formának is tekinthető a támadás és a védelem között, hiszen nem közvetlen ráhatás a támadó félre és nem közvetlenül irányul a fenyegetett rendszer(ek) védelmére. Míg a passzív megtévesztés célja a valós szándékok és képességek elrejtése, addig az aktív megtévesztés nem valós szándékokat és képességeket hitet el a szembenálló féllel, beavatkozva ezzel – mintegy támadva – annak döntéshozatali folyamatait.

Az aktív megtévesztésnek a védelem passzív formáival szemben nem a támadó kizárása a célja a megvédendő rendszerből, hálózatból, hanem a támadás átirányítása egy nem valós rendszerbe, hálózatba, amely ugyanolyan, pontosabban hasonló erőforrásokkal és adatokkal van felszerelve, mint a valós rendszer. Mindez elősegíti a támadó megtévesztését céljai elérését illetően; erőforrásainak szétforgácsolását; valamint nem utolsósorban tevékenységének, alkalmazott módszereinek és eljárásainak megfigyelését. [18, 21-22.o.]

Az informatikai aktív megtévesztés alapvető eszköze a **'mézesbödön'** (honeypot), egy csapda az informatikai rendszerek elleni támadások, jogosulatlan hozzáférések detektálására, eltérítésére és bizonyos mértékben ellenrendszabályok végrehajtására. A 'mézesbödön' általában egy speciális informatikai eszköz, amelynek nincs valós felhasználói szolgáltatása.

[12] IP megtévesztés = IP address spoofing.

[13] Napjaink egyik alapvető anonimizáló hálózat (TOR, The Onion Router) kialakítását egyébként eredetileg az Egyesült Államok Haditengerészetének Kutató Intézete (US Naval Research Laboratory) támogatta.

Így normál körülmények között nem is vesz részt az információcserében: nem küld és nem vár információkat. Amennyiben ezek mégis bekövetkeznek, az a támadás, jogosulatlan hozzáférés egyértelmű jele. Egy hálózatba kapcsolódó, egymással együttműködő 'mézesbödönök' 'mézesbödön hálózatot' (honeynet) alkotnak. A 'mézesbödönök' alkalmazásának szükségességét már 2000-ben felvetette Winn Schwartau, az információs műveletek egyik élenjáró kutatója. [23]

Az aktív megtévesztés alkalmazása közel áll, szorosan kapcsolódik a behatolás ellenőrző eszközök alkalmazásához, így általános esetben részét képezheti egy adott szervezet informatikai védelmi szakemberei, szervezeti egysége feladatrendszerének. A kritikus információs infrastruktúrák esetében azonban egy nemzeti szintű aktív megtévesztési rendszer kialakítása, telepítése, összehangolt működtetése a felderítéssel és ellentevékenységgel megbízott szervezetben – a katonai erőn belül – célszerű. Mindezt indokolja, hogy a katonai műveleteknek régóta egyik összetevője a napjainkban már az információs műveletek közé sorolt megtévesztés. [11, I-1.o.; 12, 2-D-2; 24, 95-100.o.]

### *Bűnügyi eljárások az információs színtéren*

A krimináltechnika, vagy más néven természettudományos kriminalisztika a tárgyi bizonyítékok létrejöttének, felkutatásának és rögzítésének a törvényszerűségeit valamint azokat a vizsgálati technikákat és módszereket tanulmányozza, amelyek alkalmasak a tárgyi bizonyítási eszközökön meglévő bizonyítékok feltárására és bizonyító erejük hiteles igazolására. A kontinentális krimináltechnika fogalmi megfelelője az angolszász jogrendszerekben a bűnügyi (igazságügyi) tudomány.

A **bűnügyi (igazságügyi) tudomány** (Forensic science, gyakran rövidítve forensics) a különböző tudományok széles körének alkalmazása a jogrendszer kérdéseinek megválaszolására. Más megfogalmazásban: a tárgyi bizonyítékok felkutatására, vizsgálatára, értékelésére alkalmazott tudományos ismeretanyag. [25, 41.o.] A hagyományos szakterületek közé tartozott többek között a törvényszéki orvostan, a daktiloszkópia, vagy a fegyvertan. Az új típusú bűncselekmények megjelenése és a tudományos, technikai fejlődés szükségessé és egyben lehetségessé is tette új bűnügyi szakértői, vizsgálati módszerek, szakterületek megjelenését. Az információs színtérhez, az informatikai rendszerekhez, eszközökhöz és hálózatokhoz kapcsolódóan az idők során számos fogalom megjelent.

Az **informatikai bűnügyi eljárások** összetevői időben egymást követően jelentek meg. Elsőként a számítástechnikai bűnügyi eljárások (computer forensics) jelent meg, mint a számítógépekben és a digitális adathordozókon megtalálható bűnügyi (igazságügyi) bizonyítékokhoz kapcsolódó szakterület. Egy FBI ügynök már az 1990-es évek közepén egy konferencia előadásban definiálja a 'computer forensics' fogalmát és elemzi, hogyan biztosítható a digitális információhordozóknak a hagyományos papíralapú bizonyítékokhoz hasonló elfogadhatósága. [26]

Az információtechnológia fejlődésével az információs tevékenységeket támogató különböző szakterületek (információszerzés, továbbítás, megjelenítés) eszközei egyre inkább azonos összetevőkre (processzorokra, tárakra, memória-elemekre, megjelenítő elemekre) épültek, így a szakterület a számítástechnikai jelző ellenére kiterjedt a mobiltelefonokra, digitális kamerákra, más technikai eszközökbe beágyazott informatikai részegységekre. Részben ehhez kapcsolódóan, részben ettől függetlenül találkozhatunk a 'digital forensics', vagy napjaink divatos jelzőjéhez kapcsolódóan a 'cyber forensics' kifejezéssel is.

Viszonylag önálló szakterületként jelent meg a hálózati, vagy Internet bűnügyi eljárások (network forensics, Internet forensics). A hálózati bűnügyi eljárások lényege a hálózaton továbbított adatok elfogása, rögzítése és elemzése a hálózati események azonosítása, a hálózatokon keresztül megvalósított veszélyeztetések felderítése és bizonyítása. A megvalósítás két alapvető módszere: mindent rögzíteni, majd később elemezni; vagy figyelni,

szűrni, így csak a 'gyanús' adatokat, eseményeket rögzíteni. Ez a technológia nem új, bizonyos értelemben előzményének tekinthetőek a telefonlehallgatások, az ECHELON rendszer, illetve az FBI elsősorban e-mail-ek megfigyelését szolgáló Carnivore programja. Míg a számítástechnikai bűnügyi eljárások megfogható tárgyakkal (számítógépek, technikai eszközök, adathordozók, stb.) dolgozik, addig a hálózati bűnügyi eljárások tárgya nem tartós: ha nem ismeri fel, vagy nem rögzíti, nem tud felhasználható eredményt szolgáltatni. [27]

Az előzőekben vázlatosan bemutatott módszerek és az ezeket támogató eszközök a napjainkban általánosan elfogadott értelmezés szerint mindenekelőtt a rendvédelem alkalmazási területéhez kapcsolódnak. Könnyen belátható módon szorosan kapcsolódnak a kritikus információs infrastruktúrák biztonságának megőrzéséhez is, amelyben rendvédelmi szempontból szerepük a biztonsági fenyegetések (bűncselekmények) felfedése, megelőzése, bekövetkezésük esetén pedig a cselekmények és elkövetőik azonosítása és ennek jogi erejű bizonyítása. Magyarország esetében e szakterület alkalmazásának jogosult szereplői a Nemzeti Nyomozó Iroda, valamint a szakterületen működő igazságügyi szakértők.

Az állampolgárok által birtokolt, vagy továbbított információk jogosulatlan megismerés elleni védelmét az államok többségében jogszabályok biztosítják. A különböző távközlési, informatikai és más hálózatokon áramló információkhoz történő hozzáférés jogát általában szintén törvények szabályozzák, Magyarországon pld. az elektronikus hírközlésről szóló törvény kötelezi a szolgáltatókat, hogy bizonyos adatokat folyamatosan naplózzanak, meghatározott ideig őrizzenek és azokat a nyomozó hatóságoknak meghatározott feltételek fennállása esetén adják át. [28]

A hálózatokon áramló információk rendvédelmi célú megfigyelésének eszköze az úgynevezett **jogszerű megfigyelés** (Lawful Interception). A hálózati adatforgalom valós időben történő jogszerű megfigyelésének lehetősége a hagyományos – alapvetően vonalkapcsolt – kommunikációs hálózatokban biztosított volt, mindezt a hozzáférési hálózatokban nemzetközi szabványok szabályozták. Ilyen szabványosításra a csomagkapcsolt, ezen belül az IP-alapú hálózatok esetében nem került sor és maga a csomagkapcsolt üzemmód is megnehezíti egy adott félhez köthető információcsere megfigyelését. Mindebből következően az Internet 'lehallgatása' egyrészt számos nehézségbe ütközik, másrészt az alkalmazható technikák az arra nem jogosultak számára is rendelkezésre állnak.[14]

A rendvédelmi alkalmazás mellett az **informatikai bűnügyi eljárások a katonai alkalmazásban** is meg kell jelenjenek, mint az egy információs hadviselési szakértő tanulmányában már 2002-ben megfogalmazta. Definíciója szerint az informatikai bűnügyi eljárások katonai értelemben "tudományosan igazolt módszerek felkutatása és alkalmazása digitális bizonyítékok gyűjtésére, feldolgozására, értelmezésére és felhasználására, annak érdekében, hogy:

- bizonyító erejű leírást nyújtson az összes támadó jellegű információs tevékenységről a szervezeti és kritikus infrastruktúra támadást követő teljeskörű helyreállításához;
- vesse össze, értelmezze és jelezze előre a szembenálló fél tevékenységeit, valamint azok hatásait a tervezett katonai műveletekre;
- tegye a digitális adatokat alkalmassá és meggyőzővé egy bűnügyi vizsgálati folyamatban történő felhasználásra." [29, 3.o.]

Az Egyesült Államok Védelmi Minisztériumában 2002-ben felállításra került egy Informatikai Bűnüldözési Központ (Cyber Crime Center), amely meghatározza a szakterület eljárási szabályait, módszereit és eszközeit; segítséget nyújt a katonai nyomozó hatóságok bűnügyi, kémelhárító, terrorizmus elleni és csalásokkal szembeni tevékenységéhez. A központ az 1998-ban létrehozott Számítástechnikai Bűnügyi Laboratórium (DoD Computer Forensics Laboratory) bázisán került kialakításra. A központ tevékenységének három pillére:

[14] Lásd például a 2008 nyarán felfedett, a Border Gateway Protocol hibájára épülő 'lehallgatási' lehetőséget.

a laboratórium, egy oktatási intézmény és egy kutatóintézet. Rendeltetése, hogy hozzájáruljon a Védelmi Minisztérium katonai igazságügyi, katonai biztonsági tevékenységének továbbfejlesztéséhez és az információs színtéri fölény megteremtéséhez.

Az informatikai bűnügyi eljárások megkerülhetetlen részét fogják képezni a NATO által Észtországban 2008 végéig felállítandó Informatikai Védelmi Központ[15] feladatrendszerének. A központ felállítása közvetlenül kapcsolódik a kritikus információs infrastruktúrák védelméhez, mivel indokát az Észtország – ezen belül kritikus infrastruktúrái – ellen 2007 májusában indított kiterjedt támadás képezte. A támadás egy NATO tagállamot ért, azonban az informatikai támadások hadijogi tisztázatlansága miatt, illetve a támadó fél bizonyítható azonosításának hiányában a NATO nem tudta (akarta) érvénybe léptetni az 5. cikkely szerinti reagálást, így a válaszlépés szakértők kiküldésére korlátozódott.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Egy nemzeti kritikus információs infrastruktúrának mindenképpen részét képezi az adott állam védelmi és ezen belül katonai kritikus információs infrastruktúrája is. Ennek megfelelően a katonai, illetve a védelmi szféra szervezetei saját infrastruktúrájuk védelméhez kapcsolódóan szerepet játszanak a nemzeti kritikus információs infrastruktúrák védelmében. A katonai, illetve védelmi szféra az előzőekben megfogalmazottnál bővebb feladatokkal rendelkezik, jelentősebb szerepet játszik a kritikus információs infrastruktúra védelemben.

A kritikus infrastruktúrák biztonsága a nemzeti biztonság egyik alapvető összetevője, így megvalósításában érintett a katonai, a rendvédelmi, a katasztrófavédelmi és nemzetbiztonsági szakterület is. A kritikus infrastruktúrákhoz hasonló, összetett rendszerek informatikai védelmében leginkább a többnemzeti műveletekben résztvevő katonai erőknek vannak tapasztalatai. Végül a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, a támadók elleni fellépés, de legalábbis e feladatok nagyobb része és egészének koordinációja a védelmi szféra feladata.

A kritikus információs infrastruktúra védelemmel kapcsolatos nemzeti megközelítések négy csoportba sorolhatóak:

- technikai szintű, információ-, illetve informatikai biztonsági megközelítés, kiemelt tekintettel az Internet-biztonságra;
- e-gazdasághoz kapcsolódó működésfolytonossági (üzletmenet-folytonossági) szemlélet;
- rendvédelmi megközelítés, amely az informatikai bűnözés elleni tevékenységre összpontosít;
- nemzetbiztonsági megközelítés, amely a kritikus információs infrastruktúra védelmet annak lényeges összetevőjeként szemléli.

A védelmi szférához kapcsolódó sajátos képességek iránti igények mögött állhat az, hogy a kritikus információs infrastruktúra védelemhez szükséges, vagy ahhoz nagymértékben hasonló képességek sajátos eszköz- és eljárásrendszere, valamint az ezek alkalmazására való felkészültség a védelmi szféra valamely szereplőjéhez kapcsolódik, vagy az adott tevékenység végrehajtását, illetve végrehajtóját jogszabályok írják elő, korlátozzák.

A katonai és rendvédelmi szervezeteknek mindenekelőtt a kritikus információs infrastruktúrákat tudatosan fenyegető szereplők esetében vannak (lehetnek) feladatai, a gondatlanságból származó és természeti, vagy ipari eredetű veszélyeztetések alapvetően a katasztrófavédelem feladatkörébe tartoznak. A katonai (védelmi) szféra feladatai elsősorban a következő területekhez kapcsolódhatnak: a 'passzív' felderítés/hírszerzés és az 'aktív' ellentevékenység (zavarás, lefogás, pusztítás) az információs színtéren; a megtámadott infrastruktúrák kieső, vagy csökkentett szolgáltatásai pótlása, kiegészítése; végül a bűnügyi eljárások (nyomrögzítés, szakértés) az információs színtéren.

[15] Cooperative Cyber Defense Center of Excellence.

A kritikus információs infrastruktúrák biztonságát szándékosan fenyegető szereplőkkel kapcsolatos információk megszerzése – a potenciális támadók körének naprakész meghatározása, tevékenységük figyelemmel kísérése – céljában, funkcióiban és feladataiban lényegében nem különbözik a nemzetbiztonsági szolgálatok, a katonai és a rendvédelmi szervezetek hírszerző, felderítő tevékenységétől, annak integráns részét képezi, így az ehhez szükséges képességek kiépítése és felhasználása szinte kizárólagosan a védelmi szféra feladata. Napjainkban kialakulóban van a felderítés/hírszerzés egy speciális szakterülete: az informatikai eszközökben megtalálható és az informatikai hálózatokon áramló információk megszerzése, összegyűjtése, elemzése és értékelése.

Az információs infrastruktúrák védelmét szolgáló ellentevékenység jellegét tekintve lehet adminisztratív (jogi), fizikai és információs. Az információs jellegű ellentevékenység típusai: az ellentámadás, a megelőző támadás és az aktív megtévesztés. A megelőző támadás és ellentámadás gyakorlatilag információs támadás a potenciális, vagy aktuális támadó ellen. Ennek eszköze lehet bármilyen támadó eszköz vagy módszer. A kritikus információs infrastruktúrák védelmét szolgáló megelőző és ellentámadások megvalósítása a katonai erők feladata. A megfelelő képességgel rendelkező katonai szervezetek kialakítása a nagyobb haderőkben már a 2000-es évek elején megkezdődött. Az informatikai megelőző és ellentámadások legnagyobb problémái közé a 'célmegjelölés', a hatások célzottsága és a jogi kérdések tartoznak. Az aktív megtévesztés célja a támadás átirányítása egy nem valós rendszerbe, hálózatba, ami elősegíti: a támadó megtévesztését céljai elérését illetően; erőforrásainak szétforgácsolását; valamint tevékenységének, alkalmazott módszereinek és eljárásainak megfigyelését. A kritikus információs infrastruktúrák esetében egy nemzeti szintű aktív megtévesztési rendszer kialakítása, telepítése, összehangolt működtetése a felderítéssel és ellentevékenységgel megbízott szervezetben – a katonai erőn belül – célszerű.

A kritikus információs infrastruktúrák biztonságának megőrzését is szolgáló informatikai bűnügyi eljárások mindenekelőtt a rendvédelem alkalmazási területéhez kapcsolódnak. Ezen belül a hálózatokon áramló információk rendvédelmi célú megfigyelésének eszköze az úgynevezett jogszerű megfigyelés. Az informatikai bűnügyi eljárásoknak a rendvédelmi alkalmazás mellett a katonai alkalmazásban is egyre növekvő szerepük van, amelyet számos katonai szervezet, intézmény felállítása is bizonyít.

Összességében megfogalmazható, hogy a katonai (védelmi) szféra számos sajátos képességgel vesz részt, vagy kell részt vegyen a kritikus információs infrastruktúrák védelmében. Ezen képességek, illetve kialakításuk és működtetésük részletesebb vizsgálata további kutatásokat igényel.

## FELHASZNÁLT IRODALOM


[1] MUNK Sándor: A kritikus infrastruktúrák védelme információs támadások ellen. – *Hadtudomány*, 2008/1-2. (95-106.o.)

[2] SUTER, Manuel: *A Generic National Framework for Critical Information Infrastructure Protection (CIIP)*. – Center for Security Studies, ETH, Zurich, August 2007.

[3] *COM(2005) 576, Green Paper on a European Programme for Critical Infrastructure Protection.* – Comission of the European Communities, Brussels, 17 November 2005.

[4] *The Department of Defense Critical Infrastructure Protection (CIP) Plan.* – US Department of Defense, 18 November 1998.
[http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, 2008.04.10.]

[5] *DoD Directive 3020.40, Defense Critical Infrastructure Program (DCIP).* – US Department of Defense, 19 August 2005.

[6] ABELE-WIGGERT, Isabelle-DUNN, Miriam: *International CIIP Handbook 2006. Vol. I., Vol. II.* – Center for Security Studies, ETH, Zurich, 2006.

[7] SZENES Zoltán: Válaszúton a magyar biztonságpolitika. – *Új Honvédségi Szemle*, 2005/12. (62-79.o.)
[8] *2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről.*
[9] *1994. évi XXXIV. törvény a Rendőrségről.*
[10] *1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.*
[11] *Joint Publication 3-13, Information Operations.* – US Joint Chiefs of Staff, 13 February 2006.
[12] *AAP-6(2007) NATO Glossary of Terms and Definitions (English and French).* – NATO Standardization Agency (NSA), Brussels, 2007.
[13] HAIG Zsolt-VASS Sándor-VÁNYA László: *Elektronikai hadviselés (kézirat).* – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2008.
[14] HAIG Zsolt: Az információs műveletek, a SIGINT és az elektronikai hadviselés kapcsolatrendszere. – 'A SIGINT a XXI. század kihívásainak tükrében' tudományos szakmai konferencia, Budapest, 2006. november 15., *Felderítő Szemle különszám*, 2007 február (27-48.o.)
[15] MAGYAR László: A SIGINT szerepe az aszimmetrikus fenyegetések elleni küzdelemben. – 'A SIGINT a XXI. század kihívásainak tükrében' tudományos szakmai konferencia, Budapest, 2006. november 15., *Felderítő Szemle különszám*, 2007 február (158-162.o.)
[16] PETERSON, David E.: Surveillance Slips Into Cyberspace. – *Signal* 2005/6 (61-66.o.)
[17] *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.* – Joint Chiefs of Staff, 12 April 2001 (As Amended Through 31 August 2005)
[18] HOLDAWAY, Eric J.: *Active Computer Network Defense: An Assessment.* – Air Command and Staff College, Air University, Maxwell Air Force Base, April 2001.
[19] ANDERSON, Levon: Countering State-Sponsored Cyber Attacks: Who should Lead? – In. Groh et. al. (szerk.) *Information as Power, Volume Two*. U.S. Army War College, Carlisle Barracks, 2007 (105-122.o.)
[20] *Virtual Criminology Report - Cybercrime: The Next Wave.* – McAfee Inc., November 2007.
[21] WILLIAMSON, Charles W.: Carpet bombing in cyberspace. Why America needs a military botnet? – *Armed Forces Journal*, May 2008 (20-25.o.)
[22] SCHMITT, Michael N.: Wired warfare – Computer network attack and *jus in bello*. – *International Relations Research Center Review*, June 2002 (365-399.o.)
[23] SCHWARTAU, Winn: Honeypots wreek sweet revenge against cyber intruders. – *Network World Fusion*, 2000. december 14.
[http://www.networkworld.com/columnists/2000/00173866.html 2008.08.31.]
[24] *A Magyar Honvédség Összhaderőnemi Doktrínája (Tervezet).* – HM HVK Hadműveleti Csoportfőnökség, 2002 október.
[25] KATONA Géza: *A kriminalisztika és a bűnügyi tudományok.* – BM Kiadó, Budapest, 2002.
[26] POLLITT, M.: Computer Forensics: an approach to evidence in cyberspace. – In. *Proceedings of the National Information Systems Security Conference*, Baltimore, 1995 (Volume II., 487-491.o.)
[27] BERGHEL, Hal: The Discipline of Internet Forensics. – *Communications of the ACM*, 2003/8. (15-20.o.)
[28] *2003. évi C. törvény az elektronikus hírközlésről.*
[29] GIORDANO, Joseph-MACIAG, Chester: Cyber Forensics: A Military Operations Perspective. – *International Journal of Digital Evidence*, 2002/2 (1-12.o.)

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Négyesi Imre**
Zrínyi Miklós Nemzetvédelmi Egyetem
negyesi.imre@zmne.hu

# CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE

***Abstract/Absztrakt***

*The Internet is a fundamental infrastructure of the information society. Determining role of it may become increasingly more obvious in the forthcoming years. Its significance can be increased by continuous spreading of the electronic economy and electronic services. With the help of the Internet technology new, cheap and fast, previously could not been imagined economic solutions can be originated, which may basically transform the peoples' life.*

*Az Internet az információs társadalom alapvető infrastruktúrája. Az elkövetkező években meghatározó szerepe egyre nyilvánvalóbbá válhat. Jelentőségét növelheti az elektronikus gazdaság és az elektronikus szolgáltatások folyamatos térhódítása. Az internet-technológia segítségével korábban elképzelhetetlen, új, olcsó és gyors gazdasági megoldások születhetnek, melyek alapjaiban formálhatják át az emberek életét.*

***Keywords/Kucsszavak:*** *internet, informatics, information society, information ~ internet, informatika, információs társadalom, információ*

## INTRODUCTION

The 2008 year can be an introductory of a new turning point, as a result of further dynamic expansion of the Internet and development of technology, which brings about a qualitative change. The Internet can be a primary catalyst in the course of the economical and social globalization of the countries of the Earth. The Internet may facilitate the forming of a worldwide economic competition environment, opening the door for the countries to develop knowledge-based societies. This was recognized by the OECD (Organisation for Economic Co-operation and Development), which deals with the questions that determine the further development of the Internet on a ministerial conference in 2008. This fact and another one, that a process of using the Internet and intranet on a large scale has started in the Hungarian Defence Forces made the examination of this topic current again.

## DEFINING FACTORS OF DEVELOPMENT

This article basically deals with two main topics. One is the examination of the role and development of the Internet and the other is functionally connected to this, the connection of the OECD organisation with the Internet and its change. However this publication contains only the author's thoughts arisen during the examination of the topic and the questions to be answered. This is considered the primary aim of this paper, since solutions can only be found by a comprehensive research and an action program but this is beyond the author's competence. According to this, first let us review briefly the organisation of OECD on the basis of data of the Ministry of Social Affairs and Labour. [1]

The Convention of the OECD was signed in Paris in 1960. This economic organisation, originally formed to help administer the Marshall Aid, as a legal successor of the OEEC (Organisation for European Economic Cooperation), founded in 1948, started to operate in 1961. There are currently thirty full members of it, these countries are committed to democracy and market economy, and it has active contact with another seventy states or various non-governmental organisations. Hungary became a full OECD member in 1996. The OECD's headquarters are in Paris, its official languages: French and English. (Founding members: Austria, Belgium, Denmark, United Kingdom, France, Greece, Netherlands, Ireland, Iceland, Luxembourg, Norway, Italy, Portugal, Spain, Switzerland, Sweden, Turkey, USA and Canada, then joined later: Australia, Czech Republic, South Korea, Finland, Japan, Poland, Hungary, Mexico, Slovakia.)

Among the main aims of the OECD are to support economic growth in the member states as well as to reach a high employment level, to raise living standards and financial stability. Cooperation between the member states and the non-members covers wide area of the economic and social life contributing to the growth in world trade and the development of the international economic relations. Considering its activity the OECD is a coordinative organisation, decisions are made by consensus; it has no right to apply sanctions, only moral pressure is used.

The Council and the Executive Committee are the principal organs of the OECD. The Council generally holds a meeting at ministerial level once a year and depending on economic or other topics, financial or foreign ministers participate on it. Directing functions are vested by the General Council consisted of the OECD ambassadors of the member countries. Administrative work is carried out by the OECD Secretariat headed by the Secretary-General, who is appointed by the Council. Professional work is done by more than 200 specific committees of experts and working groups covering almost the whole area of economic and social life (employment, social issues, public health, education, science, innovation, environmental protection, cooperation with developing countries, making free trade).

The OECD's professional background qualifies it for analysing economic and social processes, drawing conclusions, identifying new challenges. Its main activities are collecting comparable statistical data, publishing analyses and forecasts. OECD analyses and assessments are considered normative by the member states' and non-member states' governments as well as the broad expert public opinion. The OECD's activity with governments covers the exchange of information, co-operation programmes, and accurate examination of certain specific fields.

The OECD has been one of the main important factors of the international education from the 1960s. It is a knowledge centre, which was the starting point of numerous new realizations, thoughts, innovations and such values, which had direct influence on the governments' educational views in the developed countries of the world. In the 1960s the OECD was one of the organizations, which provided stringent arguments for those, who saw the education as one of the prime movers of economic development therefore suggested an

extensive educational policy. Later in the second half of the 1970s, after the oil crises, the OECD was one of the intellectual cradles of the paradigm shift in educational policy which resulted in raising such issues like function of education in handling unemployment of youth, more effective cost management or decentralization. An OECD member can be only that country where institutions of the democracy and market economy work dependably.

The other main topic of this article is the role of the Internet, its development and change. Determining factors of further development of the Internet can be defined on the basis of the study of Péter Bakonyi, András György and Beatrix Tóth as follows [2]:

1. As a result of convergence the functionality of the Internet will change.
2. With the help of the so-called 'multiple play' service, transfer of speech, data and broadcasting has become possible on the Internet.
3. The Internet has become an integrated part of the economy.
4. Previously the Internet has already been considered as a critical infrastructure, but nowadays it can be defined as an essential component of other critical infrastructures as well.
5. The profile of the Internet users has changed.
6. Computer science, being everywhere provides new dimensions to the Internet.
7. Our dependency of the Internet is increasing therefore it is more and more important to maintain the integrity of the network.
8. We have to pay more attention for security and threats to it, which appear in many new forms.

According to the first section, the functionality of the Internet can be experienced as the most significant change. In order to understand this section at first we must explain the meaning of the expression of the convergence, because this expression has no precise definition. In this article the definition of the ITB[1] was considered as a starting point. According to it, the expression of convergence is most generally used in the following sense:

- The convergence is the ability of various network platforms, which provide basically similar kinds of services or it is interweaving of consumer devices such as telephone, television and personal computer
- Perhaps the latter interpretation of convergence is cited most frequently in the press- it is easy to understand for the consumers; moreover it reflects the large scale struggle that exists among the trades of computer science, telecommunications and broadcasting for obtaining the control over the future markets [3].

On the basis of all these, the opinion of the OECD can not be accidental that the Internet Economy more and more is an integral part of the present-day, traditional economic and social infrastructure, so the ICT[2] policy should be considered as a determinant of the present trade-, labour- and financial policy. Considering all these the Internet is more and more essential and its sustainability has become the centre of global interest.

Hereafter let's examine the questions that the OECD deals with in connection with the future of the Internet and how are these questions linked with the factors mentioned in the Hungarian study above. The questions can be grouped in many ways, but it is clear that the main principle is the examination of the changes that promote economic development and social welfare from the point of view of the 'use' of the Internet.

[1] ITB=Informatikai Tárcaközi Bizottság=Inter-departmental Committee of Informatics
[2] ICT=információtechnológiai forradalom=revolution in the information technology

## MAIN ISSUES OF THE FUTURE [4]

The Internet is an economic and social infrastructure of crucial importance in global economic growth and social development. In this context every guiding principles is evolved with the aim of creating an environment which makes it possible to frame a homogeneous vision for the future which stride over national boundaries and political and personal communities protecting various interests. Such guiding principles are needed in the Internet economy in the next decade. Accordingly the OECD stands for that the national governments should consider the possibilities concerning business, technical collectivity, civil society and the social, economic and technological tendencies, which may form the development of the Internet Economy.

The Internet increases our ability to create, to work out figures, to communicate, moreover it is synchronized with other systems, and it carries out reforms and does away with obstacles, which limited a lot of economic and social activities in the past. Hereby new ways are made for increased productivity, reduced costs, and higher living standards, which were inconceivable a couple of years ago.

The Internet intensified creativity, which helps to produce new software-, and hardware products, sensor technologies by this means new ways can be made, global businesses can be done, new places of employment can be created. So, the question is that how can we encourage innovations, establishment of new co-operative models, which can foster the growth. It is necessary of course to make possible the maximal reach of the state sector information and contents. All these may upgrade the value of the electronic science in the innovation policy and in the OECD's innovation strategy.

As the Internet is becoming the main device and area of the economic and social activities, it immediately attracts frauds and malicious activities, which keep growing in size and refinement and threaten both the consumers and the users. Thus it is becoming a key question that by what means can be the safety of the critical information infrastructure insured and how can we fight against vicious softwares. Cooperation of many interested persons over national borders has begun for privacy, security and consumer protection. These can be interpreted in brief questions as follows:

- What did the governments accomplish in their structural reforms and what kind of priorities did they determine?
- What are the key factors that generate reform initiatives?
- What can be the role of the European establishments in the structural reforms?
- How can the national economy policy help the structural changes?

Defence of information is one of the most important questions, which can be corroborated with a recent example from the military scope. [5] The NATO is establishing a centre for defence of data stored or exchanged on computers and the Internet according to the agreement, which was signed by seven member states in Brussels. Experts and financial support for the new centre (Seat: Tallinn) will be provided by Estonia, Latvia, Lithuania, Italy, Spain, Germany and Slovakia. The United States has already showed intention to join for the cooperation and joining of other federal member states is expected too. The task of the centre will be to prevent penetration attempts and attacks against computers and networks and to act against the perpetrators.

The establishment of the centre shows that the NATO considers this kind of activity a more serious military and civil threat. Estonia was chosen because the computer systems of this Baltic state, its banks and the local media were unprecedentedly attacked in succession, last year. Estonia already suggested setting up this kind of agency many years ago. After the incidents of the last spring, the NATO sent information specialists to investigate the events.

The centre, with some 30 persons for the present will probably start the work in this summer, although its official initiation is planned by the next year.

The agreement was signed before the meeting of the chiefs of the general staff of the NATO member states in Brussels. On the two days' session the military tasks of Afghanistan and Kosovo were in the focus, but the cooperation with the Balkan states and the former member republics of the Soviet Union are on the agenda as well. The establishment of the computer centre was ratified by the prime ministers and the heads of the NATO member states at the beginning of April. It was already remarked at that time that joining to its work is voluntary.

Here are some of the main questions of the future, which are to be answered and can motivate us for further thinking.

1. Which are those unsettled questions which, after finding answers for them, can help the cooperation among the countries in the course of the realisation?
2. What were the main causes of the successful expansion of the Internet access recently and what kind of steps are necessary to continue this tendency in the developing countries?
3. Which political causes hinder development?
4. How can a correct ICT policy help the closing up of the developing countries' economy and society?
5. What can be the role of the cooperation over the boundaries in strengthening trust in the Internet Economy?
6. How can the consumers completely exploit the benefits of competing offers appearing on the online market?
7. How can the consumer protection be insured in the course of the commercial transactions on the Internet?
8. In what way can the profitable branches of industry be convinced of the advantages of the Internet Economy?
9. Are a structural change of the branches of industries and marketing strategy necessary after joining to the online trade?
10. How can the information of the state sector be utilized in introducing online trade?
11. What information can be made public by the governments on behalf of spreading the e-economy?
12. What kind of political decisions are necessary to help on creating a new generation of networks?
13. How can a homogenous law regulation be realized in national and international frameworks?
14. How can an international economic environment be built and co-ordinated, which provides competition, facilitates decision making processions, and is equally convenient for the consumer society?
15. What is the right balance between the public and the private investments?
16. Which area can get to a more advantageous position in providing services?
17. How can we enable the consumers to make advantage of changing in the communicational and information services?
18. What kind of factors should the Internet fit to in order to help to achieve economic and social aims?
19. What kind of conflicts can be arisen between the use of Internet and political activities of the governments, which may hamper its spread?

## THE ANSWERS OF THE OECD CONGRESS [6]

The above mentioned OECD congress looked for the answers for these questions too. Without claim of completeness, let‘s look over some answers, which can give opportunity for further reflecting too.

The OECD member states are jointly taking every effort to provide an access to ICT networks and services reachable from everywhere, which can make the participation in the Internet Economy possible. The further expansion of the Internet Economy will support the free flow of information, the freedom of speech, the defence of individual freedom. Besides, it can serve as means to treat global challenges too (e.g.: consequences of climatic change etc.). The main goal is that the Internet Economy should cover the whole range of the economic, social and cultural activities, and improve the quality of life with the support of the Internet and the connected informational and communicational technologies.

The security is a significant problem to be solved, which can diminish the users' worries concerning informational systems and networks. The participants on the congress encouraged and supported the more effective use of radio frequency spectrum, which can facilitate access to the Internet and the new innovative services. They also suggest the governments to accept the new version of Internet Protocols, the IPv6, which has the following characteristics.

The IPv6 is an Internet Layer protocol for packet-switched internetworks, which was designed to improve the Ipv4 (briefly IP). The IPv6 features a larger address space than that of IPv4: addresses in IPv6 are 128 bits long versus 32 bits in IPv4. The reason for this that the free IPv4-es titles will run out expectedly in the immediate future and it is not possible to hand out new IP addresses, and later on, could not be already long in this manner to join the system. Onto the solution of this problem it started being developed it IPv6 (the 5 version serves a totally other aim, the next version was because of that the 6). The IPv6 has several benefits compared to IPv4 apart from a much bigger address range. The IPv6 favours it on the one built into the protocol the multicast. Safety solutions are at his disposal, since it IPv6 the part of a protocol IPSec.

It is evident, that the OECD has found feasible answers for some problems of the Internet Economy, of which I mentioned only some. At the same time it is clear, that in the area of Internet Economy new problems to be solved arise every day, therefore solutions need everyday consultations among the experts of the member states.

## SUMMARY

Since our aim was only to draw attention to the use of the Internet, only some issues were mentioned related to it. We can explicitly state that in the future the Internet will play an important role in the development of economy and society as well. As a result of this the national and international participants of politics will pay distinguished attention to it. That's why the future role of the Internet is in the centre of interest of the OECD and NATO; and that is why providing the conditions that determine the further development of the Internet was discussed by the OECD on a ministerial conference in 2008.

One of the keys to the following success of the Internet is that – although the infrastructure of the Internet was built up, brought into action and developed by the business world, and the improvement of the services was initiated by the private sector- the national governments should also take actions on behalf of the further development. Accordingly it is important that the research activity of the new generation of the Internet should be supported by the governments and the EU too, since the system has more and more function and serves bigger and bigger part of the population of the world, development of new disciplines and technologies are necessary.

The next generation of the networks will have such a big velocity that provides large access for ‘everybody’ to informational services of science, health, environment and everyday life, thus raising social welfare too. Accordingly it is expected that research of the new generation Internet will remain one of the leading research topics in the military and civil life alike. As it is evident from the description of the new organization, the NATO and the Hungarian Defence Forces have also joined into this process, making possible immediate employment of the achieved results in many fields of the military life.

## REFERENCES


[1] http://www.szmm.gov.hu

[2] Péter Bakonyi - András György - Beatrix Tóth: The future of the internet (Study, http://www.nhit-it3.hu, 2007)

[3] ITB Green Books I. Chapter, I.1. Convergence - defining his extent

[4] http://www.oecd.org

[5] http://www.honvedelem.hu/

[6] http://www.oecdministerialseoul2008.org/en/

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Pándi Erik**
Zrínyi Miklós Nemzetvédelmi Egyetem
pandi.erik@zmne.hu

# A RENDŐRSÉGI INFORMÁCIÓTECHNOLÓGIAI SZERVEZET FEJLESZTÉSÉNEK NÉHÁNY KÉRDÉSE

***Absztrakt***

*A jelenlegi Rendőrség információtechnológiai szervezete a Rendőrség és Határőrség szakállományának összevonása révén jött létre folyó év január 1-jével. Az eddigi működési tapasztalatok az idő rövidsége miatt még nem engedik meg közép- és hosszútávú következtetések levonását, azonban a korábbi nyilvánvaló működési problémák, illetőleg a jelenlegi szervezeti struktúra kialakításának gyakorlata felvet néhány olyan kérdést, amelyek átgondolás nélkül történő elvetése nem segítheti elő a homogén, stabil szakmai alapokon álló IT ágazat tényleges kialakítását.*

*The current IT organisation of the Police has been established by merging the professional staff of the Police and the Border Guard at the 1st of January 2008. The operating experiences so far are too small to be able to draw any mid- and long-term consequences. However the earlier apparent operational problems and the practice of establishing the current organisational structure, raises a number of questions. Rejecting these questions without thinking them through would not promote the establishment of a homogeneous and professional IT sector.*

***Kulcsszavak**: információtechnológia, felkészítés, szervezetek, struktúrák ~ IT, training, organizations, structures*

## 1. A JELENLEGI INFORMÁCIÓTECHNOLÓGIAI SZERVEZET KIALAKULÁSA

A Magyar Köztársaság Rendőrségének integrált információtechnológiai (a továbbiakban: IT) szervezete (vagy ágazata) a jogelőd szerveknél működtetett szakszervek összevonása révén jött létre. A folyó év január 1-jén hatályba lépett, a Rendőrség Szolgálati Szabályzatáról szóló 62/2007. (XII.23.) IRM rendelet 2. § (5) bek. a) pontja szerint az *információ technológia* területe a gazdasági szakszolgálathoz kerül besorolásra. A jelenlegi szervezeti struktúra kialakításának gyakorlata felvet néhány problémás területet, amelyek lényegének megértéséhez célszerű áttekintetni a jogelőd szakszervek néhány jellemzőit.

### 1.1. A Rendőrség egykori IT ágazata

Az IT ágazat egykori felépítése elveinek tisztázására néhány korábbi szakmai anyag összességében korrekt felvilágosítást adhat [1], [2]. Az integráció során bekövetkezett

szervezeti változásokig a rendőrségi IT ágazat elvi felépítése többé-kevésbé a hetvenes évekre kialakult szervezeti struktúrát (szervezési koncepciót) őrizte meg. Ennek lényege a központosított szakirányítás, amely egyrészt a központi, valamint a területi és helyi rendőri szervek kommunikációs igényeit kiszolgáló szervezeti egységek tekintetében valósult meg.

Az 1990-es éveket megelőzően a szakirányító szerv a Belügyminisztérium egyik osztálya[1] volt, amelynek funkcióját a későbbiekben az ORFK-n megalakuló osztály, majd főosztály[2] látta el. A központi szervek kiszolgálását kezdetekben a szakirányító szerv végezte, majd a kilencvenes évek első harmadától a korábbi szakirányító szervből alakult üzemviteli szervezet[3] látta el. A területi és helyi rendőri szervek ellátását a megyei (fővárosi) rendőr-főkapitányságokon, valamint a különleges rendőri szerveknél[4] létrehozott szervezeti egységek[5] végezték. A központi szervek ellátási gyakorlatában – *lényegében* – 2003-tól újabb változások mentek végbe, amikor a Rendőrség legnagyobb üzemviteli szervezete a felügyeletet ellátó minisztérium háttérintézményeként működött, majd az integrációt megelőző egy évvel közigazgatási szervvé került átalakításra.[6] A szervezeti változások ellenére elmondható, hogy a legfőbb irányítási alapelvek több mint három évtizeden keresztül nem változtak, vélhetően többé-kevésbé sikeresen töltötték be funkcióikat, amelynek lényegét egy szakértő a következőképpen fogalmazza meg: [az] *„…irányítás célját legáltalánosabban a […] jogszerű működésnek átfogó és teljes körű biztosítása, továbbá a működéshez szükséges feltételekről való gondoskodás adja. Az irányítás lényege tehát az […] akaratérvényesítés a […] működés fölött."* [3].

A megfogalmazottakkal ellentétben, az IT ágazat tekintetében, a kilencvenes évektől kezdődően az akaratérvényesítés – *a korábbiakban megszokott gyakorlattól eltérően* – meggyengült, aminek egyenes következménye egy olyan – *napjainkra is jellemző* – vákuum, amelyre jellemző a teljes szabályozatlanság,[7] valamint az anyagi-pénzügyi erőforrások szükségesnél nagyobb mértékű dekoncentráltsága.[8] E két fő probléma lényegében az ágazat átlátható és a tervszerűségen alapuló célszerű működését teszi nehézkessé. A kialakult – *és napjainkra akuttá vált* – helyzet ok-okozati összefüggéseinek feltárása komplex és mélyreható vizsgálatokat igényelne, amelyre jelen publikáció keretei nem adnak lehetőséget, azonban néhány, a felszín közvetlen közelében rejtőzködő – *a felkészítéssel, a rendfokozati és beosztási rendszerrel is összefüggő* – problémára ezúton szeretnék röviden rávilágítani.

A kilencvenes évektől kezdődően hazánkban is megjelentek a korszerű távközlési és informatikai technológiák, illetőleg szolgáltatásaik, amelyek az idő előrehaladtával egyre inkább beépültek a rendőri tevékenységekbe oly módon, hogy azok eredményes végrehajtása napjainkban már elképzelhetetlen nélkülük, amely tényt a szakirodalom is megfelelően alátámaszt [4]. A korszerű eszközök és szolgáltatások térhódítása, a technológiai konvergencia ténye a globális gazdasági és társadalmi térség kialakulásával egyértelművé vált, e folyamatot az ezredfordulótól – *mint az előzőekben azt már láthattuk* – a magyar kormányzat sajátos jogi-szervezeti és anyagi-pénzügyi megoldásokkal erőteljesen támogatja.

---

[1] BM Anyagi-Pénzügyi-Technikai Főcsoportfőnökség Híradástechnikai Osztály (BM I/2. Osztály)

[2] néhány megnevezés: ORFK Híradástechnikai Iroda, ORFK GIF Anyagi-Technikai és Informatikai Főosztály, ORFK GF Információtechnológiai és Műszaki Főosztály, stb.

[3] ORFK GIF Híradástechnikai Szolgálat, illetőleg ORFK GF Híradástechnikai Szolgálat

[4] például: Köztársasági Őrezred, Készenléti Rendőrség, stb.

[5] a kilencvenes éveket megelőzően a főkapitány alárendeltségében működő alosztályokként, majd az elmúlt évtizedekben a gazdasági igazgató alárendeltségében működő osztályokként

[6] 2002. december 1-jén a BM Távközlési Főosztály és az ORFK GF Híradástechnikai Szolgálat bázisán, kettős (belügyi ágazati szakirányító és központi üzemeltető) funkcióval megalakult a BM Távközlési Szolgálat (BM TÁSz). A BM TÁSz a 276/2006. (XII.23.) Korm. rendelet révén, 2007. január 1-jén szűnt meg. Jogutódja a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

[7] a jogszerű működés átfogó és teljeskörű biztosítása

[8] a működéshez szükséges feltételekről való gondoskodás

A szakmai vezetés e kihívásra szervezetileg jól reagált, hiszen a hagyományos *„híradó”* kultúrára építkezve megalakította a *„híradó és informatikai”* szervezeti elemeket, amelynek keretében megindult a helyi szervekhez történő szakállomány kihelyezése is. Ugyanakkor, egyfajta elhibázott lépésként értékelhető, hogy a szakmai szervezetek belső tartalmának súlypontjaival kapcsolatos gyorsütemű átszervezések szükségességét viszonylag későn ismerte fel, szinte csak akkor, amikor a technológiai konvergencia beteljesedése már nyilvánvaló ténnyé vált. Ennek egyik oka talán az is lehet, hogy a változások időszaka során túlsúlyban voltak az átalakítások önálló kezdeményezéséért és végrehajtásáért felelős azon személyek, akiknek szakmai gyökerei, valamint szakmai szocializálódásuk környezete egyértelműen a hagyományos távközlésben voltak megtalálhatók.

A Rendőrség jelenleg is tapasztalható, hosszú évtizedekre visszanyúló sajátja, hogy a funkcionális tevékenységek ellátására tervszerű, egységes közép- és felsőfokú szak-, illetve felsőoktatási képzést nem szervez, utánpótlását a szervezetek önállóan, a fellépő lokális igényekhez és az adott időszakban, adott területen fennálló belső és külső körülményekhez igazítva hajtják végre. A helyzet a szakterületi tovább- és átképzések, illetőleg felsőoktatási beiskolázások terén is hasonló. Úgy tűnik, a Rendőrség hosszú évtizedek óta kimondatlan szabálynak tekinti azon eljárást, amely szerint a szakma kívánalmainak megfelelő iskolarendszerű képzés révén szakképzettséget szerzett szakállománynak a szakterületi jártasságot, majd készséget mindenekelőtt a beosztási helyen kell tudnia megszerezni. Ténykérdés azonban az, hogy az IT területe tekintetében, a gyakori technológiaváltás a tudásszint igen gyors elévüléséhez vezet, tehát ezen hallgatólagos gyakorlat fenntartása az ágazat eredményes működése szempontjából nem lehet előremutató.

Visszatérve korábbi fejtegetésemhez, mindenképpen elgondolkodtató, hogy a kilencvenes évek előtt minőségét és szervezettségét tekintve magasabb színvonalon álló „híradó szolgálat” utódja, a szervezetileg megújuló „híradó és informatikai szolgálat”, vagyis az IT ágazat jelenünkben is működési problémákkal küszködik. Fentiek révén úgy gondolom, hogy a közel két évtizede tapasztalható hullámzó, de ugyanakkor a korábbiakhoz mérten nagyarányúnak tekinthető – *és talán folyamatosnak tekinthető* – fluktuáció a többségében hagyományos elveken és eljárásokon nevelkedett vezetői állományt arra sarkalta, hogy a hiányzó, a megváltozó szakmai környezetbe eredményesen beilleszkedő humán erőforrásokat elsősorban a szervezeten kívülről pótolja. Ez a lépés egyúttal egyre sürgetőbb feladattá vált, hiszen az IT ágazat belső, időben történő, mélyebb strukturális átalakítása korábban elmaradt, vagy vontatottan haladt, azonban a rendőrszakmai és ezeken keresztül egyes közigazgatási feladatok korszerű informatikai és kommunikációs szolgáltatásokkal való támogatása tekintetében a rendőri felsővezetés egyre nyomasztóbb követelményeket támasztott az ágazati vezetőkkel szemben. A humán erőforrások pótlására több lehetőség adódott, egyrészt a társszervek állományából,[9] másrészt a polgári társadalomból, azonban mindenképpen elmondható, hogy e létszámkonjunktúra révén a korábban egységes elvek mentén szocializálódott „híradó szolgálat” – *a fogalom jó- és rossz értelmében egyaránt* – felhígult. Ennek egyik pozitív jele, hogy sok olyan új gondolat, gyakorlati tapasztalat és eljárás került a rendszerbe, amelyet alkotó módon lehetett felhasználni a mindennapi munkában, ugyanakkor negatívumként értékelhető, hogy a hagyományos és a szervezet egészének működése szempontjából is bevált gyakorlatok elsajátítására és átörökítésére sem elegendő idő, sem megfelelő kvalitású mentorállomány – *az idő előrehaladtával* – már nem állt rendelkezésre.

Mindenképpen szükséges néhány szót ejteni a szervezeten kívülről érkezett szakemberállományról és motivációiról, mivel e kérdéskör felveti az állománytáblával kapcsolatosan kialakult problémákat is. Köztudomásúak azon tények, amelyek egyrészről alátámasztják, hogy a polgári IT ágazat tekintetében napjainkban is inkább a munkaerő-

[9] itt lehetőség nyílt a Magyar Honvédség, valamint a Határőrség állományából történő átvételre egyaránt

kereslet a jellemző, másodrészről bizonyítják a vidéki és ezen belül a keleti megyék magas munkanélküliségi rátáit, harmadrészről nyilvánvalóvá teszik ezen ágazatban elérhető rendőri és polgári illetmények különbségét. Ezekből kiindulva elmondható, hogy a polgári életből érkezők Rendőrséggel szembeni elkötelezettsége és szakmai kvalitása – *vélhetően* – alacsonyabb, mint azon társaiknak, akiket a hazai, illetőleg nemzetközi üzleti szféra természetes úton „választott" ki. Számunkra ezen állománycsoportba sorolható munkavállalók jelentik azt a kategóriát, amelyek tudatos „szocializáció" nélkül – *még ha hivatásos állományba is kerülnek* – soha nem fognak azonosulni[10] sem az IT ágazattal, sem magával a szervezettel, amelynek egyik hosszútávú következménye lehet a szakmai diszkvalifikálódás. Ezzel ellentétben, a társszervektől érkező – *elsősorban hivatásos állományú* – munkavállalók szervezettel kapcsolatos – *karrierközpontú* – motiváltsága mindig is jóval magasabb volt, így esetükben, korábbi pályafutásuk révén mesterséges „szocializációs" folyamatra általában nincs szükség. E kategóriába tartozó munkavállalók szempontjából, sok esetben a karrierközpontúság jóval meghatározóbb, mint a szakmai motivációs tényezők, ami tudatos beavatkozás nélkül szintén egyfajta szakmai diszkvalifikálódáshoz vezethet akár anélkül, hogy az egyén ezt érzékelhetné.

Az egykori „híradó szolgálatra" is jellemző volt, hogy állománytábla szempontjából vegyes szervezeteket[11] hoztak létre, amelynek egyik fő szempontja volt, hogy a munkakörök egy elég széles rétegében a magasabb szintű kötődés[12] útján a szervezettel szembeni elkötelezettséget és ezzel a végrehajtás minőségét növeljék az érintett állományban. Általánosságban elmondható, hogy a kilencvenes éveket megelőzően az ágazatban az állománytáblák kialakítására az egységesség volt jellemző. Megítélésünk szerint, az integrációt megelőzően a Rendőrség IT ágazatában alkalmazott állománytábla az ágazat feladatával, tevékenységével, szervezetével, állományával és hatáskörével kapcsolatos részletes szabályozás hiánya miatt a múlt szokásjogára támaszkodva, a személyzeti hatáskört gyakorló illetékes vezető belátása és meggyőzése, valamint a rendelkezésre álló bérkeret, mint kényszer által kialakított helyzetet tükrözte vissza. A kialakult gyakorlat tehát a vonatkozó jogszabály, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény preambulumában foglaltakkal sem volt összhangban, hiszen lényegében nem volt tisztázott, hogy az IT ágazat mely tagjával kapcsolatosan várt „*az állam tántoríthatatlan hűséget, bátor helytállást […] a törvények és más jogszabályok, valamint a nemzetközi jog előírásainak megfelelően, a fegyveres szervek feladataihoz igazodó szakmai ismeretek birtokában…"* [5]. Ez különösen akkor lehetett gond, amikor – *hosszú évekre visszavezethetően, a gyakorlatban is bizonyítható módon* – két ugyanolyan felelősséggel és kötelezettséggel bíró munkakört két különböző besorolással, de azonos szakmai végzettséggel bíró munkavállaló látott el. A legszembetűnőbb kontrasztok vidéken alakulhattak ki, ahol példaként véve két különböző rendőrkapitányság állományában dolgozó rendszergazdát, az egyik már elvégzett egy főiskolát, így a megyei- és országos rendőrfőkapitány támogatásával a miniszter kinevezte tisztté, amíg a másik ugyanazon főiskola egy évvel fiatalabb hallgatójaként csak középfokú végzettsége szerinti közalkalmazotti besorolásban (és bérrel) látja el hasonló típusú és felelősségi körű feladatát.

A kilencvenes évek közepétől további nehézségeket jelentett a tiszthelyettesi állomány megszervezése, mivel az állományba való felvétel alapkövetelménye az egységes rendészeti tiszthelyettes-képzés rendszerében való szakképzettség megszerzése lett, amelyet az

[10] Megítélésünk szerint az azonosulás nem más, mint megismerni és elfogadni a szervezet erősségeit és gyengeségeit, az általa nyújtott előnyöket és okozott hátrányokat, megtanulni ezekkel pozitív módon együtt élni és ennek tudatában együttműködni az egyént körbevevő szűk közösséggel a szervezet pozitív irányú fejlődése érdekében

[11] Alapvetően: főtiszt, tiszt, zászlós, tiszthelyettes és kinevezett polgári alkalmazott

[12] És ezzel szélesebb kedvezmények, valamint magasabb illetmények

állományilletékes vezetők többnyire nem támogattak. A tiszthelyettesi beosztások többnyire a már rendészeti képesítést szerzett állomány átképzése révén kerültek feltöltésre, de összességében elmondható, hogy a problémakör kezelése a gordiuszi csomó mintája alapján történt, vagyis státuszok általában átminősítésre[13] kerültek. A tiszti állományba való felvétel különleges problémákat nem vetett fel, hiszen mind a társszervektől áthelyezéssel érkezők, mind a megfelelő főiskolai-, vagy egyetemi végzettséggel rendelkező, alkalmasság szempontjából megfelelő[14] köztisztviselők és közalkalmazottak az előírt szaktanfolyam elvégzését követően „képzett" rendőrtiszteknek minősültek. A hivatásos, köztisztviselői és közalkalmazotti státuszok kapcsán fennálló ellentmondások mellett sok esetben nem lehetett egységesnek tekinteni a középfokú és felsőfokú, valamint főiskolai és egyetemi végzettséghez kötött státuszok kialakításának gyakorlatát sem, amely egyes esetekben a fentiekben ismertetett problémákat vetette fel.

Mindezeket összefogva úgy ítélem meg, hogy a Rendőrség IT ágazata az integrációt megelőzően, személyi állományának jogviszonyát, azok felkészültségét és végzettségét, valamint korábbi szakmai pályafutását illetően heterogénnek, a korfa a dinamizmus kívánalmai szempontjából kedvezőnek tekinthető. Az állományt pozitív értelemben vett kozmopolitizmus, vagyis retrográd korlátok nélküli szakmai sokszínűség jellemzi. Az ágazat hátránya, hogy az elődök által felhalmozódott szakmai tapasztalat, ismeretanyag – *különböző okok miatt* – gyengén örökítődött át, ezért a szervezet által korábban már érdemben hasznosított és bevált gyakorlati eljárások újbóli alkalmazása nehézkesen, továbbfejlesztésük szinte alig realizálódik. Ennek okán az ágazat tevékenysége kevéssé tekinthető átláthatónak, koordináltnak és tervezhetőnek, vagyis amely probléma leginkább a szabályozás és az ehhez szervesen kapcsolódó szakirányítás kérdésköreiben jelentkezik.

## 1.2. A Határőrség egykori IT ágazata

Az egykori IT ágazat szemléltetésre néhány egykori szakmai anyag összességében megfelelő szintű felvilágosítást adhat [6], [7]. A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény módosításai révén visszavezetve, a Határőrség státuszában 2005. január 1-jén következett be – *a korábbiakhoz képest* – az első jelentősebb változás, amikor is megszűnt a fegyveres erőkben[15] betöltött státusza. Ettől kezdődően a szervezet alapvető feladata az államhatár őrzése és rendjének fenntartása lett [8]. Az integrációig fennmaradt három esztendőben a szervezet – *a Rendőrséghez hasonlóan* – hármas tagozódásban[16] működött. Az IT ágazat szervezetének átalakítására jóval korábban, már a kilencvenes évek közepén megtörtént, amikor a hagyományos „híradó szolgálat" „informatikai szolgálattá" való szervezése ténylegesen végrehajtásra került.

Az IT szakirányítás problematikája és érdemi megvalósítása a Határőrség tekintetében különösebb kérdéseket nem vetett fel, hiszen a teljes szervezet korábbi múltja[17] inkább volt militáns és így erőteljesen centralizált, mintsem kissé liberálisabb, közigazgatási vénájú. A szakállomány a három vezetési szint mindegyikén jelen volt.[18] Hasonlatosan a rendőri szervekhez, az IT állomány feletti munkáltató illetékesség gyakorlásában az ágazati vezetők

[13] többnyire közalkalmazotti státuszra
[14] fizikálisan és mentálisan egyaránt
[15] fegyveres erők: a Magyar Honvédség és a Magyar Köztársaság Határőrsége
[16] központi, területi és helyi szervek összessége. Az integráció során lényegében csak a helyi szervek, vagyis a határrendészeti kirendeltségek maradtak fenn változatlan szervezetben. E szervek Rendőrségbe való konkrét betagozására a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről szóló 329/2007. (XII.13.) Korm. rendelet alapján történt
[17] lényegében: 1947-től
[18] központi szinten: Informatikai Főosztály, területi (igazgatósági) szinten: Informatikai Osztály, helyi szinten: kirendeltségvezető-helyettes, vagy referens

nem vettek részt. A kilencvenes éveket követően az IT ágazat szabályozottsága – *ellentétben a Rendőrséggel* – továbbra is kimunkáltnak és begyakoroltnak volt tekinthető, amellyel párhuzamosan az anyagi-pénzügyi erőforrások alsóbb fokú szerveknél történő dekoncentrálása kisebb mértékben történt meg. Ezek alapján úgy ítélem meg, hogy a Határőrség IT ágazatának működése a szabályozottabb és kiegyensúlyozottabb jelzővel illethető, amely természetesen elgondolkodtató kijelentés is egyúttal. Tekintettel arra, hogy mind a Rendőrség, mind a Határőrség alapfeladata a legmagasabb szintű törvénytől kezdve – *a jog hierarchiáján keresztül* – a legalsóbb fokú normákig szabályozott volt, ezért a szakszolgálatok tevékenységei között tapasztalható minőségi különbségek véleményem szerint egyértelműen a személyi állomány felkészültségében és tevékenységének minőségében keresendők.

A Határőrség korábbi „híradó szolgálata" és „informatikai szolgálata" személyi állományának összetételét vizsgálva megállapíthatjuk, hogy a kilencvenes éveket megelőző időszakokban, a szervezet különleges helyzete miatt az arányok inkább voltak hasonlatosak a hadseregben alkalmazott megoldásokhoz, vagyis döntően hivatásos tiszti és tiszthelyettesi státuszok kerültek kialakításra, amelyek mellett, viszonylag szűk keretben – *többségében a kisegítő tevékenységek*[19] *körében* – megtalálhatók voltak a polgári státuszok is. A személyi állomány utánpótlása a tiszti állomány körében nem jelentett problémát, mivel azokat a katonai felsőoktatás rendszere – *az előre tervezett létszám szerint* – rendelkezésre bocsátotta [9]. A tiszthelyettesi állomány utánpótlása jellemzően a sorállományból történt.

Az „informatikai szolgálattá" történő átszervezés időszakában a Határőrségnél már megindultak azon folyamatok, amely a rendészeti szervvé történő átalakuláshoz vezettek. Ennek keretében a sorállományú határőrök létszáma folyamatosan csökkent, majd megszűnt, így a testület gerincét egyre inkább alkotó tiszthelyettesi állomány szerepe felértékelődött. A belügyi ágazatban egységesülő tiszthelyettes szakképzés[20] révén a kilencvenes évek második felétől ezen állománykategóriába már csak a rendészeti szakközépiskolák elvégzését követően lehetett kerülni. A rendészeti szakközépiskolákban a szervezetek alaptevékenységi körén túlmutató feladatokra, vagyis szakszolgálati feladatokra szakképzés nem folyt és nem folyik, vagyis az „informatikai szolgálat" ezirányú szükségleteit e forrásból megoldani nem volt képes. A probléma megoldását jelentette egyrészt az erre alkalmas, képesített (kiképzett) határőr tiszthelyettes Határőrségen kívüli tanfolyami átképzése, másodrészt a polgári státuszra felvett közalkalmazott, köztisztviselő rendészeti szakközépiskolában, munka mellett megvalósuló szakképzése, majd tiszthelyettessé való kinevezése. A középfokú végzettséghez kötött munkakörök betöltését az „informatikai szolgálat" fentieken túl, egyre bővülő létszámban oldotta meg köztisztviselői és közalkalmazotti státuszra, polgári életből való, megfelelő szakképzettséggel rendelkező állomány felvételével.

Az „informatikai szolgálat" megszervezésével és az IT, mint szakma előretörésével a tiszti állomány utánpótlásának gyakorlata kétség kívül megváltozott. A katonai felsőoktatásból érkezők[21] aránya csökkent, amíg nőtt azoknak tiszthelyetteseknek, közalkalmazottaknak és köztisztviselőknek a száma, akik a megfelelő szakképzettség megszerzését és a tiszti kinevezéshez szükséges rendészeti szaktanfolyam elvégzését követően hivatásos tiszti állományba lehetett venni.

A Határőrség esetében is érzékelhető, hogy a szakma belső tartalmának megváltozása az IT ágazat vezetői számára elég komoly kihívásokat jelentett, hiszen a különböző információs

[19] ennek keretében jellemzően anyagi-technikai-pénzügyi segédtevékenységekről van szó

[20] a kezdetben különálló határrendészeti és rendészeti szakközépiskolák évtizedünk közepén folyamatosan összevonásra (integrálásra) kerültek, amellyel párhuzamosan számuk is redukálódott

[21] míg korábban a beiskolázásra kerülők a hagyományos híradó szakokon folytatták tanulmányaikat, addig a kilencvenes évek végétől mindinkább az igényeket jobban kielégítő informatikai szakokon történt a képzés

és kommunikációs rendszerek modernizálása[22] nem elsősorban belülről fakadó szervezeti igényként jelentkezett, így e terület a nemzetközi érintettség okán mind szakmailag, mind politikailag exponálttá vált [10]. A szakmai vezetés a vele szemben támasztott követelményeknek lényegében sikeresen megfelelt, ezért felmerül a kérdés, hogy a Határőrség „informatikai szolgálata" látszólag miért tűnt sikeresebbnek?

A kérdésre egyrészről már válaszoltam, hiszen utaltam arra, hogy a múltból fakadó gyökerek okán a szakirányítási eljárás gyakorlatban való megvalósulása, valamint az anyagi-pénzügyi források központosítottabb felhasználása eredményesebb volt. A szakállomány ugyancsak „felhígult", hiszen a korábban rendelkezésre álló iskolarendszerből a szakmai igények kielégítése nem volt megoldható, így hasonlóan a rendőrségi gyakorlathoz az IT ágazat vezetői merítettek a polgári élet kínálta lehetőségekből. Ténykérdés egyrészről, hogy a szakirányítás elemeinek konzekvens alkalmazása révén a szakmai vezetők az állományilletékes parancsnokoknál érvényre tudták juttatni az általuk kialakított és széles körben elfogadott szakmai elveket, amelynek egyik része volt az egységes elvekre épülő, homogén állományszervezés. Másrészről szintén ténykérdés, hogy a Határőrség szervezete folyamatosan csökkent, az integráció előtt létszáma már csak alig volt egyharmada a Rendőrség létszámának, amely egyebek iránt megmutatkozott a feladatkörök szélességében is. E körülmények között nyilvánvaló, hogy időben több lehetőség adódott egyrészt az egyéni szakképzések támogatására, valamint a teljes IT ágazat szakmai közösségének rendszeres és együttes továbbképzésére, amely egyúttal jó táptalaja volt az állomány szervezeti érdekeknek megfelelő „szocializálására" is. Felmerül a képzési és átképzési költségek problematikája, azonban a Határőrségnél általánosan elfogadott elv volt, hogy a szakmai jártasságok kialakítását és a készségek elsajátítását nem csak a beosztási helyen eltöltött szakmai gyakorlat révén kell végrehajtani, hanem azt mind közösségi, mind egyéni formában segíteni szükséges, így a költségtervezés mindenképpen tudatos és előrelátó tevékenységként jelentkezett.

Mindezeket összefoglalva elmondható, hogy az IT ágazatot illetően kódexszerű, belső norma a Határőrség esetében sem létezett. Az egyéb működési okmányokban rögzített, a szervezetben íratlanul elfogadott magatartási formákra (hagyományokra) épülő egységes gyakorlat, valamint a tudatos és kevésbé tudatos „szocializációs" eljárások a más rendészeti szervek szakállományától képességek szempontjából gyökeresen nem eltérő személyi állományt azonban a szervezettel azonosulni tudó közösséggé formálták. Talán kijelenthető, hogy a Határőrség „informatikai szolgálatát" képezők nagy többsége – *akarva, akaratlanul* – elsajátította az **egy nyelven való beszéd, beszélgetés** képességét.

## 1.3. A jelenlegi, integrált IT ágazat

Az Alkotmány, illetőleg a Rendőrségről szóló 1994. évi XXXIV. törvény módosítása révén 2008. január 1-jén megszűnt a Magyar Köztársaság Határőrsége. A szervezet jogutódjaként a Magyar Köztársaság Rendőrsége került kijelölésre, amelynek belső struktúrája módosításra került oly módon, hogy a határvédelmi és -rendészeti funkciók továbbra is zökkenőmentesen legyenek elláthatók. Ennek egyik folyományaként a Rendőrségi gazdasági szakszolgálatában és ezen belül az IT ágazatban is szervezeti rekonstrukciók kerültek végrehajtásra.

Ahogyan azt az előző fejezetben már érintettük, az IT ágazat a gazdasági szakszolgálatba tagozódik. A szakállomány továbbra is mindhárom szinten jelen van. A szakirányítás és a végrehajtás struktúrájában – *tekintettel a gazdasági szakszolgálat átalakítására* – a területi szinteken következtek be jelentősebb változások. A megyei rendőr-főkapitányságokon szervezett híradó és informatikai osztályok, valamint a határőr igazgatóságokon funkcionált

[22] legismertebb: a SIS rendszerhez való csatlakozás hazai műszaki-technikai és szervezeti hátterének kialakítása

informatikai osztályok a régiós illetékességi körökre kialakított gazdasági ellátó igazgatóságok hatáskörébe kerültek. Az igazgatóságok keretében regionális IT osztályok alakultak, amelyek azonban közvetlenül nem vezetik a megyei rendőr-főkapitányságok gazdasági osztályain[23] létrehozott IT csoportokat, azok szempontjából csak szakirányítást gyakorolnak.[24] E szervezési megoldás alól többek között a Köztársasági Őrezred, a Budapesti Rendőr-főkapitányság, a Pest Megyei Rendőr-főkapitányság és a Készenléti Rendőrség[25] is mentesült, amely szerveknél a korábbi szakmai struktúra[26] fennmaradt, egyúttal esetükben a Központi Gazdasági Ellátó Igazgatóság IT szerve szakirányítást nem gyakorol. Központi szinten, az ORFK Gazdasági Főigazgatóság szervezetében IT főosztály került kialakításra, amelynek keretében szakterületi osztályok kezdték meg működésüket.[27] Az IT főosztály egyúttal ellátja a Rendőrség központi szerveit, valamint működteti és menedzseli a központi IT szolgáltatásokat.[28]

Az állománytábla kialakításánál a központi IT főosztály, valamint a regionális gazdasági ellátó igazgatóságok esetében a köztisztviselői és közalkalmazotti státuszok kerültek jelentős túlsúlyba,[29] vagyis mind a Rendőrségtől, mind a Határőrségtől érkezett hivatásos szakállomány eltérő státuszon kerül alkalmazásra. A helyi szervek esetében a korábbi gyakorlat fennmaradt. Ténykérdésnek kell azonban tekinteni egyrészt azt, hogy az integráció során a személyi állomány egy része kihasználta a nyugállományba vonulás kedvező lehetőségét, másrészt a hivatásos jogviszony rövid- és hosszútávú féltése miatt az állomány egy másik része szakmaváltást[30] hajtott végre, harmadrészt, saját elhatározása révén távozott a szolgálatból. Az integráció során többnyire befogadásról lehet beszélni, ugyanakkor mind a Rendőrség, mind a Határőrség területi IT szerveinél hivatásos szolgálatot teljesítők számára az alkalmazott szervezeti megoldások és az alkalmazási feltételek egyaránt újszerűen hatottak, a korábbi körülményeikhez, elképzeléseikhez képest merőben más jövőképet vázolnak fel.

Összességében véve, a Rendőrség IT ágazatának személyi állománya, valamint szervezési megoldásai jelenleg heterogénnek tekinthetők. Az ágazatban megvalósult szervezeti rekonstrukciók újszerűen hatnak, elsősorban a területi szerveknél szolgálatot teljesítők körében. A kialakított struktúra alapvetően alkalmas a szakfeladatok ellátására, azonban az eltelt rövid időszak miatt jelenleg még nincs lehetőség sem az előnyök, sem a hátrányok korrekt, messzemenő eredményeket felvonultató értékelésére, elemzésére.

## 2. FEJLESZTÉSI IRÁNYOK

A Rendőrség az IT igazgatást – *hallgatólagosan* – a következőképpen definiálja: az információ gyűjtését, tárolását, visszakeresését, terjesztését és biztonságos továbbítását szolgáló optimális módszerek, eszközök és rendszerek kifejlesztésének (megvalósításának) hatékony elősegítése tervező, előkészítő, szervező, rendelkező és adminisztrációs

[23] a megyei rendőr-főkapitányságok gazdasági osztályai szintén a regionális gazdasági ellátó igazgatóságok szervezetében kerültek megszervezésre

[24] a mostani szervezési helyzet némi bizonytalanságot okoz a helyi szervek számára, hiszen néhány esetben nem tisztázott kellőképpen, hogy a megyei IT csoport, vagy a regionális IT osztály gyakorol-e szakirányítást

[25] a Készenléti Rendőrség esetében az IT szervezet nem a gazdasági igazgatóság szervezetébe, hanem a fő szakmai tevékenységet jelentő bevetési ágazatba került integrálásra

[26] mindegyik szervezet esetében speciális megoldásokat alkalmaztak korábban is

[27] az osztályok mennyisége növekedett, a szakterületi beosztás a szakmai elveknek megfelelően került meghatározásra

[28] elsősorban: adatbázisok

[29] az alkalmazott megoldás megfelel az úgynevezett „civilesítés” követelményeinek, amelynek lényege, hogy a nem alapfeladatot ellátó, vagyis funkcionális területen szolgálatot teljesítő állomány nem sorolható be az 1996. évi XLIII. tv. hatálya alá. Besorolásukra vagy közalkalmazottként, vagy köztisztviselőként kerülhet sor

[30] amelyet a tiszti, vagy tiszthelyettesi kinevezéshez szükséges szakmai végzettség tett lehetővé

tevékenységgel.[31] A Rendőrség integrált IT ágazatának – *az alaptevékenységek eredményes támogatása érdekében* – a jövőben tehát úgy kellene célszerűen működnie, hogy az egyrészt a gyakorlatban megoldja az információ gyűjtését, tárolását, visszakeresését, terjesztését és biztonságos továbbítását, másrészt tervező, előkészítő, szervező, rendelkező és adminisztrációs tevékenységgel hatékonyan segítse mindezen funkciók megvalósítását szolgáló optimális módszerek, eszközök és rendszerek kialakítását, kifejlesztését.

Látszik, hogy az *elmélet* komplex probléma elé állítja az ágazat vezetését, hiszen ezen feladatoknak (elvárásoknak) való magas szintű megfelelés elérésének és fenntartásának gyakorlati kivitelezése igen bonyolult és egyúttal jól átgondolt megoldásokat igényel. Nem lehet elég sokszor hangoztatni azon elvet, amely szerint [az] *„elmúlt évtizedekben a számítástechnika alapú rendszerek általánossá és meghatározóvá váltak a személyes felhasználásban éppúgy, mint az állam működésében. A közigazgatás, a rendvédelem, a honvédelem ma már elképzelhetetlen információs technológia nélkül, az adatok gyűjtése, továbbítása, tárolása, felhasználása, az eljárások és módszerek alkalmazása nélkülözhetetlenné vált működésükben."* [11]. Úgy ítélem meg, hogy az integrált Rendőrség kialakítása rendkívül jó lehetőség arra, hogy a korábbi erősségekből és gyengeségekből, valamint az elméleti megalapozásból kiindulva, illetőleg más pozitív gyakorlati tapasztalatra építve jelen fejezetben – *kizárólag vitaindítás gyanánt* – néhány lehetséges, esetlegesen célszerűnek mutatkozó fejlesztési irányra felhívjam a figyelmet. Mindezt teszem annak érdekében, hogy a magam módján elősegítsem az IT ágazatra nehezedő és egyre fokozódó belső és külső elvárásoknak – *az objektív korlátok által behatárolt mozgástér keretein belül* – történő minél magasabb szintű megfelelést.

## 2.1. A szabályozottság kérdéskörei

Az ágazat által végzett tevékenységeket többé már nem lehet *lokális* jelzővel és lokális módon kezelni. A Rendőrség életében napjainkra *globális* szinten vált meghatározóvá[32] az IT, amely szerepkört maga a kormányzat is folyamatosan erősít mind az egyén, mind a szervezetek szintjén. A lokálisból a globális minőség felé való egyértelmű haladás miatt megítélésem szerint hosszútávon már nehezen tartható fenn az a gyakorlat, amely mind az üzemviteli,[33] mind az irányítói (szakirányító)[34] tevékenység során előnyt, illetve igen tág teret biztosít a tapasztalati úton való és egyéni megítélés szerint történő végrehajtásnak. Természetesen megkövetelhető a személyi állománytól, hogy szakmája tekintetében ismerje a vonatkozó előírásokat,[35] azonban az ágazatban – *mint ahogyan azt az előző fejezetekben már bemutattam* – a konzekvens szabályozás, mind állami, mind szervezeti szinten hiányosnak tekinthető. A hiányosság mellett elmondható, a meglevő előírások sok esetben az érintett, vagy érintetté váló személyi állomány számára nem elérhetők.[36]

Miután az IT-nek az alaptevékenység szempontjából egyrészről támogató, illetőleg kiszolgáló funkciói is vannak, ezért a területet interdiszciplinárisnak is tekinthetjük, ami

[31] a Rendészeti Szakvizsga Bizottság Műszaki-Technikai és Informatikai Albizottsága által szerkesztett tananyag szerint

[32] példának okáért gondolhatunk itt a „Robotzsaru"-ra, vagy a határregisztrációs rendszerekre

[33] információ gyűjtése, tárolása, visszakeresése, terjesztése, biztonságos továbbítása

[34] tervező, előkészítő, szervező, rendelkező, adminisztratív

[35] szabványok, jogi normák és jogszabályok

[36] példának okáért egyes szabványokhoz való hozzáférés néhány esetben csak anyagi ellentételezés mellett lehetséges, vagy megemlíthető, hogy egy területi szerv kiadmányozásra jogosult vezetője által kiadott normatív szabályozás más illetékességi területen működő területi vagy helyi szerv, de akár a központi szerv számára nem válik automatikusan ismertté. Ilyenek lehetnek: ügyrendek, szervezeti és működési szabályzatok, intézkedések, utasítások

ugyancsak problémaforrásokat generál [12]. Sok esetben[37] az alaptevékenységet szabályozó normatív háttér olyan széleskörű,[38] hogy egyszerűen nem várható el a személyi állomány egyes tagjától a mélyebb összefüggések önálló felismerése, illetőleg a levont konzekvenciák alapján az elvek gyakorlatba való beépítése, holott több esetben ezen ismeretek hiánya szakmai tevékenységének minőségét, illetőleg megítélését jelentősen befolyásolja. E témakörökben további konfliktusokat lehet előidézni azzal, ha egy problémára – *az egymás információitól való elszigeteltség miatt* – több, esetlegesen rossz megoldás születik és épül be a gyakorlatba. Természetesen nem azt kívánjuk ezzel sugallni, hogy nincs helye egyéni, önálló kezdeményezésnek és kreatív tevékenységnek, hanem inkább arra kívánunk rámutatni, hogy a helyes megoldások intézményesítése, bevált gyakorlattá alakítása jelentheti az IT ágazat és ezzel a szervezet elsőszámú érdekét.

Mindezek alapján javaslom egy olyan keretszabályozás, avagy **kódex** kidolgozását, amely moduláris felépítése révén, a változó igényeknek megfelelően rugalmasan változtatható, azaz szűkíthető, bővíthető, átdolgozható. E kódex általános célja tehát egy olyan átfogó, **komplex ismeretanyag** és ehhez köthető **részszabályozások** összefoglalása és közreadása, amelynek kiadmányozásával többek között:

- megteremthető az IT ágazat identitástudata;
- megismerhetők az ágazat aktuális stratégiai céljai;
- iránymutatás adható a követendő szakmai alapelvekről;
- rögzíthetők az ágazat szervezeti és működési alapelvei;
- meghatározhatók az ágazati párbeszéd formái, keretei;
- lefektethetők az egyénre és szervezetre vonatkozó minőségbiztosítási alapelvek;
- kialakíthatók az egyén szakmai és beosztásban történő előmenetelének alapelvei;
- áttekinthetők az érdekvédelem alapkérdései;
- egybefoghatók a vonatkozó szabályozások, alkalmazásuk alapelveinek magyarázatai.

Kétségtelen ugyanakkor, hogy a kódex összeállítása egyrészről hosszabb időt igényel, másrészről az ágazat részéről széles támogatottságot. A fentiekben felvázolt témakörök részletes kifejtése jelen publikáció kereteit sajnálatosan mindenképpen meghaladja, ezért – *a kódexhez szervesen kapcsolódva* – néhány, általam relevánsnak tartott kérdéskörre kívánok a továbbiakban kitérni.

## 2.2. Részterületek

Kiragadva az ismertetett részterületek közül a *szakmai alapelvek*, valamint a *szervezeti és működési alapelvek* kérdéskörét az alábbiakban szeretnék néhány problémára rávilágítani, illetőleg azok megoldására egyfajta javaslatokat adni.

### 2.2.1. Szakmai alapelvek köre

A Rendőrség alapfeladata igen sokrétűvé vált, így a polgári jellegű közigazgatási feladatoktól kezdődően a félkatonai jellegű csapaterős feladatokig bezárólag a rendészeti tevékenységi körök széles palettájával és ezek megoldására létrehozott szervekkel találkozhatunk az integrált szervezetben. Mint azt már korábban megállapítottam, a központi szervektől a helyi szervekig mindenhol megtalálható az IT szakállománya, vagy szakszerve.

A szakmai alapelvek felvázolása során, megítélésem szerint szükséges lenne pontosan *felmérni* és *kategorizálni* az egyes rendőri szerveknél megjelenő IT feladatokat, meghatározni az ellátáshoz szükséges szakállomány kvantitatív és kvalitatív mutatóit. A kvalitatív mutatók

[37] például: adatvédelem, információbiztonság, stb.
[38] akár mennyiségét, akár bonyolultságát tekintve

esetében egzakt módon meg kell határozni a szakmai felkészültség elégséges színvonalát, vagyis azt, hogy az állomány milyen konkrét végzettséggel rendelkezzen. Ennek kidolgozását elsősorban azért ítélem fontosnak, mert – *szintén hivatkozva a korábbiakra* – az ágazat tekintetében nem beszélhetünk egységes alapelveket magába foglaló felkészítési rendszerről.[39] A mennyiségi és minőségi felmérést követően vizsgálni kell a rendőri szerv alaptevékenységének jellegét, hiszen csak ennek ismeretében lehetséges meghatározni az alkalmazandó állományviszonyt. Nézőpontom szerint nagyon durva megközelítés azon elvnek az alkalmazása, amely szerint a funkcionális tevékenységet ellátók nem lehetnek a Rendőrség hivatásos állományú tagjai.[40]

Ezen információk birtokában az IT ágazatra jellemző beosztások már kategorizálhatókká válnak. Célszerű csoportosításnak tűnik a közép- és felsőfokú végzettségű, valamint a főiskolai és egyetemi végzettségű halmazok kialakítása, amelyeken belül műszaki-üzemviteli és adminisztratív-irányítói részhalmazokat érdemes alakítani. Az *egy nyelven való beszélgetés* képességének kialakítása érdekében a négy alapkategória számára kompetenciaszinteket kell kidolgozni, amelyeket értelemszerűen a fejlődéssel párhuzamosan alakítani, módosítani kell. Természetesen a kategóriák száma bővíthető, ugyanakkor látni kell, hogy kezdetben a megfelelő kompetenciák tartalmának kidolgozása is igen időigényes tevékenység. A kompetenciaszintek és kompetenciák meghatározását követően átgondolhatóvá válnak a teljesítésükre irányuló megoldások is. A szakmai kompetenciák kidolgozására megítélésem szerint az IT ágazat tagjaiból álló testület hivatott, amelynek munkáját külső szakértők[41] is segíthetik. Az irányvonalak[42] kialakítását és az aktualizálási feladatok végrehajtását is e grémium látná el. A kompetenciákat kezdetben úgy célszerű meghatározni, illetőleg felvázolni, hogy azok teljesítése elméleti felkészülést igényeljen [13].

A következő, a kompetenciák teljesítésére szolgáló szükségszerű lépés a differenciált ismeretanyag összeállítása és annak eldöntése, hogy milyen módon, módszerrel sajátítható el, illetve ellenőrizhető vissza a teljesülés a leghatékonyabban. Alkalmazható a klasszikus módszer, vagyis az ismeretanyag mennyiségének és bonyolultsági fokának függvényében, elsősorban kislétszámú, csoportos foglalkozás keretében megismertetni a tananyagot, majd meghatározott időtartamú egyéni felkészülést követően írásbeli és/vagy szóbeli visszaellenőrzést végrehajtani. Modernebb megoldásnak tekinthető a multifunkcionális, multimédia elemeket tartalmazó mobil elérésű távoktatási tananyag egyéni elsajátíttatása, majd visszaellenőrzése [14]. Ez esetben az ellenőrzés szintén történhet korszerűen, vagyis az elektronikus rendszeren keresztül, de ez esetben a vizsgáztatóknak le kell mondaniuk az orális számonkérés lehetőségéről. A távoktatás alkalmazása költségkímélőbb megoldás, de ugyanakkor a személyes kontaktus hiánya miatt az állomány ágazat kívánalmainak megfelelő „szocializációja", mint egyik elérendő fő célt nem szolgálja kellőképpen. Az ismeretanyag kidolgozásában, az oktatási módszer eldöntésében, illetőleg a végrehajtásban természetesen igénybe vehető az Igazságügyi és Rendészeti Minisztérium, illetőleg a Honvédelmi Minisztérium felügyelete alatt működő oktatási intézményrendszer, mint szakmai bázis.

Külön kérdéskörként kell kezelni az iskolarendszerű szakképzést, valamint a főiskolai és egyetemi képzést. Megítélésem szerint minden esetben meg kell ismertetni az IT ágazat által

[39] sem középfokú, sem felsőfokú, sem főiskolai, illetve egyetemi szintű

[40] a legeklatánsabb példája ennek a Készenléti Rendőrség, ahol a szakállomány a rendőri műveletek során az irányító törzzsel együtt, azt kiszolgálva tevékenykedik

[41] külső szakértők lehetnek a katonai- és rendvédelmi felsőoktatásban, a rendészeti szakközépiskolákban, illetőleg közigazgatási, tudományos, társadalmi, vagy vállalatok elismert szakértői, munkatársai

[42] fontos annak eldöntése és rögzítése, hogy az egyéni kompetenciák felülvizsgálata milyen időközönként történjen, hiszen az egyes beosztási kategóriák esetében az ismeretanyag megújítására és aktualizálására eltérő időben van szükség éppen jellegük miatt

preferált intézményeket és programokat az e képzési formába belépni[43] kívánó állománykategóriával annak érdekében, hogy a szakmai egyenszilárdság hosszútávon is biztosítható legyen. Az ajánlások összeállításánál tekintettel kell lenni a lokális, valamint a támogatási lehetőségekre egyaránt.

Mindezen feladatok hatékony koordinálása és irányítása érdekében, az IT ágazat központi szervének kezelésében, a személyiségi jogokkal összhangban levő személyügyi adatbázist kell felállítani. Ugyanakkor konszenzus révén dolgozandók ki az IT ágazatban bevezetendő kompetenciarendszerrel kapcsolatosan alkalmazható ösztönző, illetve szankcionáló elvek. Egy megoldásként alkalmazható lehet olyan szabályozás bevezetése, amely lehetővé teszi, hogy a szakállomány minősítésére jogosult illetékes vezető számára legyen kötelező figyelembe venni a kompetencia teljesítését, avagy sikertelen megfelelést igazoló IT testületi határozatot.

A szakmai alapelvek körénél szükségszerűnek tartom megemlíteni, hogy az IT ágazatban megindult a hivatásos állománykategória visszaszorítására, illetőleg megszüntetésére irányuló törekvések egyúttal azt is jelentik, hogy az ágazat – *az érintett állomány megszűnése révén* – véglegesen kiszorulhat mind a rendészeti szakvizsga, mind a rendészeti vezető- és mestervezető-képzés rendszeréből, amely jelenleg az egyetlen intézményesített, továbbképzésre irányuló szisztéma. Ennek okán mindenképpen megfontolandónak tartom a kompetenciaalapú rendszer ágazati működési rendbe történő beillesztését és elterjesztését.

Az ismertetett elképzelés megvalósításához, azaz a részterület kialakításához belső szabályozás, vélhetően miniszteri, vagy ORFK vezetői utasítás kiadmányozására van szükség. Ezen norma természetesen részét képezné az IT ágazat szakmai kódexének.

### 2.2.2. Szervezeti és működési alapelvek köre

Az ágazat sajátja, hogy a mindhárom szinten, egyes, illetve szervezetben működő szakállomány állományilletékes vezetője nem IT szakmai vezető, vagyis *közvetlen szakmai vezetés* megvalósulásáról lényegében nem beszélhetünk. Ez a gyakorlat más rendvédelmi szervnél is hasonló, tehát a szakmai munka minőségét elvi síkon nem befolyásolja. Mint azt a korábbiakban, a szakmai irányítás (szakirányítás) kapcsán azonban már rögzítettem, úgy tűnik, hogy normatív szabályozás híján e terület a Rendőrség esetében lényegében „szokásjog” alapján működik, minden félreérthetetlen előnyével és hátrányával.

A szakmai irányítás témakörének újragondolása, illetve rendezése egyúttal elősegítheti az előző alfejezetben felvázolt modell megvalósítását és működtetését. Nézőpontom szerint a szakmai elvek mind szélesebb körű érvényre juttatása érdekében lehetőséget kell biztosítani az IT ágazat vezetése számára, hogy az egyes rendőri szervek esetében véleményezési és egyetértési jogot szerezhessen az alábbi területeken:

- az IT szakfeladatok beazonosítása;
- az IT szakfeladatokkal kapcsolatos szabályozás;
- a szükséges szakállomány létszámának meghatározása;
- a szakállomány képzettségi követelményének meghatározása;
- az egyes szakközeg kinevezése, elbocsátása;
- az állományviszony beazonosítása;
- az IT szakterülethez kötődő, de nem az ágazat által szervezett szakmai közép- és felsőfokú szakképzés, főiskolai és egyetemi képzés;
- az egyes szakközeg teljesítményértékelése, minősítése.

Fenti feladatok helyi és egyes területi szerveknél történő végrehajtása az IT ágazat központi, illetve területi (regionális) szintjén működő irányító szervek között természetesen

[43] ebben az esetben többnyire a saját elhatározás alapján, államilag elismert, magasabb szakmai végzettség megszerzésére irányuló tevékenységről van szó

megoszthatók, azonban az előző alfejezetben említettek okán célszerű, hogy a végrehajtással kapcsolatosan keletkező adatok és információk tárolása a központi szinten létesített adatbázisokban történjen.

Az IT ágazat személyi állománya kapcsán fentiek szerint kialakítható szorosabb kötődés, illetve felügyelet (irányítás) mellett megítélésem szerint célszerű javítani a technikai működés egységét és egységességét biztosító témakörökkel összefüggő működési gyakorlatot. Erre elsősorban a rendszerszemléletű gondolkodás erősítése okán van szükség, hiszen e tevékenység *„…nem csak (nem is elsősorban) a meglevő rendszerek részekre (végső soron elemekre) bontásához, az elemek rendszerezéséhez, a rendszer belső és külső kapcsolatainak feltárásához, a sokféle vizsgálati szempont (tudományközi együttműködés) lehetőségeinek és szükségességének felismeréséhez szükséges, hanem ahhoz, hogy meglevő elemekből az új igényeknek megfelelő és a környezettel összhangban levő rendszereket tudjunk összeállítani. […] A meglevő rendszerek működtetése – valamilyen meghatározott szempont szerint – optimális üzemviszonyok között szükségessé teszi egyes részek megújítását, esetleges cseréjét. […] A társadalom fejlődése miatt nemcsak a rendszer működésével szembeni követelményértékek, hanem még a – már többször említett – biztonsági tartomány is változik. A „változatlan” technikai rendszer általában – a környezet szakadatlan változása miatt – elavul, használhatatlanná válik, tehát: relative visszafejlődik. […] A rendszerelemzés következtetései – mindezek miatt – nem egyszeriek, örökérvényűek, hanem olyanok, amelyeket időszakonként felülvizsgálni, a környezeti feltételek változása és a rendszer egyes részeinek (erkölcsi és anyagi) kopása miatt módosítani kell.”* [15]. Ez összességében azt jelenti, hogy még a meglevő rendszerek működtetése is szükségessé teszi az állandó megújítást, a részek cseréjét, a használati mód fejlesztését, illetve új rendszerek létrehozását, amely országos rendszerek esetében mindenképpen szabályozott üzemviteli tevékenységet feltételez. Javaslom tehát olyan, az előzőekben ismertetett műszaki jellegű tevékenységekhez köthető szabályozási keretrendszer kidolgozásának megindítását, amely révén az ország bármely rendőri szervezete részére egyértelmű viszonyokat teremthet a működtetés és fejlesztés terén.

Az ismertetett elképzelések megvalósításához, azaz az újabb részterület kialakításához belső szabályozás, vélhetően szintén miniszteri, vagy ORFK vezetői utasítások kiadmányozására van szükség. A kidolgozásra kerülő normák – *hasonlatosan az előzőekhez* – részét képeznék az IT ágazat szakmai kódexének.

## ÖSSZEGZÉS, JAVASLATOK

A közlemény **aktualitását** a technológiai környezetben folyamatosan, illetőleg a belügyi igazgatás rendszerében bekövetkezett gyökeres változások, valamint a Rendőrség és Határőrség szervezeti integrációja alapozta meg. A megváltozó körülmények lehetőséget biztosítottak egyes ágazati problémák feltárására és vizsgálatára.

Az **első rész** a Rendőrség és a Határőrség egykori IT ágazatát volt hivatott részletesen elemezni. A korábbi nyilvánvaló működési problémák, illetőleg a jelenlegi szervezeti struktúra kialakításának gyakorlata felvetett néhány olyan kérdést, amelyek átgondolása elősegítheti a stabil szakmai alapokon álló IT ágazat tényleges kialakítását. A korábbi IT ágazatok vizsgálata során megállapítottam, hogy a kilencvenes évektől kezdődően mindkettő szervezet esetében generális, a megváltozó körülményekhez lényegében jól igazodó változások mentek végbe. Az eltérő szervezeti kultúra és működési hagyományok okán a szervezetek működési hatékonyságában különbözőségek voltak megfigyelhetők, amelyek okai nem az egyéni képességek területe révén voltak magyarázhatók. Széleskörű vizsgálatok alapján leszögeztem, hogy a jogszerű működés átfogó és teljeskörű biztosítása, valamint a működéshez szükséges feltételekről való gondoskodás – *főként az elmúlt években* – a Határőrség esetében valósulhatott meg sikeresebben. Vélelmezhetően azért, mert a személyi

állomány direkt és indirekt „szocializációja” eredményesebb volt, így a személyi állomány nagyobb része – *akarva, akaratlanul* – elsajátította *az egy nyelven való beszéd, beszélgetés* képességét.

Rávilágítottam arra a tényre, amely szerint az IT ágazatok összevonása két szakmai kultúra mentén került végrehajtásra, azonban mind a befogadó, mind a befogadott állomány szempontjából a jelenleg alkalmazott szervezési és működési megoldások újszerűnek hatnak.

A **második részben** áttekintettem a lehetséges fejlesztési irányokat. Javaslatokat fogalmaztam meg az IT ágazat identitástudatának kialakítása, az aktuális ágazati stratégiák, a szakmai, a szervezeti és működési, a minőségbiztosítási, valamint előmeneteli alapelvek, illetőleg a vonatkozó szabályozások összefoglalása és közreadása kapcsán.

Az egységes szemléletmód meghonosítása érdekében kidolgoztam a beosztások kategorizálásának elvét és főbb jellemzőit, illetve a kompetenciák révén meghatározottak teljesítésének elősegítése érdekében áttekintettem a felkészítés lehetséges megoldásait, azok előnyeit és hátrányait. Kifejtettem, hogy a kompetenciaalapú rendszer ágazati működési rendbe történő beillesztését és elterjesztését mindenképpen megfontolás tárgyává kell tenni.

További vizsgálódásaim során tett megállapításaim szerint, a szakmai elvek mind szélesebb körű érvényre juttatása érdekében lehetőséget kell biztosítani az IT ágazat vezetése számára, hogy az egyes rendőri szervek esetében véleményezési és egyetértési jogot szerezhessen jól körbehatárolt területeken. Végezetül, a rendszerszemléletű gondolkodás erősítése okán a műszaki jellegű tevékenységekhez köthető szabályozási keretrendszer kidolgozását láttam megvalósítandónak, amely révén az ország bármely rendőri szervezete részére egyértelmű viszonyok teremthetők a működés és fejlesztés területén.

A közlemény **legfőbb javaslatai, ajánlásai, illetőleg megállapításai** az alábbiak szerint foglalhatók össze:

- az egykori IT ágazatok vizsgálata rávilágított arra, hogy az integrált ágazat tekintetében, a működés jövőbeni sikeressége érdekében, az állomány körében ki kell alakítani az egy nyelven való beszélgetés, beszéd képességét;
- javaslatot tettem az IT ágazat szakmai kódexének kidolgozására;
- a szakmai kódex belső tartalmának részeként, néhány részterületet érintve, szabályozási, működési és felkészítési tárgyú javaslatokat dolgoztam ki.

Jelen cikk végső zárásaként, a kollektív gondolkodás szükségességének megerősítéseként, illetőleg az IT ágazat megújulásának reményében szeretném **Dr. Lindner Miklós** nyá. altábornagy úr, egykori híradó és automatizálási csoportfőnök, címzetes egyetemi tanár szavait felidézni [16]:

***„Ez a szakma nem tűri meg a sztárokat!”***

## HIVATKOZÁSOK:

[1] Pándi Erik – Vörös Szabolcs: A belügyminisztériumi ágazati távközlés fejlesztésének néhány kérdése (tanulmány), Tudomány Napja 2000. pályázat, fődíjnyertes pályamű, 22-55. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest, 2000.;

[2] Pintér Sándor: A magyar rendőrség átvilágításának fő tapasztalatai, azok hasznosításának lehetőségei a rendőrség korszerűsítésében, A magyar rendőrség és a határőrség a közvéleményben és a valóságban, A Belügyminisztérium és a Hanns-Seidel Alapítvány konferenciája, 15-19. oldal, Hans-Seidel Alapítvány – Batthyány Lajos Alapítvány – HM – BM, ISBN 963 7703 80 2 16, Budapest, 1993. február 23.;

[3] Mráz István: A haderő vezetése békétől eltérő (minősített) időszakokban, „Kommunikáció 2003.” nemzetközi szakmai tudományos konferencia, 222. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 86229 6 2, Budapest, 2003. október 15.;
[4] Mráz István: A vezetés információs támogatásának vezetői követelményei, „Kommunikáció 2001.” nemzetközi szakmai tudományos konferencia, 153-154. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, 179-191. oldal, Budapest, 2001. november 28.;
[5] A fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;
[6] Egri Gábor: Projektek a Belügyminisztériumban, „Kommunikáció 2001.” nemzetközi szakmai tudományos konferencia, 243-246. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, Budapest, 2001. november 28.;
[7] Határőrség Országos Parancsnokság: A Határőrség középtávú informatikai stratégiája az 1999-2001. évekre, 1-21. oldal, ORFK ITF irattár, Iktatási szám: 1/2-5/1999., Budapest, 1999.;
[8] A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény, DVD jogtár 2007/12. szám, Complex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., ISSN 1788-5027, Budapest, 2007.;
[9] Koczka Ferenc: Az alapfokú híradótiszt-képzés elemzése, javaslatok a fejlesztés fő irányaira, „Kommunikáció 2001.” nemzetközi szakmai tudományos konferencia, 86-89. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 00 8819 3, 180. oldal, Budapest, 2001. november 28.;
[10] Egri, Gábor: Integration of the Schengen Information System in Hungary, „Kommunikáció 2007.” nemzetközi szakmai tudományos konferencia, 403-416. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;
[11] Sebestyén Attila: Csökkenthető-e a „Superuser”-el kapcsolatos biztonsági kockázat?, „Kommunikáció 2007.” nemzetközi szakmai tudományos konferencia, 220. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;
[12] Kassai Károly: Az elektronikus adatkezeléssel kapcsolatos kockázatok kezelésének egyes kérdései, „Kommunikáció 2007.” nemzetközi szakmai tudományos konferencia, 78-79. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;
[13] Rajnai Zoltán – Kerti András: Az információvédelmi szakállomány továbbképzési rendszere, „Kommunikáció 2007.” nemzetközi szakmai tudományos konferencia, 86-89. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 978 963 7060 31 1, Budapest, 2007. október 16.;
[14] Busznyák János: Multifunkcionális, multimédia elemeket tartalmazó mobil elérésű távoktatási anyag összeállítása és tesztelése, X. Multimédia az Oktatásban Konferencia, 35-42. oldal, Szegedi Tudományegyetem, ISBN 963 7179 88 7, Szeged, 2004.;
[15] Szücs Ervin: Rendszer és modell I., Egységes Jegyzet (ELTE TTK), Kézirat, Tankönyvkiadó, Budapest, 99-100. oldal, 1987.;
[16] Szép József: A NATO és a Magyar C3, „Kommunikáció 2002.” nemzetközi szakmai tudományos konferencia, 255. oldal, Zrínyi Miklós Nemzetvédelmi Egyetem, ISBN 963 86229 2 XX, Budapest, 2002. október 30.

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Horváth Csaba**
Zrínyi Miklós Nemzetvédelmi Egyetem, hallgató

# AZ ORSZÁGVÉDELEM RENDSZERE ÉS KÖZPONTI IRÁNYÍTÁSA

***Absztrakt***

*Az országvédelem rendszere centrális alárendeltségű, központi, területi, helyi és települési szintekre tagozódik. Az országvédelem rendszere a védelmi igazgatás rendszerével mutat hasonlóságot, azzal a különbséggel, hogy a védelmi igazgatás rendszere tágabb értelmezést kapott a 71/2006. (IV.3.) kormányrendeletben. Központi irányítás szempontjából vizsgálva a kiindulási alap akár a szabályozási rendszerét, akár az irányítási rendszerét tekintjük át, azonosságot mutatnak.*

*The national defence is a centralised system constituted by central, area, local and settlement levels. The national defence system is similar to the defence administration system with one difference: the latter was given a broader definition by government regulation (71/2006, IV.3). From the perspective of the central administration, both show similar regulatory and management systems.*

***Kulcsszavak:*** *védelmi igazgatás, honvédelem, országvédelem, Magyar Honvédség, közigazgatás, Honvédelmi Tanács ~ defence administration, national defence, country defence, Hungarian Defence Forces, public administration, National Defence Board*

## AZ ORSZÁGVÉDELEM

Az országvédelem centralizált igényeit, a közigazgatás szervezeti struktúrájára épülő védelmi igazgatási rendszer elégíti ki. A védelmi igazgatás a közigazgatás alkotórészét képező olyan feladat-, szervezet- és intézményrendszer, amely a védelmi felkészítés és az országmozgósítás hatékonyságának érdekében a társadalom erőit összefogja, kormányzati, területi és helyi szinten egyaránt biztosítja a minősített helyzetek hatékony kezelését.

A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény egyes rendelkezéseinek végrehajtásáról szóló 71/2006. (IV. 3.) Korm. rendelet egy pontosabb megfogalmazását adja a védelmi igazgatásnak:

„*…a közigazgatás részét képező feladat- és szervezeti rendszer. Az állam komplex védelmi feladatainak megvalósítására létrehozott, valamint e feladatra kijelölt közigazgatási szervek által végzett végrehajtó, rendelkező tevékenység, amely magában foglalja az Alkotmányban szabályozott minősített időszakokra és az azokat kiváltható helyzetekre történő felkészülést, továbbá az említett időszakok és helyzetek honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatainak tervezésére, szervezésére, a feladatok végrehajtására irányuló állami tevékenységek összességét*”.

A védelmi igazgatási rendszer központi, területi és helyi szintekre tagozódik. A központi elemhez az Országgyűlés, az Országgyűlés Honvédelmi Bizottsága, a Honvédelmi Tanács, a köztársasági elnök, a kormány és a minisztériumok tartoznak. A területi elemet a fővárosi, megyei és a helyi (városi, kerületi) védelmi bizottságok alkotják. A helyi elemhez soroljuk a polgármestereket (és a jegyzőket).

Az Országgyűlés - védelmi jellegű hatáskörében - megállapítja az ország biztonság- és védelempolitikai alapelveit, megalkotja a minősített időszakokkal összefüggő jogszabályokat, dönt a honvédség és a határőrség létszámáról, fejlesztési irányairól és főbb haditechnikai rendszereiről, az ehhez szükséges költségvetési forrásokkal együtt, a minősített időszakok kihirdetéséről, a Honvédelmi Tanács létrehozásáról, továbbá a honvédségi erők részvételéről, vagy alkalmazásáról, illetve a külföldi fegyveres erők magyarországi alkalmazásáról, vagy állomásoztatásáról.

Az Országgyűlés Honvédelmi Bizottsága, az Országgyűlés más bizottságainak általános hatáskörén túl, sajátos honvédelmi jellegű hatáskörrel rendelkezik. Gyakorolja a honvédség és a határőrség feletti polgári ellenőrzést, továbbá szükségállapot idején, az Országgyűlést helyettesítő jogkörében eljárva, a rendkívüli intézkedések felülvizsgálatának jogát.

A Honvédelmi Tanács a honvédelem rendszerének rendkívüli állapot idején működő kivételes hatáskörű szerve, amely gyakorolja az Országgyűlés által rá átruházott, a köztársasági elnök és a Kormány teljes jogait.

A Köztársasági Elnök a honvédség főparancsnoka és rendkívüli állapotban a Honvédelmi Tanács elnöke, jóváhagyja az ország fegyveres védelmének tervét, szükségállapot idején dönt a rendkívüli intézkedések bevezetéséről és az Országgyűlés akadályoztatása esetén a honvédségi erők alkalmazásáról.

A Kormány az ország alkotmányos berendezkedésének megfelelően az országvédelem, és a rendkívüli helyzetek kezelése kormányzati rendszerének központi, meghatározó eleme. Összehangolja a minisztériumok és országos hatáskörű szervek országvédelemmel kapcsolatos tevékenységét, meghatározza az ország védelmi célú tartalékait, hadiipari kapacitását, valamint a közlekedés, a távközlés és a hírközlés védelmi célú felkészítésének és fejlesztésének állami feladatait.

A kormányzati feladatmegosztás szerint a miniszterek és az országos hatáskörű szervek vezetői irányítják az ágazat védelemmel kapcsolatos felkészítését a minősített időszaki feladataik ellátására.

Az Alkotmány a helyi-, települési közigazgatási feladatok szervezésénél az önkormányzatiság elvét érvényesíti, ennek megfelelően a fővárosi, megyei és helyi önkormányzatok bázisán alakulnak meg a védelmi igazgatás irányító, koordináló szerveiként, a védelmi bizottságok.

A fővárosi, megyei védelmi bizottság a Kormány centrális alárendeltségű szerve, amely illetékességi területén ellátja a védelmi felkészüléssel és az országmozgósítással kapcsolatos feladatokat.

A fővárosi, megyei védelmi bizottság alapvető feladata a helyi védelmi igazgatási szervek és a védelemben részt vevő más szervek védelmi felkészítésének irányítása és a végrehajtás koordinációja, a gazdaságmozgósítási és lakosság ellátási feladatok szervezése, a honvédelemben részt vevő szervek felkészülési és országmozgósítási feladatainak meghatározása, illetve azok helyi végrehajtásának összehangolása.

A fővárosi, megyei védelmi bizottság legfőképpen azért alkalmas a széleskörű koordinációra, mert a testületben a felelősségi terület valamennyi, a rendkívüli helyzetek kezelésével kapcsolatos feladatokat ellátó szervezete képviselve van, és szükség esetén munkájába bevonhatja más szervek vezetőit is

A főváros kerületeiben, a megyei jogú városokban és a megyei védelmi bizottság által kijelölt városokban, a városok vonzáskörzetébe tartozó településekre kiterjedő felelősséggel

(honvédelmi körzet) helyi védelmi bizottság irányítja és hangolja össze a helyi feladatok végrehajtását.

Feladatai közé tartozik irányítani és összehangolni a honvédelemmel kapcsolatos közigazgatási feladatokat, szervezni a lakosság polgári védelmével és ellátásával kapcsolatos feladatokat, összehangolni a honvédelmi körzetre háruló gazdasági és anyagi szolgáltatási kötelezettségek teljesítését, és közreműködni a rendkívüli intézkedésekből adódó helyi feladatok végrehajtásában.

A polgármester illetékességi területén ellátja a védelmi felkészítéssel és az országmozgósítással kapcsolatos feladatokat, irányítja és összehangolja azok helyi végrehajtását, megszervezi a gazdaságmozgósítás helyi feladatai és a lakosság ellátását.

A komplex szervezet- és intézményrendszer modulszerűen épül fel, átfogja az államigazgatási rendszert, a gazdaságot, a honvédséget és a rendvédelmi szerveket, a polgári védelmet, valamint a lakosságot.

A rendszer hibája, hogy kialakításakor elsősorban a honvédelmi kötelezettségekre alapozva, a honvédelmi típusú feladatok megoldására hozták létre. A katasztrófák elleni védekezésben, a rendszeres tiszai árvizek során, helyi (területi) szinten jól bevált, a gyakorlatok tapasztalata szerint a nukleáris baleset-elhárítás kezelésére is megfelelő lenne, azonban válságkezelésre csak szükségképpen alkalmas.

A Kormány az ország alkotmányos berendezkedésének megfelelően az országvédelem és a rendkívüli helyzetek kezelésének központi, meghatározó eleme. A rendkívüli helyzetekre történő felkészülésért a Kormány a felelős.

Ez a felelősség azonban jelenleg átruházott jogkörben valósul meg. Az érvényes szabályozás szerint a védelmi bizottságok irányítása és a honvédelmi típusú feladatok koordinálása a Honvédelmi Minisztérium feladata. A katasztrófák elhárítása során, valamint az azokra való felkészülésben a Belügyminisztérium koordinálja a többi minisztérium és országos hatáskörű szervek, valamint a fővárosi, megyei védelmi bizottságok feladatait. Az új kormányzati struktúra a BM feladatait kettéosztotta, a közigazgatás, a településfejlesztés és önkormányzati ügyek, valamint a katasztrófák elleni védekezés irányítása az Önkormányzati és Területfejlesztési Minisztérium, a rendvédelmi szervek irányítása az Igazságügyi és Rendészeti Minisztérium hatáskörébe került.

Napjainkban újabb változások előtt áll a terület. A védelmi igazgatás eddig két tárca között megosztott felelőssége nem vált be, a gyakorlatban nem valósított meg központi irányítást, sőt esetenként rivalizáláshoz, együttműködési hiányosságokhoz, információvesztéshez vezetett. Ha az eddigi szisztéma szerint egy újabb minisztérium is szerepet kapna az irányításban, még kevésbé lenne várható az összehangoltabb koordináció, ezért nem odázható el a védelmi igazgatás irányítási mechanizmusának áttekintése és racionalizálása. Az egyik (és valószínűleg a legcélszerűbb) megoldás a hatáskörnek, és a két védelmi hivatalnak a Miniszterelnöki Hivatalba integrálása lehetne.

## AZ ORSZÁGVÉDELEM KÖZPONTI IRÁNYÍTÁSA

Az országvédelem központi irányítási hatáskörei és feladatai az alkotmányos szabályok szerint békében megoszlanak az Országgyűlés, a köztársasági elnök, a Kormány, a honvédelmi miniszter és az illetékes miniszter között.

Ez a hatalommegosztás követi a békeidejű kormányzati struktúrát, de az egyes minősített időszakok szerint a hatáskör elosztási szabályok lényegesen megváltoznak. Rendkívüli állapot időszakában a központi irányítási jogköröket a kihirdetéssel egyidejűleg megalakítandó különös hatáskörű Honvédelmi Tanács veszi át.

*Az Országgyűlés védelmi jellegű fontosabb hatáskörei:*

- a Magyar Köztársaság honvédelmét meghatározó alapelvek megállapítása, a feladatok végrehajtásának irányai és feltételei meghatározása;
- a minősített időszakokkal összefüggő jogszabályok (pl.: honvédelemről, polgári védelemről, katasztrófa elhárításról, stb.) megalkotása;
- a Magyar Honvédség és a rendvédelmi szervek létszámának, hosszú távú fejlesztési irányának, főbb haditechnikai rendszereinek meghatározása és az ehhez szükséges költségvetési források biztosítása;

*Az Országgyűlés:*

- dönt a hadiállapot kinyilvánításáról és a békekötés kérdéséről;
- rendkívüli állapotot hirdet ki hadiállapot és háborús veszély esetén, ezzel egyidejűleg létrehozza a Honvédelmi Tanácsot, amely – többek között – gyakorolja az Országgyűlés által átruházott jogokat;
- kihirdeti a megelőző védelmi helyzetet és a szükségállapotot;
- dönt a Magyar Honvédség külföldi vagy országon belüli alkalmazásáról;
- veszélyhelyzetben felhatalmazást ad a Kormány részére rendkívüli intézkedések bevezetésére;
- a köztársasági elnök által bevezetett rendkívüli intézkedések alkalmazását felfüggesztheti, illetve 30 nap elteltével hatályukat meghosszabbíthatja.

*A köztársasági elnök*

- a Magyar Honvédség főparancsnoka;
- kinevezi és felmenti a Honvédség és a rendvédelmi szervek vezetőit, gyakorolja a tábornokokkal kapcsolatos személyzeti hatásköröket
- jóváhagyja az ország fegyveres védelmének tervét;
- az Országgyűlés akadályoztatása esetén gyakorolja a hadiállapot kinyilvánításának, a rendkívüli állapot kihirdetésének, valamint a Honvédelmi Tanács létrehozásának jogát;
- a Honvédelmi Tanács elnöke;
- szükségállapot idején dönt a rendkívüli intézkedések bevezetéséről és az Országgyűlés akadályoztatása esetén a fegyveres erők országon belüli alkalmazásáról.

*A Kormány*

- irányítja, illetve összehangolja a minisztériumok és országos hatáskörű szervek országvédelemmel kapcsolatos tevékenységét, irányítja a Magyar Honvédség és a rendvédelmi szervek működését, meghatározza és összehangolja a honvédelemben közreműködő szervek honvédelmi feladatait,
- meghatározza a polgári védelmi felkészítés feladatait,
- meghatározza az ország védelmi célú tartalékait, hadiipari kapacitását, valamint az infrastruktúra honvédelmi célú felkészítésének és fejlesztésének állami feladatait, meghatározza a nemzetgazdaság felkészítésével kapcsolatos követelményeket, és dönt a nemzetgazdaság mozgósításáról,
- engedélyezi a Magyar Honvédség, illetve külföldi fegyveres erők magyarországi, vagy az ország területéről kiinduló, az Észak-atlanti Tanács döntésén alapuló alkalmazását, valamint a külföldi fegyveres erők NATO döntésen alapuló magyarországi csapatmozgásait,
- veszélyhelyzetben és megelőző védelmi helyzetben az Országgyűlés felhatalmazása alapján egyes törvények rendelkezéseitől eltérő rendeleteket és intézkedéseket hozhat.

A Kormányon belül, a kormányzati feladatmegosztás szerint az egyes miniszterek irányítják a szakágazatba tartozó szervek védelemmel kapcsolatos felkészítését és minősített időszaki feladataik ellátását.

*A Honvédelmi Tanács*

A rendkívüli állapot idején a Honvédelmi Tanács gyakorolja az Országgyűlés által átruházott jogokat, valamint a köztársasági elnök és a Kormány jogait.

A Honvédelmi Tanács elnöke a köztársasági elnök, tagjai az Országgyűlés elnöke, az országgyűlési képviselőcsoportok vezetői, a miniszterelnök, a miniszterek, továbbá tanácskozási joggal a vezérkari főnök.

*A Honvédelmi Tanács irányítja:*

- az ország fegyveres védelmében részt vevő szervek védelmi tevékenységét (fegyveres védelem);
- a közrend, a közbiztonság és a belső rend védelmét (rendvédelem);
- a védelmi igazgatás működését;
- a lakosság támadó fegyverek hatásai elleni védelmét (polgári védelem);
- az ország erőforrásainak védelmi célú felhasználását és a védelem anyagi szükségleteinek kielégítését (gazdasági védelem).

A Honvédelmi Tanács kivételes hatáskörének egyedüli korlátja az Alkotmány, mert annak alkalmazása nem függeszthető fel, az Alkotmányban felsorolt alapvető alkotmányos jogok betartása kötelező, továbbá az Alkotmánybíróság működése nem korlátozható.

## IRODALOM


- A honvédelemről és a Magyar Honvédségről szóló 2004. évi CV. törvény egyes rendelkezéseinek végrehajtásáról szóló 71/2006. (IV. 3.) Korm. rendelet

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Horváth Zita**
Zrínyi Miklós Nemzetvédelmi Egyetem, hallgató

# A RENDKÍVÜLI ÁLLAPOT

***Absztrakt***

*A közigazgatás rendszerében a védelmi igazgatási tevékenység centrális alárendeltségű, központi, területi, helyi és települési szinteken valósul meg. A védelmi igazgatás rendszerében a rendkívüli állapot minősített időszak kiemelkedő jelentőségű, mert csak az egész ország területére hirdethető ki. Rendkívüli állapot idején az ország teljes potenciálja mozgósításra kerül. A különböző központi területi. Helyi és települési szinteken működő szervezeti elemeknek szorosan együtt kell működni.*

*Defence administration activities within the system of national defence are realised in a centralised way on central, areal, local and settlement levels. Emergency periods in the system of national defence are of outstanding importance as it may be announced for the whole country only. In the course of an emergency period the whole potential of the country is mobilised. Close cooperation of central, area, local and settlement-level organisations is essential.*

***Kulcsszavak:*** *védelmi igazgatás, minősített időszak, rendkívüli állapot, Magyar Honvédség, közigazgatás, Honvédelmi Tanács ~ defence administration, classified period, emergency, Hungarian Defence Forces, public administration, National Defence Board.*

A közigazgatás szervezetrendszere az ország fegyveres és nem fegyveres védelmét biztosító honvédelmi rendszer elemeként meghatározó szerepet tölt be. Az államvezetés e területe az ország védelemmel kapcsolatos rendkívüli időszakokban centrális irányítású, hierarchikus felépítésű rendszerben működik és az ország védelemmel kapcsolatos irányító, végrehajtó feladatait a védelmi felkészítés időszakában kialakított és begyakorolt eljárásmódok alkalmazásával, a jogszabályokban és az állami irányítás egyéb jogi eszközeiben felhatalmazott rendkívüli jogalkalmazási tevékenységével biztosítja.

A védelmi igazgatás szervezetrendszerébe az általános hatáskörű, valamint a szakigazgatási feladatokat ellátó állami szervek tartoznak. Általános hatáskörű szervek csoportjába tartoznak a védelmi igazgatás központi (az Országgyűlés, a Honvédelmi Tanács, a Köztársasági Elnök, a Kormány, a minisztériumok és országos hatáskörű szervek), területi (megyei, fővárosi védelmi bizottságok, helyi védelmi bizottságok) valamint települési (polgármester, jegyző) szervei. Alapvető feladatuk, hogy centrális irányítási rendszerben biztosítsák a fegyveres erők, rendvédelmi szervek és a védelemben részt vevő állami és nem állami szervek, továbbá az önkormányzati szervek és a lakosság felkészítését, mozgósítását a védelmi feladatok érdekében. A védelmi igazgatás szakigazgatás szervei közé tartoznak az

ország védelem sajátos feladatait ellátó katonai igazgatás szervei, valamint a polgári lakosság oltalmazását és az anyagi javak védelmét, mentését végző polgári védelmi szervek. A védelmi igazgatás általános, illetve szakigazgatási szervein túl bevonásra kerülnek a rendvédelmi és polgári szervek is.

A védelmi igazgatás szervezete átfogja az állam normál (béke) időszakát veszélyeztető valamennyi helyzetet. A veszélyhelyzeteket megelőzi a felkészülés időszaka, míg a veszély kezelése a hatáskörrel rendelkező szervek azonnali, hatékony és szervezett beavatkozását igényli.[1]

A minősített időszakokban a béke időszakhoz képest jelentős szigorító jellegű intézkedések vezethetők be, melyet legmagasabb jogi szinten az Alkotmány szabályoz.

A Magyar Köztársaság Alkotmánya meghatározza az egyes minősített időszakokat és meghatározza ezek bevezetésének módszerét. A 2004-ben módosított Alkotmány szerint a következő minősített időszakokat különböztetjük meg:

1. rendkívüli állapot
2. szükségállapot
3. veszélyhelyzet
4. Alkotmány 19/E § szerinti minősített időszak;
5. megelőző védelmi helyzet[2]

A minősített időszakok közös jellemzője, hogy az állam normál működését, az állampolgárok élet- és vagyonbiztonságát külső vagy belső társadalmi illetve természeti veszély fenyegeti. A veszélyek elhárítására, illetve következményeinek felszámolására a rendkívüli jogrend eszközei vehetők igénybe.

Jelen írásban a rendkívüli állapot feladataival kívánok bővebben foglalkozni.

Mindent törvényt legmagasabb szinten az alkotmány szabályoz, természetesen ez igaz a minősített időszakokra, így a rendkívüli állapotra is.

Az Alkotmány meghatározása alapján: „… *az Országgyűlés hadiállapot vagy idegen hatalom fegyveres támadásának közvetlen veszélye (háborús veszély) esetén kihirdeti a rendkívüli állapotot, és Honvédelmi Tanácsot hoz létre* …”.[3]

A közvetlen veszély meghatározás szerint a rendkívüli állapot kihirdetésének nem alapfeltétele a konkrét haditevékenységek bekövetkezése, csupán a veszélye. Haditevékenység esetén hadiállapot jön létre, ennek kinyilvánításának joga szintén az Országgyűlés hatásköre.

A háborús veszély olyan nemzetközi helyzet, amelyben a Magyar Köztársaság szuverenitását, függetlenségét, területi integrálását, alkotmányos rendjét, idegen hatalom fegyveres támadása közvetlenül veszélyezteti.

Rendkívüli állapot kihirdetésére, valamint a Honvédelmi Tanács létrehozására az Országgyűlés jogosult. Előfordulhatnak olyan események, amelyek nem teszik lehetővé az Országgyűlés összehívását, vagy szavazóképességének elérését, ezért ez esetekben az Alkotmány a Köztársasági Elnök kezébe adja ezt a jogot. Azonban a kihirdetés indokoltságát az Országgyűlés elnöke, a Miniszterelnök és az Alkotmánybíróság elnöke a Köztársaság elnökével együttesen állapítja meg.

A rendkívüli állapot kihirdetésével egy időben létrehozzák a *Honvédelmi Tanácsot*. A Honvédelmi Tanács a védelmi igazgatás szervezetrendszerének rendkívüli jog- és hatáskörével felhatalmazott szerve, gyakorolja az országgyűlés által rá átruházott jogokat, valamint az államfői és a végrehajtó hatalmi ágak jogkörét. A Honvédelmi Tanács rendkívüli állapot idején a Magyar Köztársaság honvédelmének és fegyveres erőinek legfőbb irányítója.

A Honvédelmi Tanács rendeletet alkothat, ebben egyes törvények alkalmazását felfüggesztheti, illetve törvényi rendelkezésektől eltérhet, egyéb különleges intézkedéseket

[1] Dr. habil. Horváth László: Az országvédelem szervezeti rendszere ZMNE Egyetemi jegyzet Budapest, 2005.

[2] A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény, módosításáról szóló, 2004. évi CIV. törvény 1 §

[3] A Magyar Köztársaság Alkotmánya 19.§ (3) számú pontja

hozhat, azonban az Alkotmány alkalmazását és az Alkotmánybíróság működését nem függesztheti fel.

A Honvédelmi Tanács elnöke a Köztársasági Elnök, tagjai: Országgyűlés elnöke, az Országgyűlésben képviselettel rendelkező pártok képviselő-csoportjainak vezetői, a Miniszterelnök, a miniszterek és tanácskozási joggal a Honvéd Vezérkar Főnöke.[4]

A Honvédelmi Tanács, mint a legfőbb irányító szerv, irányítja:

1. a fegyveres erők és a fegyveres védelemben részt vevő szervek tevékenységét;
2. a közrend, közbiztonság és a belső rend védelmét;
3. az ország védelmi erőforrásainak védelmi célú felhasználását és a védelem anyagi szükségleteinek kielégítését;
4. a védelmi igazgatás működtetését;
5. a lakosság támadó fegyverek hatása elleni védelmét és a következmények felszámolását.

A Honvédelmi Tanács jogkörében:

1. meghatározza a kormányzás szervezetét, irányát, feltételeit;
2. megköti a Magyar Köztársaság szempontjából kiemelkedően fontos nemzetközi szerződéseket (a békeszerződés kivételével);
3. engedélyt ad a fegyveres erők részére az államhatár átlépéséhez;
4. dönt az idegen fegyveres erőknek az ország területén való felhasználásáról, állomásoztatásáról, átvonulásáról;
5. meghatározza a közigazgatás rendkívüli rendszerét, feloszlatja az Alkotmánnyal vagy a Honvédelmi Tanács rendeletével ellentétesen működő önkormányzati képviselő-testületet;
6. közkegyelmet gyakorol.

A rendkívüli állapot ellentétben a többi minősített időszakkal, csak az ország egész területére kiterjedően rendelhető el.[5]

A minősített időszakokról általánosan elmondható, hogy három egymást követő szakaszra oszthatók, mindháromban különböző feladatok hárulnak a védelmi igazgatási szervekre.

1. Béke időszak:
   A béke időszak a védelmi igazgatás felkészülésének időszaka. Ekkor az állami vezetés, a fegyveres erő és a rendvédelmi szervek tevékenységével, a gazdaság mozgósításával, az ország területének védelmi célú előkészítésével és a lakosság védelmével kapcsolatos feladatköröket alkotja meg. Ebben az időszakban történik a feladatok megtervezése, a megoldásukra való felkészítés és elhárításuk gyakorlása.
2. Minősített időszak bevezetését közvetlenül megelőző időszak:
   A minősített időszakot közvetlenül megelőző időszakra jellemző, hogy a társadalmi, bel- és külpolitikai, biztonságpolitikai viszonyokban olyan mértékű változások következnek be, amelyek veszélyeztetettségi helyzetet idéznek elő, de a rendezésükre vagy megelőzésükre még van lehetőség. Ezen időszakban a védelmi igazgatás felkészítésével összefüggő feladatok, a lakosság, a fegyveres erő és a rendvédelmi szervek felkészítésére, az ország védelmi célú előkészítésére, valamint a gazdaságmozgósítás megszervezésére kerül sor.
3. Kihirdetett minősített időszak:
   A kihirdetett minősített időszak alkalmával életbe lép a rendkívüli jogrend, rendkívüli intézkedések bevezetésére kerül sor.

[4] A Magyar Köztársaság Alkotmányának módosításáról szóló 2001. évi XLII. törvény 1. §

[5] Dr. habil. Horváth László: Az országvédelem szervezeti rendszere ZMNE Egyetemi jegyzet Budapest, 2005.

A rendkívüli állapottal kapcsolatban felmerül egy korábban az általános hadkötelezettség idején, a sorozott hadseregünknél nem létező probléma, kit mozgósíthatunk azonnal?

A honvédelmi törvény szerint - az általános hadkötelezettség megszüntetését követően - a hadkötelezettség teljesítésére csak a megelőző védelmi helyzet és rendkívüli állapot időszakában kerülhet sor. Bevezetése esetén minden magyar állampolgárságú nagykorú férfire kiterjed, a hadkötelezettség, feltéve, ha a Magyar Köztársaság területén lakóhellyel rendelkezik. Bevezetésekor a hadkötelezettség a 18. és 40. életév közöttiekre vonatkozik.[6] A hadkötelesek nyilvántartása és mozgósítása a Hadkiegészítő Parancsnokságok feladatkörébe tartozik.

## IRODALOM


- Dr. habil. Horváth László: Az országvédelem szervezeti rendszere ZMNE Egyetemi jegyzet Budapest, 2005.
- A Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény, módosításáról szóló, 2004. évi CIV. törvény
- A Magyar Köztársaság Alkotmánya
- A Magyar Köztársaság Alkotmányának módosításáról szóló 2001. évi XLII. Törvény
- 2004. évi CV. Törvény a honvédelemről és a Magyar Honvédségről


[6] 2004. évi CV. Törvény a honvédelemről és a Magyar Honvédségről

HADMÉRNÖK
III. Évfolyam 3. szám - 2008. szeptember

**Pántya Péter**
Zrínyi Miklós Nemzetvédelmi Egyetem, hallgató
panpet1@freemail.hu

# A HIVATÁSOS SZOLGÁLATI TÖRVÉNY ÁTTEKINTÉSE A 2008. ÉV ELEJÉN

***Absztrakt***

*A Magyar Köztársaságban élők életét, testi épségét és vagyonát a fegyveres és rendvédelmi szervek hivatottak szolgálni. Ezen speciális területeken feladataikat végzőkre különleges jogszabályoknak kell, hogy vonatkozzanak. A Munka Törvénykönyve számukra nem hatályos, szolgálati körülményeiket a 1996. évi XLIII-as törvény, közismertebb nevén a Hszt. szabályozza.*
*E törvény felépítését, gyakorlati működését jelenítem meg ebben a cikkben. Példák levezetésével teszem érthetőbbé az olvasó számára a törvény esetlegesen speciálisabb részeinek jelentését, hatását. Felsorolásra kerülnek a hatálya alá tartozó rendvédelmi szervezetek és feladatkörük is.*

*Armed forces and defence authorities serve the life, soundness, and properties of citizens in the country of Hungary. We need special law for these special activities. The Law of Work is extinct to us, our circumstances of duty is ruled by the law of 1996./XLIII, or known as Duty Laws.*
*I write the system and practical working of this law in this article. I make the readers understand the specialties and effects of this law by examples. Defence authorities and their duty are also listed.*

***Kulcsszavak:*** *rendvédelem, HSZT, fegyveres, szervek ~ defence, authorities, law, duty*

## BEVEZETÉS

Jelen cikk elkészítése során fontosnak tartottam, hogy a Magyar Köztársaság állampolgárai nyugalmát biztosítók szolgálati viszonyát szabályozó törvényt alaposabban nagyító alá vegyem. Természetesen itt az 1996. évi XLIII.-as törvényt értem, amely a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szól, közismertebben nevén a Hszt.

Több helyen és forrásból próbáltam kutatni hasonló publikálásokat és feltűnt, hogy ez a – véleményem szerint igen fontos – terület ez idáig nem volt fókuszban a védelmi tudományterület oktatásában. Az állomány tagjainak a szolgálattal kapcsolatos preferenciái meglehetősen szabályozottak e módon és nem jelenthető ki kategorikusan, hogy: - legyen ez csak a jogászok dolga. A rendvédelemben e törvény legalább alapszintű ismerete nélkül nehéz jogszerűen ellátni akár a napi szolgálati feladatokat is. Mivel a Hszt. a hivatásos állományúak szolgálattal kapcsolatos viszonyát meglehetősen szerteágazóan szabályozza, könnyen

mulasztási hibába kerülhet az egyén, aminek akár fegyelmi következményei is lehetnek. A jogok és érdekérvényesítési lehetőségek nem megfelelő szintű ismerete érdeksérelemhez vezethet, tehát mindenkinek elemi szükséglete kell (kellene?) legyen, hogy ismerje a rá vonatkozó szabályokat, legyenek azok megengedők, juttatók vagy szigorítók, előírók.

A Hszt.-t időnként frissítik, aktualizálják a változásoknak és az esetleges újabb céloknak (pl.: egy szektor preferálása) vagy szakszervezeti törekvéseknek megfelelően. Az újabb módosítások folyamatosan napirenden vannak, az egyeztetések napjainkban is folytatódnak. Az időszerű változásokat szeretném bemutatni ismertetve várható hatásukat és talán egy kicsit úttörőként, megkérdezve a közvetlenül érintetteket.

Bízom benne, hogy ezzel a munkámmal sikerül – akár csekély mértékben is – egy kis ismeretterjesztéssel szolgálni a kollégák és bajtársak felé. Remélhetőleg az elemzéseimből és következtetéseimből eljuthat valamennyi rész akár döntéshozókhoz is a Hszt. módosítások kapcsán. E törvény hatásában megjelenik mind a gazdasági, mind a szociológiai területeken is nem elhanyagolva a pszichológiát és a társadalomlélektant és alapot biztosít több jogszabályhoz, jogághoz.

Ki kívánok térni magára a Hszt. felépítésére, értelmezésére, megalkotásának körülményeire és előzményeire, napjaink módosításaira. Helyenként bizonyára sokaknak egyértelmű dolgokat ismertetek, azonban célom a teljes körű ismeret adása. A hivatásos szolgálati törvény minden, a Magyar Köztársaságot szolgáló fegyveres és rendvédelmi szervnél állományban lévő hivatásosra vonatkozik, ide nem értve a Magyar Honvédséget, mivel e területen a 2001. évi XCV. törvény hatályos (a Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról). Röviden bemutatásra kerülnek a fegyveres és rendvédelmi szervek valamint feladatköreik, hogy jobban megismerhetőek legyenek az állományuk tagjainak.

Megkerestem néhányat az érintett szakszervezeti vezetők közül is, nézetüket ismertetem.

## A FEGYVERES ÉS RENDVÉDELMI SZERVEK

A fogalmak tisztázása nélkül nehéz lenne a témáról beszélni. Nézzük tehát, hogy melyek is az úgynevezett fegyveres és rendvédelmi szervek, milyen feladatok vannak számukra meghatározva és ezen feladatokat milyen módon teljesítik.

*Fegyveres és rendvédelmi szervek (országos vezetősége):*

- Rendőrség (Országos Rendőr-főkapitányság, immár a Határőrséggel integrálódva)
- Polgári védelem (Országos Katasztrófavédelmi Főigazgatóság)
- Vám- és pénzügyőrség (Vám és Pénzügyőrség Országos Parancsnoksága)
- Büntetés-végrehajtási intézet (Büntetés-végrehajtás Országos Parancsnoksága)
- Állami és Hivatásos önkormányzati tűzoltóságok (Országos Katasztrófavédelmi Főigazgatóság)
- Polgári nemzetbiztonsági szolgálatok (vezetője a főigazgató)

A Magyar Köztársaság alkotmányos rendjét és biztonságát tehát ezek a szervek biztosítják saját területükön, a számukra meghatározott feladatok ellátásával. E szervek összlétszáma körülbelül ötvenötezer fő.

A fenti felsorolás és a létszámadatok nem tartalmazzák a Magyar Honvédséget, amelyet természetesen nem akarok figyelmen kívül hagyni! A haza érdekében kifejtett tevékenysége mindenképpen elismerésre méltó, azonban a Magyar Honvédség hivatásos tagjai a Hszt. hatálybalépésétől 2001-ig tartoztak e törvény alá. 2001-ben került elfogadásra a 2001. évi XCV. Törvény a Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról szólt.

Mivel tehát a hivatásos katonák szolgálati viszonyát nem érinti a Hszt. és ez nem is várható, így az ő helyzetükkel csak érintőlegesen foglalkozom.

A feladatok ellátásának módjáról az 1996. évi XLIII-as törvény világosan fogalmaz: *„A Magyar Köztársaság függetlenségének, alkotmányos rendjének, valamint a lakosság és az ország anyagi javainak védelmét ellátó szervek hivatásos állományától az állam tántoríthatatlan hűséget, bátor helytállást követel.”*


*1. számú kép. Mozaik a fegyveres és rendvédelmi szervek jelképeiből. Saját összeállítás, 2008.*

Az állomány hivatásos állományú tagját igazolja egyenruhája, némely szerveknél jelvénye valamint akár civil ruházatban is, szolgálati igazolványa. A fegyveres és rendvédelmi szervek tagjait megkülönböztethetjük az állományra utaló jelzéssel, eltérő rendfokozatokkal és más-más beosztásokkal. Például.: rendőr orvos alezredes, tűzoltó törzszászlós (hírközpont-kezelő), pénzügyőr őrmester (kutató), polgári védelmi százados (osztályvezető).

## A HIVATÁSOS SZOLGÁLATI TÖRVÉNY

Az 1996 évi XLIII-as törvény, a fegyveres és rendvédelmi szervek hivatásos állományú tagjainak szolgálati viszonyáról szól. Alapvetően azért jött létre, hogy elismerje a hivatásos (szerződéses) szolgálatban állók különleges szolgálatát és szabályozza ezt a kapcsolatot, ami az állam és a hivatásos szolgálatot vállaló között jött létre.

A törvény elfogadására készült indoklás megjeleníti a Hszt. létrehozásának szükségességét: *„Az országunk függetlenségének, belső rendjének, biztonságának védelme - amit a honvédség, a határőrség, a rendőrség, a polgári nemzetbiztonsági szolgálatok, a polgári védelem, a vám- és pénzügyőrség, a büntetés-végrehajtási szervezet, valamint az állami és önkormányzati tűzoltóság... ...látnak el - állami, közösségi tevékenység. E szervek személyi állománya ennek megfelelően - a szervi hovatartozástól függetlenül - közszolgálatot teljesít… ...Abból indul ki, hogy a hivatásos állomány tagjai az általánoshoz képest szigorúbb függelmi rendben és fegyelmezettséggel, fokozott pszichikai és fizikai terheléssel, áldozatvállalással, veszélyes helyzetben az élet kockáztatásával végzik feladataikat. Emellett a szolgálati viszony létesítésének feltételeként önkéntesen lemondanak alkotmányos jogaik gyakorlásáról… …Mindezek figyelembe vételével a Javaslat az ugyancsak közszolgálatban álló köztisztviselők járandóságai alapulvételével, a társadalmi megbecsülés kifejezéseként kedvezőbben állapítja meg a hivatásos állomány tagjait megillető jogokat, juttatásokat.”*[1]

[1] Az 1996. évi XLIII. törvény indokolása

Körülbelül 55.000 fős hivatásos állomány áll jelenleg a Hszt. hatálya alatt. Az ő szolgálati körülményeiket valamint közvetve családjaik életét meghatározó törvényre nem lehet úgy tekinteni, mintha az „csak" egy jogszabály volna. A törvény megalkotása abszolút időszerű volt, hiszen előzőleg egy 1971-es törvény szabályozta ezeket a kereteket.

Az érintettek nagy félelemmel várják az idén várható változtatásokat. Ezekből néhány:

- megkezdődik a civilesítés, bizonyos beosztások (humán és munkaügyi, gazdasági, üzemeltetési, stb.) munkakörök közalkalmazotti státusszá alakulnak;
- átalakul a nyugdíjrendszer, nő a szolgálatban eltöltendő évek száma, változik a nyugdíjszámítás módja;
- módosul a teljesítményértékelés és a pótlékok rendszere.

Ezek a várható változások az állományon belül már elindítottak bizonyos folyamatokat.

## A TÖRVÉNY FELÉPÍTÉSE

Preambulumában olvasható a jogalkotó célja a fegyveres és rendvédelmi szervek tagjainak elismerésére és szolgálati viszonyuk rendezett szabályozására.
Megalkotása óta sok-sok módosításon esett át a szolgálati törvény felépítését a jelenleg is hatályos változata alapján vizsgálom. A törvény részeit végrehajtási rendeletekkel tették teljessé és módosíthatóvá.

Példaképpen néhány végrehajtási rendelet:

- 9/1997. BM rendelet, a belügyminiszter irányítása alá tartozó szervek, valamint az önkormányzati tűzoltóság szolgálati viszonyban álló tagjai szolgálati viszonyának egyes kérdéseiről és a személyügyi igazgatás rendjéről.
- 15/2000. BM rendelet, az egészséget nem veszélyeztető és biztonságos munkavégzés szabályairól a belügyminiszter által irányított rendvédelmi szerveknél.
- 140/1996. Kormányrendelet, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény végrehajtásáról

Szerkezetében három részre tagolódik, ezeken belül pedig fejezetekre, a végén található mellékletekben, formaszövegek és táblázatok találhatóak a szolgálati viszonyhoz.

- I. Rész. Ez a fő rész, amely tartalmazza a törvény hatályát, jognyilatkozatokat, az alkotmányos jogok korlátozását, érdekképviseleti lehetőségeket, a szolgálati viszonnyal kapcsolatos szabályokat és tartalmat többek között a szabadság számítását is.
- II. Rész. Itt találhatóak az úgynevezett különös szabályok. A közös szabályok után megtalálhatóak a szakmaspecifikus fejezetek. Ilyen például a XXI. Fejezet, amely csak a polgári nemzetbiztonsági szolgálatok állományára vonatkozóan határoz meg szabályokat.
- III. Rész. A vegyes, átmeneti és záró rendelkezések helye. Ilyenek például a minden hivatásosra vonatkozó szolgálati idő számítások, hatálybalépési előírások, jogalkotási felhatalmazások valamint a mellékletek a rendfokozatokról, annak illetményszorzóiról, a besorolási osztályok és az esküszövegek.

## A SZOLGÁLATI TÖRVÉNY A GYAKORLATBAN

A következőkben példákon és számításokon keresztül mutatom be, hogy a paragrafusok közül néhány kivonatolt, milyen hatással van a hivatásos állományú dolgozókra.

**Az I. Részből:**

*„**2 §** s) magasabb beosztás: nagyobb felelősséggel, szélesebb hatáskörrel és ennek megfelelően magasabb rendfokozattal és illetménnyel járó státusz”*[2]

A magasabb beosztásba akkor kerülhet a hivatásos állományú, ha rendelkezik a megfelelő iskolai (polgári és rendészeti szakmai) végzettséggel és természetesen van üres beosztás. Beleegyezése nélkül is megbízható más beosztással, amennyiben rendelkezik a megfelelő szakképzettséggel és gyakorlattal.

A nagyobb felelősség és szélesebb hatáskört jól jellemzi, hogy amíg szerparancsnokként egy gépjárműfecskendő és a rá beosztott legfeljebb öt fő tartozott alá, addig ezután a teljes aznapi készenléti állomány, a szerek, felszerelések, valamint a tűz és kárelhárítások során az egyszemélyi felelősség is az övé. A magasabb illetmény és a magasabb rendfokozat az állománytáblában meghatározottak alapján értendő. A beosztási illetmény a köztisztviselői illetményalap és a beosztás szerinti szorzószám szerint alakul.

Például: egy tűzoltó törzszászlós, szerparancsnok kinevezése szolgálatparancsnok beosztásba. A szerparancsnok rendfokozati maximuma főtörzszászlós lenne, de tiszti beosztásba kerül és a példában az Önkormányzati és Területfejlesztési Miniszter kinevezi hadnaggyá. Az elérhető rendfokozati maximuma alezredessé változik (amit 18 év szolgálat után ér el). Az illetményének számítása is megváltozik a Hszt. 6/A mellékletének megfelelően. A szerparancsnoki beosztásban a beosztási illetményszorzó 3,6 –tól indul, tehát a soros, fizetési fokozatokban való előrelépésekkel elérhető az adott beosztásban legmagasabb 4,25-ös szorzó. Az új, szolgálatparancsnoki beosztásban két fizetési fokozat van. Az 5,7-es és a három év szolgálat után járó 5,8.

A végeredmény szerint tehát egy zászlósból hadnagy vált, a bruttó beosztási illetménye pedig (3,0*38.650 Ft) 115.950 Ft-ról (5,7*38.650 Ft) 220.305 Ft-ra változott.

***„30. §** (1) A szakszervezettel való együttműködés keretében az állományilletékes parancsnok köteles:*

*a) a szükséges tájékoztatás megadásával a szakszervezet érdekképviseleti tevékenységét elősegíteni;*

*b) a szakszervezet által tett észrevételekre, javaslatokra vonatkozó álláspontját és ennek indokait közölni…”*[3]

A Hszt. elismeri az érdekképviseletek jogát a rendvédelmi szerveknél való működésre. Az együttműködést a parancsnok kötelességévé teszi. A Hszt. előtti szabályozáshoz képest ez nagy előrelépés volt.

***„77. §** A rendfokozatban való előmenetel a magasabb rendfokozatba történő előléptetéssel és kinevezéssel valósul meg. A hivatásos állomány tagja előléptethető*

*a) soron,*

*b) soron kívül,*

*c) a 81. §-ban meghatározott egyéb okból.”*[4]

A törvény a kiszámítható életpályamodellnek megfelelően biztosítja a hivatásos előrejutását. Csak állománycsoporton belül van lehetőség előléptetésre, ez azt jelenti, hogy az őrmesterként pályára kerülő dolgozó az adott beosztásában sorosan csak főtörzsőrmesteri rendfokozatig léphet elő a meghatározott várakozási idők leteltével. A soron kívüli előléptetéssel elismerhetővé válik az állomány tagjának teljesítménye, érdeme.

***„99. §** (1) A hivatásos állomány tagja szolgálati viszonya alapján havonta illetményre jogosult.*

---

[2-16] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

*(2) Az illetmény beosztási illetményből, rendfokozati illetményből, illetménykiegészítésből, szolgálati időpótlékból, valamint az e törvény által meghatározott feltételek fennállása esetén illetménypótlékból áll. A beosztási illetmény és a rendfokozati illetmény együttes összege képezi az alapilletményt."*[5]

A beosztási és rendfokozati illetmény szorzószámait a 6/A.

A magasabb rendfokozathoz magasabb rendfokozati szorzók is tartoznak.

Például forintosítva: Őrmester = 0,38*38.650 Ft.= 14.687 Ft
Hadnagy = 0,56*38.650 Ft.= 21.644 Ft
Alezredes = 0,75*38.650 Ft.= 28.988 Ft

Amint látható, a rendfokozatok közötti különbségek összegek alapján nem jelentősek.

Az illetménykiegészítés a hivatásos állományú, a szervezeti hierarchiában elfoglalt státuszát ellensúlyozza. Minisztériumi, országos, területi és helyi szervnél betöltött beosztása alapján 50, 40, 30 és 15 százalék felsőfokú végzettségű esetében. A szolgálati időpótlék az állomány tagjának hivatásosként eltöltött idejét és tapasztalatát kompenzálja. 10 év szolgálat után adható először, majd ötévenként emelkedik a mértéke. Sajnos összege ennek sem jelentős, 10 év után a köztisztviselői illetményalap 12,5%-a, 4.831 Ft.

Az illetménypótlékok rendszere meglehetősen sokrétű. A hivatásos a beosztásához kapcsolódó feladatok végzésének okán jogosult lehet: idegen-nyelvtudási, járőr, vezetői, éjszakai, ügyeleti, stb. illetménypótlékra.

Az érdemek elismerésére a következő paragrafus tartalma ad lehetőséget:

***„118. §*** *A hivatásos állomány tagja az adott szolgálati feladat kiemelkedő teljesítéséért, illetve a szolgálati feladatok hosszabb időn át történő eredményes végzéséért a következő elismerésekben részesíthető:*

*a) a fizetési fokozatban eltöltendő várakozási időnek 1 évvel történő csökkentése,*
*b) egy fizetési fokozattal való előresorolás,*
*c) pénz- vagy tárgyjutalom,*
*d) hazai vagy külföldi jutalomüdülés,*
*e) a miniszter által adományozott, névre szóló szál- vagy lőfegyver, emléktárgy,*
*f) a miniszter által alapított kitüntető cím, díj, plakett, oklevél, emléklap stb.*
*g) soron kívüli előléptetés,*
*h) szolgálati jel,*
*i) kitüntetés."*[6]

A fegyelmi szabályok elsőrendű célja, hogy védje a szolgálati rendet és a fegyelmet, valamint, hogy mind az elkövetőt, mind másokat visszatartson a fegyelemsértéstől

***„123. §*** *(1) A hivatásos állomány tagjával szemben a következő fenyítések alkalmazhatók:*

*a) feddés,*
*b) megrovás,*
*c) pénzbírság,*
*d) egy fizetési fokozattal 1 évre való visszavetés,*
*e) a soron következő rendfokozatba való előléptetés várakozási idejének 6 hónaptól 2 évig terjedő meghosszabbítása,*
*f) eggyel alacsonyabb rendfokozatba 6 hónaptól 2 évig történő visszavetés,*
*g) alacsonyabb szolgálati beosztásba helyezés,*
*h) a szolgálati viszony megszüntetése,*
i) lefokozás."[7]

[5] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról
[6-20] 1996.évi XLIII-as törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról

Sokan tévesen a rendfokozatban való visszavetést ismerik lefokozásnak, holott valójában ez még a szolgálati viszony megszüntetésénél is súlyosabb eszköz. Az ezzel sújtott személy elveszíti eddig szerzett rendfokozatát is.

**A II. Részből:**

***„245/D. §*** *(1) A hivatásos állomány tagja a vezetői beosztásából indokolás nélkül azonnali hatállyal felmenthető, illetve arról az érintett 30 napos határidővel indokolás nélkül bármikor lemondhat."*[8]

A vezetői beosztásúak számára ez egy igen súlyos fenyegetettség. A indoklás nélküli felmentés lehetősége meglehetősen szabad kezet ad az állományilletékes parancsnoknak.

*„***261.** § *(1) A bűnözés elleni eredményes fellépés céljából a rendőr, hivatásos szolgálati viszonyának fenntartása mellett - szolgálati feladatként, a rendőrséghez tartozás leplezésével - más foglalkoztatási jogviszony létesítésével, vagy egyéb jövedelemszerző tevékenység folytatásával bízható meg."*[9]

Amint látható a hivatásos állományú számára nemcsak az alkotmányos jogaik korlátozottak, hanem – szolgálati érdekből – még a hagyományos élete is megváltoztatható.

**III. Részből**

***„342. §*** *(1) Felhatalmazást kap a Kormány, hogy rendeletben részletesen szabályozza:*

*a) a más szervhez vezénylésre és áthelyezésre kerülők szolgálati viszonya módosításának rendjét, a foglalkoztatásukkal, jogaikkal és kötelezettségeikkel összefüggő kérdéseket, továbbá a velük kapcsolatos személyügyi igazgatást;*

*b) a szolgálati viszony szünetelésének eljárási rendjét…"*[10]

A már említett végrehajtási rendeletek e paragrafus felhatalmazása alapján készülhetnek el az illetékes szervek, szakminiszterek részéről.

Részlet a Hszt. mellékleteiből:

***„1. számú melléklet az 1996. évi XLIII. törvényhez***
***A rendfokozatok és a rendfokozati várakozási idők***

*A rendfokozatok rendfokozati állománycsoportok szerinti sorrendben:*
*a) tisztesek:*
*- őrvezető,*
*- tizedes,*
*- szakaszvezető;*
*b) tiszthelyettesek:*
*- őrmester,*
*- törzsőrmester,…*
*…Az egyes rendfokozatokban eltöltendő várakozási idő:*

| | |
|---|---|
| *- tisztesi rendfokozatokban* | *6 hónap,* |
| *- őrmesteri rendfokozatban* | *3 év,* |
| *- törzsőrmesteri rendfokozatban* | *4 év,…* |

*"*

Amint látható világosan megjelennek a különböző rendfokozatok, láthatóak az állománycsoportok (tiszthelyettesi, zászlósi, tiszti, főtiszti) valamint az adott rendfokozathoz artozó várakozási idők a magasabb ranghoz.

## VÉLEMÉNYEK

A Hivatásos szolgálati törvény a jogalkotó szándéka szerint részletesen szabályozza a hatálya alá tartozók jogviszonyát, munkakörülményeit, a különös részekkel az eltérő feladatú rendvédelmi szervezetek közötti különbségek szabályzását teszi lehetővé.

Tartalmában megjelenik a szabadságszámítás, az érdekképviseleti szerv jogai és a rendfokozatok várakozási idejének meghatározása mellett a fegyelmi szabályok valamint a nyugdíjjal kapcsolatos előírások, tehát valóban sokrétű törvényről van szó.

A folyamatos módosításokkal megpróbálták az aktuális körülményeknek megfelelően fenntartani a törvény állapotát. Sajnos ez bizonyos kérdésekben bonyolultabbá tette a szerkezetét például az illetménypótlékok esetében.

Az érintett területeken tevékenykedő érdekképviseleti szervek véleménye alapján:

- A küszöbön álló Hszt. módosítással nem az a probléma, hogy változik a törvény. Alapvetően sok mindent meg kellene reformálni a tartalmán és ebben mindenki egyetért. A fő gond az, hogy a kormányzat részéről takarékossági szempontból akarnak elsősorban hozzányúlni a szolgálati törvényhez
- Szükséges rekreációs üdülés, kafetéria rendszer létrehozása plusz forrásból.
- Korlátozása annak, hogy személyi forrásból ne lehessen dologiba áttenni pénzeszközöket.
- Legyen döntési kötelezettsége a munkáltatóknak és a kormányzatnak a szakszervezetekkel a tárgyalások során, bízzanak meg jobban az érdekképviseletekben.
- Lehetne rövidebb próbaidőt meghatározni az újonnan belépők számára
- Fontos volna a tiszthelyettesek beosztási illetmény szorzóinak emelése, valamint a továbbjutási lehetőségeinek biztosítása akár közvetlenül a zászlósi állománycsoportba. Jelenleg a tiszthelyettes kevesebb, mint 10 év alatt elérheti az adott beosztás csúcsát.
- Folyamatosan nyílik a tiszti/tiszthelyettesi bérolló. Jelenleg már elérheti az 1:4 arányt is.
- A jelenlegi pótlékrendszer túl bonyolult, körük szűkítése szükséges.
- A szakszervezetek számára plusz érdekérvényesítő eszközök kellenek.
- Alapvetően fontos a Hszt. életpályamodellje miatt, hogy 2/3-os törvény legyen.
- Jelenleg a túlszolgálatért a hivatásos még a rendes illetményüknél is kevesebbet kapnak, mivel a nem rendszeres jövedelem nem tartozik bele. Ez ellentétes a Munka Törvénykönyvének (és a józan ész) logikájával.

Alapvetően nem tartják rossz törvénynek, különösen, hogy a szakszervezeteknek sikerült „beleharcolni” sok fontos részt.

Egy régóta szolgáló hivatásos katonatiszt véleményét kikérve, elmondása alapján a Honvédelmi jogállásúak törvényét, azaz a Hjt.-t számukra jobbnak tartja a Hszt.-nél. Véleménye szerint, mivel a Honvédség feladatrendszere eltérő és más irányítás alatt van, ezért volt szükséges egy más szabályozás. Mivel egy új törvényt kreáltak a hivatásos és szerződéses katonáknak, sokkal összeszedettebbé vált jó szerkezettel és részletes – néha túlságosan részletes - szabályzással. A Hjt. megalkotását az is szükségessé tette, hogy csökkent a Magyar Honvédség szerepe és súlya a fegyveres és rendvédelmi szervek között.

A Fegyveres és Rendvédelmi Dolgozók Érdekvédelmi Szövetsége (FRDÉSZ) elnökével, Kónya Péterrel a Hszt.-vel és annak várható módosításaival kapcsolatosan beszélgettem:

*„Véleményem szerint a Hszt. elavult. 1996-ban a Magyar Honvédség tagjai is ennek hatály alá tartoztak, így meglehetősen militáns törvény lett. Időközben a Honvédség számára új törvényt alkottak és a Határőrségből is rendvédelmi szerv vált, de a Hszt. nevében még mindig fegyveres. A militáns jelleg fölösleges például a tűzoltó vagy a rendőrnyomozó*

*számára. Szükségtelen korlát például az igen szigorú fegyelmi jog, az állampolgári jogok nagymértékű korlátozása vagy az, hogy tűzoltó pártnak tagja nem lehet.*
*A kiszámítható életpályát bonyolították a többszöri –bérrel kapcsolatos – módosítások, a pótlékok szétverik a rendszert. A tiszthelyettesek számára nem biztosít megfelelő előmenetelt, hamar bekövetkezik a „helybejárás”.*
*A szakszervezetek számára korlátozzák a jogosítványaikat. Tekintettel arra, hogy nincs a hivatásosoknak sztrájkjoguk, kompenzálható lenne egy az érdekképviseleti egyeztetések során történő megállapodási kötelezettséggel.*
*Sajnos szinte minden évben módosítják a Hszt.-t és a Hjt-t. Ez nagyfokú bizonytalansághoz vezet. Alapvető különbség a két törvény között, hogy amíg a Hszt. egy életpálya modell, addig a Hjt. az előre vagy ki szemléletű (pl. japán szervezeteknél, ha a dolgozó nem tud folyamatosan magasabb beosztásokba jutni karrierje során, akkor el kell távoznia a szervezettől – a szerző).*
*A szolgálati törvényekben túl sok a –ható/-hető szabály, azaz a munkáltatóra van bízva, hogy odaad-e, megenged-e valamit a beosztottnak.*
*A várhatóan kibontakozócivilesítéssel fölöslegessé fog válni a Hszt/Hjt különbség. Fölösleges és nem hatékony több minisztériumban irányítani a csökkent mértékű fegyveres és rendvédelmi állományt. Jelenleg az Igazságügyi és Rendvédelmi Minisztérium irányítja a Rendőrséget és egyben jogalkotó is. Ez nem megfelelő szervezés és aggályos is.*
*A Hszt. megalkotása mindenképpen nagy előrelépés volt akkoriban a fegyveres és rendvédelmi szféra számára. Elismertté vált a szakma jogalkotó szándéka alapján, a szakszervezeti jogok törvényesítve lettek. A különleges részek megfelelő lehetőséget biztosítanak az eltérő szervek számára. Az illetményalap közös a Köztisztviselői törvénnyel, aminek jó és rossz oldala is van, de inkább jó a hivatásosoknak, mivel azok is köztisztviselők, akik döntenek az illetményalap módosításáról.”*

## ÖSSZEGZÉS

Az érdekképviseleti szervek véleményét szakmailag mindenképpen megalapozottnak kell tekinteni. Megjelenik nézetükben a Hszt. által nyújtott kedvezmények megvonásával szemben, pontosan a kör bővítésének igénye. A szakszervezeti érdekérvényesítési eszközök bővítését szintén igényként jelenítik meg. Egy egyszerűbb, átláthatóbb és lehetőleg 2/3-os törvény mindenki számára megfelelőbbnek tűnik.

A körülbelül 55.000 fős rendvédelmi szervezet és tagjainak helyzete nem elhanyagolható az ország érdekében sem bár a közszolgálatban dolgozóknak csak egy kis részét alkotják.

A megállapításom, hogy a Hivatásos Szolgálati Törvény, azaz a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII-as törvény valóban megérett a módosításra. A tervezetben található módosítások közül van, amelyik minden érintett részéről támogatott (pl.: pályáztatás rendszere) és van, amelyet sokan csak más módon látnak megfelelően (pl.: civilesítés). Egyes megszorító, költségtakarékos intézkedések tervezete nagyfokú bizonytalanságot alakított ki a hivatásos állományban. Már egyre erősebben tapasztalható, ahogyan az idősebb, tapasztaltabb hivatásosok a szolgálati nyugdíjba „menekülnek”. Mivel sok vezetői posztra fiatalokat, kevesebb szolgálati idővel rendelkezőket kell majd tenni, ez a következő években némi problémákat jelenthet.

Látható, hogy a Hszt. alapvetően egy jó, részletes törvény. Többségében megfelelően szabályozza a hivatásosok szolgálati viszonyát. Felmerült az igénye annak is, hogy a civilesítés és a Magyar Honvédség nagyarányú létszámcsökkentése után újra közös törvény szabályozhatná az összes magyar hivatásos élet és munkakörülményeit.

Az ország gazdasági helyzete és teljesítőképessége rányomja a bélyegét a közszférának adható juttatásokra is. Fontos eszköz lehet a köz szolgálatában álló hivatásosok elismerésére

és motiválására a pénzen nem megváltható eszközök használata és megtartása. A kafetéria rendszer bevezetését jó megtartó erőnek gondolom, de csak ha mindez többletforrás biztosításával és nem a jelenlegi lehetőségekből való kigazdálkodással történik. A nyugdíjrendszer átalakítása az ország helyzete miatt érthető, de mindenképpen óvatosan kezelendő. Minisztériumi és országos vezetési szemlélet alapján a nyugdíjjal kapcsolatos szabályokat a már rendszerben lévő hivatásosok számára már csak jogi szempontból sem volna célszerű módosítani.

A szféra legnagyobb veszélye – mind az egyén, mind az ország számára -, hogy a bizonytalan és várhatóan az egyén számára kedvezőtlen változtatások miatt a tapasztaltabb, de lassan már a fiatalabbak is a pályaelhagyáson gondolkodnak. Az új belépőnek jelentkezők átlagkompetenciái valószínűleg elmaradnak az elmúlt évekétől, hiszen a magasabb kvalitásúak nem látják majd megfelelő módon biztosítva az egzisztenciájukat.

Mindezek mellett érdemes figyelembe venni azt, hogy az előrejelzések alapján azok számára, akik az elkövetkező években kitartanak és a pályán maradnak, 2013-tól jobb lehetőségek várnak mind a nyugállományba helyezés, mind a szolgálati viszony körülményei terén.

## FELHASZNÁLT IRODALOM


- A Civilisztikai és Igazságügyi Szakállamtitkár előterjesztése a foglalkoztatási jogviszonyok felülvizsgálatának Hszt-re vonatkozó irányairól, Igazságügyi és Rendészeti Minisztérium, 2006.
- Vadász János előterjesztése a kormány részére az egységes közszolgálati kerettörvény koncepciójáról, Közszolgálati Reform Kormánymegbízotti Hivatal, 2003.
- Koltay Jenő és Neumann László szerkesztésében: Közelkép, Munkaügyi kapcsolatok Magyarországon. 2005.
- Berki Katalin – Suba Katalin: A tizenharmadik havi illetmény története,
- Fundamentum, 2005/4. szám
- Dr. Szakács Gábor: Előtanulmány a hivatásos állomány rendfokozati, illetve bér és besorolási rendszere között meghúzódó ellentmondás feloldására, egy új differenciált bér és besorolási rendszer kialakítására, BM Oktatási Főigazgatóság, 2005.

**Törvények:**

1949. évi XX. törvény, A Magyar Köztársaság Alkotmánya.

1989. évi II. törvény, az egyesülési jogról.

1996. évi XLIII. törvény, a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról.

2001. évi XCV törvény, a Magyar Honvédég hivatásos és szerződéses állományú katonáinak jogállásáról.

**Egyetemi jegyzet**:

Dr. Horváth László: Az országvédelem szervezeti rendszere egyetemi jegyzet (Távoktatási tananyag), ZMNE, Budapest, 2005.