HADMÉRNÖK

A ZMNE BOLYAI JÁNOS KATONAI MŰSZAKI KAR
ÉS A KATONAI MŰSZAKI DOKTORI ISKOLA
ON-LINE TUDOMÁNYOS KIADVÁNYA

V. Évfolyam 3. szám 2010. 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
web: http://hadmernok.hu

Kiadó: Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
Kiadásért felelős: Dr. Lakatos László ny. vezérőrnagy, a ZMNE főtitkára
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Bakosné Diószegi Mónika – Óbudai Egyetem tanársegéd

Bárdos Zoltán pv. alezredes – Fejér Megyei Katasztrófavédelmi Igazgatóság, KMDI doktorandusz

Prof. Dr. Bolgár Judit ny. ezredes – ZMNE KLHTK egyetemi tanár

Dr. Berkovics Gábor ny. alezredes – ZMNE BJKMK egyetemi docens

Bihari Hunor – MH 86. Szolnok Helikopter Bázis

Farkas Csaba – Corvus Aircraft Kft., KMDI doktorandusz

Dr. Földi László alezredes – ZMNE BJKMK egyetemi docens

Illési Zsolt – ZMNE KMDI doktorandusz

Inkovics Ferenc – ZMNE KMDI doktorandusz

Jobbágy Szabolcs főhadnagy – ZMNE KMDI doktorandusz

Dr. Kassai Károly mk. alezredes – HM Informatikai és Információvédelmi Főosztály

Koleszár Béla – ZMNE KMDI doktorandusz

Dr. Kozma Tibor – HBM RFK

Dr. Krajnc Zoltán alezredes – ZMNE KLHTK egyetemi docens

Krasznay Csaba – ZMNE KMDI doktorandusz

Kuris Zoltán – ZMNE KMDI doktorandusz

Lipics László – ZMNE HDI doktorandusz

Miskolczi Ildikó – ZMNE KMDI doktorandusz

Dr. Molnár Mihály ny. alezredes – ZMNE BJKMK főiskolai docens

Prof. Dr. Munk Sándor ny. ezredes – ZMNE BJKMK egyetemi tanár

Prof. Dr. Óvári Gyula ny. ezredes – ZMNE BJKMK egyetemi tanár

Dr. Réger Béla alezredes – ZMNE BJKMK egyetemi docens

Dr. Sándor Miklós ny. ezredes – ZMNE BJKMK főiskolai tanár

Prof. Dr. Solymosi József – ZMNE BJKMK egyetemi tanár, KMDI vezetője

Szegediné Lengyel Piroska – Zsigmond Király Főiskola, ZMNE KMDI doktorandusz

Tamási Béla – ZMNE KMDI doktorandusz

Urbán László – MH 86. Szolnok Helikopter Bázis

Varga Péter – Óbudai Egyetem, ZMNE KMDI doktorandusz

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Berkovics Gábor
berkovics.gabor@zmne.hu

Krajnc Zoltán
krajnc.zoltan@zmne.hu

AIR DEFENCE ARTILLERY IN THE HUNGARIAN ARMY AFTER THE WORLD WAR I

Absztrakt/Abstract

A „Nagy háborút" követően Magyarország úgy politikailag, mint katonailag nehéz helyzetbe került. A trianoni békediktátum akadályozta, megtiltotta egy ütőképes, modern hadsereg kialakítását. A politikai és katonai vezetés úgy döntött, hogy a „határozványok" egy részét nem tartja be. Ennek megfelelően került megszervezésre a tiltott légvédelmi tüzérség is. A cikk bemutatja a magyar légvédelmi tüzérség löveganyaggal történő ellátásának első lépéseit, 1929-ig.

After the Great War Hungary got into a dificult situation both politically and militarily. The Trianon Peace Treaty hurdled and prohibited to develop a powerful and modern army. The political and military leadership decided not to comply some parts of the decisions. Accordingly, the forbidden air defense artillery was organized as well. This article describes the first steps of how the Hungarian anti-aircraft artillery was supplied with cannons, until 1929.

Kulcsszavak/Keywords: *légvédelmi tüzérség, légvédelem,első világháború ~ world war I, air defence, air defence artillery*

INTRODUCTION

After the World War I no state could plan and organize their countries' protection without air defence. The aircrafts did not only do reconnaissance during the war accompanied by a courier service and fire command tasks but increasingly, the bombing of troops and objects as well. It became clear to all individuals and organizations dealing with military issues that the heartland was just as vulnerable as the front. It only depended on the development of their aircraft and armaments.

The future of the winners' will about air defence was evident. On the one hand, their own armed forces were equipped with these weapons, on the other hand, the losers were not only prohibited to manufacture air warfare system and compliance but the ban was also imposed

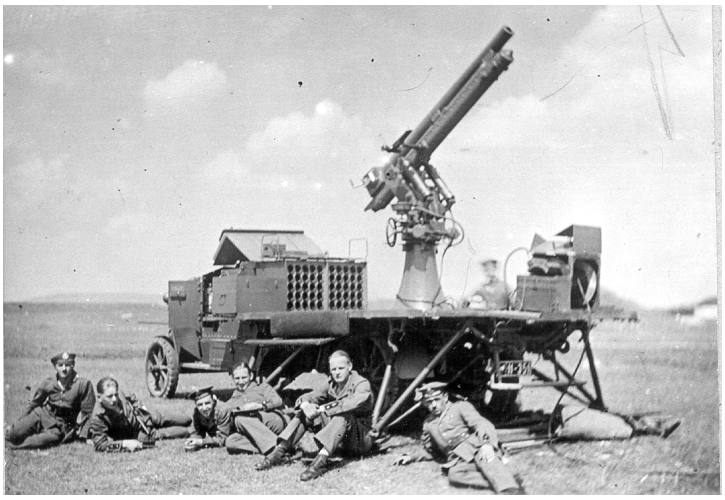
on deploying eliminating weapons. Thus, the losers were not allowed to produce nor to acquire anti-aircraft artillery.

DECISION ON THE CREATION OF AIR DEFENCE ARTILLERY

After the losses of the *"Great War"* and because of the *Decisions1 of the Hungarian Peace Treaty*, Hungary faced great difficulties. The latter deprived the country of the possibility of an active air defence, the former left a very poor legacy in the field of anti-aircraft artillery and aircraft equipment. Yet the experience of World War clearly demonstrated that the air operations will take priority over the next armed conflict.

The Hungarian idea solving air defence (particularly internal air defence) included the following:

1. Passive protection from the land.
2. Active protection from the land.



Picture 1 5/8M légvédelmi löveg
(Hadtörténeti Intézet Fotóarchívuma)

3. Defensive protection/blocking by the shooter forces.
4. Counter offensive, by attacking and retaliatory bombing of the hostile air forces.[2]

The making of the 1st point happened continuously but very slowly, because it cost a lot. For point 4, very strong bomber forces were needed, and Hungary neither then, nor later had them. For us, the 2nd and the 3rd points seemed to be the most appropriate to implement. Truly enough they were also expensive but at least they had the fastest results. The fighters in the anti-aircraft system were effective tools with high agility and also had the power to win a decision.

However, until 1939, they failed to organize a monitoring system which was necessary for their activities and alert in time. It would have been difficult to protect the whole country by fighters because of the size of the area as well. The frontier problem also highlighted the issue of which armament could and should be used: "*Because of the reconnaissance, the fighters cannot operate successfully in 60-80km range. But the protection of a district requires a huge amount of cannon."*[3]

The anti-aircraft artillery, however, had a number of advantages over the hunters:

1. Quick readiness to fight.
2. Permanent readiness to fight in any weather conditions. (If you have the necessary optical and beam materials.)
3. The ability of the long engagement.

---

[1] The Vth part of the Hungarian Peace Treaty – Military, military shipping and ballooning provision - signed 4th June 1920 prohibited to deploy an air force. As the Vth part 1st chapter 108th article stated that 'It is prohibited to use any troops which is not mentioned in the above annexed tables.', neither air force nor air defence cannons could be „kept" by Hungary.

[2] Magyar Katonai Szemle 1932. lvi II. évfolyamának II. évnegyedéhez 5. Füzet, vitéz Szentnémedy Ferenc: A honi légvédelem problémái és korszerű légvédelmi gyakorlatok 110. oldal

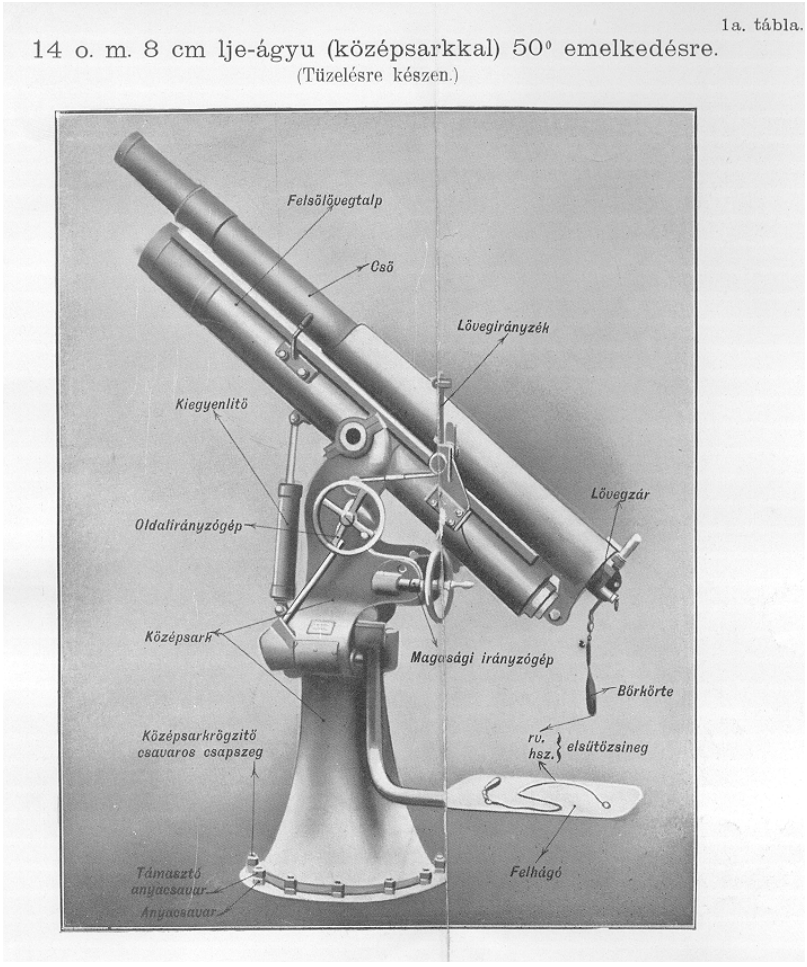
[3] Magyar Katonai Szemle 1933. évi III. évfolyamának II. évnegyedéhez 6. Füzet, Rákosi Béla ezredes: A földről ható aktív légvédelem jelentősége 98. – 99. oldal

4. The greater clarity of reviewing fight.[4]

Naturally, the monitoring and forecasting service was necessary for their work as well, but it was not as crucial as for the fighters. The two arms were equally important for the protection of the country, but in the field of national air-defence the anti-aircraft artillery clearly had to be prioritized.

Their work was defined as follows:

1. making the aerial reconnaissance job difficult.
2. Destroying the bomber aircrafts.



Picture 2 O.M 14 anti-aircraft gun
(Tüzér ismeretek, 14 O.M. 8cm. Légjárműelhárító ágyú 1918. Hadtörténeti Könyvtár, Sz. 64.)

3. Supporting their own aircraft in an air battle.[5]

The statement of one of the soldiers of those times, major József Bálint, indicates the recognized significance of the weapon: *"... there is no air defence , nor home defence without anti-aircraft artillery."*[6] Of course he also added that the tasks must be solved by the two arms together and none of them should be overestimated at the expense of the other. In terms of military applications a *"Bombardier Code of Practice"* got accepted (air defence booklet setting out the principles). In this booklet the idea of placing the weapons in an even order was abandoned, and also stated that it is no use applying anti-aircraft artillery without making the centre of gravity – *"it is pointless and a priori inefficient."* The mixed use of tools also became a principle. There was another argument for strengthening the air defence with cannons and later with defence guns: *the money*! The acquisition of air defence artillery assets and the operation was significantly cheaper than the fighter forces. Truly enough, their efficiency and mobility were significantly lower as well.

The calculations and analysis of Laszlo Captain Frederick in 1940 also showed an acceptable rate for the 20s.[7]

[4] same
[5] Sípos Béla: Honi légoltalom, 25. oldal, 1936. Békéscsaba
[6] Magyar Katonai Szemle 1933. évi III. évfolyamának II. évnegyedéhez 4. Füzet, Bálint József őrnagy: A földről ható aktív légvédelem jelentősége 116. oldal
[7] Magyar Katonai Szemle 1941. évi X. évfolyam 9. Füzet, László Frigyes százados: Gondolatok a légvédelem köréből, 762. oldal

The set up cost of a gun battery:

- 1.2 mP[8]
- 8000 shots for 4 shot guns: 1.2 mP
- Four barrel replacements: 0.16 mP
- Total: 2.56 mP

Captain Laszlo calculated about 0.5 million pengős for a plane, including thee tools and personal preparations. This was generally acceptable to the average, because an HE-111 cost 800 000 pengős, an ME-109 400,000 pengős, an Ar-96 / B, 175,263 pengős in 1941.[9] The prices above may be related to the prices in the 20's as well, as the production and maintenance money in the armament did not change significantly. In his writing he calculated with 1% efficiency (which turned out generally lower in the later military experience), so the damage caused to the enemy could by 40 million pengős. The own expense of spent material and amortized guns was about 0.36 million pengős. This, of course is purely a theoretical calculation, however, when compared with the known data on this forecast, it turned out that it was not totally unfounded. In the battles of the 2nd Hungarian Army the 3 per thousand efficiency of the 29M type anti-aircraft guns was still very good.

In 1920, the General Staff forecast that in a future war the air strikes would have a significant role, and therefore they would have major implications for air defence from the ground as well. The military leadership therefore decided that - in contrast to the peace agreement – they would not give up their anti-aircraft artillery arms, but make it hidden.

THE EARLY HUNGARIAN AIR DEFENCE ARTILLERY

Hungary didn't have the necessary extent of professional subject matter for her own air defence artillery. Only 2-bit and 10-bit 14 5/8M O.M. gun was available for the Army. In addition, the 14 O.M. tools were basically not air defence artillery weapons, they were only used in need for this task and they had low efficiency in it. The main part of the 14 O. M. gun were the tube, the breechblock, the middle-corner, the pedestal ring, the upper cannon pedestal and the gunner. The back funicular-tube device was able to elevate 50, and 70 degrees depending on the applied middle-corner.

The most important technical parameters of the gun are illustrated on Table1.

Table 1

Type Typical	14 O.M.	5/8M
Calibre (mm)	76,5	76,5
Total pipe length (mm)	2284	2298
Projectile initial velocity (m / s)	500	520
Elevation (degrees)	-7 (-10) ÷ 50 (75)	-7 ÷ 75 (85)
Range (m)	7300	9360
Range of high (m)	5000	4800
Rate of fire (rounds per minute)	10 ÷ 15	15
Transport	Towed	automobile, rail
The danger radius around the detonation point (m		25
Bullet weights (kg)	6,5 ÷ 6,6	6,68

[8] *"million Pengős"*

[9] Szabó Miklós: A Magyar Királyi Légierő technikai és szervezeti fejlődése (1938-1944) 1981., 148. oldal

So the Army leadership decided, that despite the prohibitions they would set up and maintain one - at least minimally - operational anti-aircraft artillery of tools. Accordingly, in 1922, the Ministry of Defence decided to continue the production of the gun 5/8M, and they ordered 20 pieces from Diósgyőr Gépgyár, which was later raised to 23. The guns were no longer modern, and they were very slow and difficult to move, however, the decision was motivated by the conceptual design possessed. This anti-aircraft gun consisted of a tube with cannon cradle, a upper cannon pedestal , a lower cannon pedestal and a pedestal ring.

The 5/8M was a middle-cornered tool. In 1923, in the Military Major Group Chief Section it was decided that the guns would be applied on automobiles. The ordered material was produced by 1924. The technical parameters of the asset are in Table1., its limit of power is in Draft1.

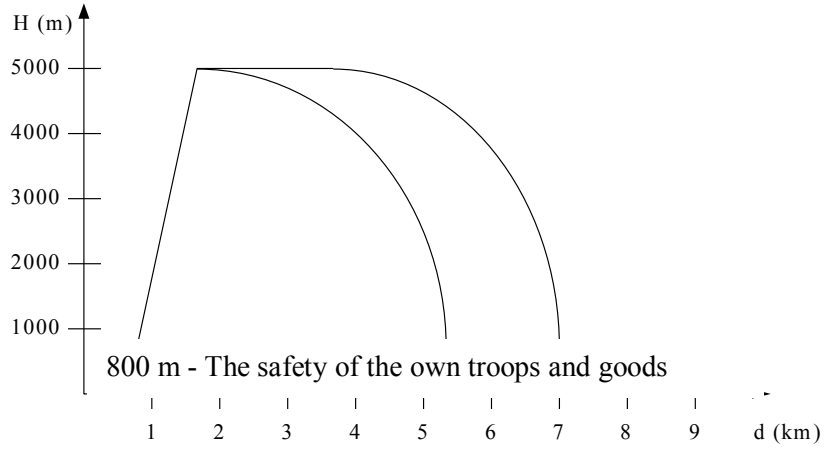
Several solutions were experimented to modernize the gun and the additional instruments. The Technical Research Institute increased the elevation angle from 75 º to 85 º. Later, a new cannon sighting was attached to the anti-aircraft gun, because the original one was outdated and had low efficiency.

DECIDING FOR A NEW WEAPON

In 1928 it finally became clear that the national production of cannons did not bring the expected results. New problems occurred with 5/8M. The cannon barrels burned out quickly, mainly due to the poor quality of raw materials. The experiments on air defence artillery cannons of Technical Research Institute of Experimental neither brought the expected results. The 8.8 cm, 8.35 cm, 8 cm, 7 cm and 6.6 cm calibre guns in fact - except for the 6.6 cm - only existed on the drawing table. In the latter case an experimental piece was constructed in 1927, but its production failed because of the technical difficulties and the opposition of the Chief of Army Staff, because the lowest limit of the calibre was specified as 8cm![10]

Thus, the military was forced to seek for new solutions. According to the regulations of the Peace Treaty we were not allowed to buy military material, so a decision was made to obtain an authorization (license) for manufacturing.

Out of the options, a Swedish 8 cm L/50 model was chosen, the later Hungarian 29M anti-aircraft gun.



The range area of 5/8 M air defence cannon
(Légvédelmi Tüzérségi Szabályzat 3. füzet: Lőutasítás, Budapest, 1938. Attila nyomda részvénytársaság)

[10] Hadtörténeti Levéltár, VKF 1.o. 5381/T 1928.

REFERENCES

[1] Balassa Imre: A 8 cm-es légvédelmi ágyúk, MKSZ 1941/10

[2] Dr. Barcy Zoltán: A magyar légvédelmi tüzérség fejlődése a Horthy korszakban, HL, Tanulmánygyűjtemények

[3] Dr. Barcy Zoltán: A magyar légvédelmi tüzérség fejlesztése és rejtése 1922–1938, Hadtörténeti Közlemények, 1985/4

[4] Dombrády Lóránd – Tóth Sándor: A magyar királyi honvédség 1919–1945, Zrínyi Katonai Kiadó, Budapest 1987.

[5] Dr. Varga József: A légvédelmi tüzérség története a kezdetektől a második világháború végéig, Magyar Honvédség Légvédelmi Rakéta- és Tüzérfőnökség kiadványa, 1996.

[6] A Magyar Békeszerződés (The Hungarian Peace Treaty), Kiadja a M. Kir. Külügyminisztérium Bp. M. Kir. Tud. - Egyetemi nyomda, 1920.

[7] F-21 Tüzérismeretek 14M 8cm légijárműelhárító ágyú, Budapest 1918.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Bihari Hunor
bihari.hunor@gmail.com

Urbán László

AGGASZTÓ KIHÍVÁSOK – PROFESSZIONÁLIS VÁLASZ

Absztrakt

Az emberiség biztonsága továbbra is függ a tömegpusztító fegyverekkel rendelkező nagyhatalmak erőegyensúlyától. Ezt a kényes biztonságot fenyegeti a terrorizmus, melynek legaggasztóbb jellemzője a kiszámíthatatlanság. Potenciális fenyegetésként említhetők a proliferáció, az ipari és természeti katasztrófák, valamint az energiaellátó létesítmények elleni támadások lehetősége.
A megelőzés a védelem leghatékonyabb eszközei közé tarozik, mert az időben megszerzett információ segítségével a megfelelő válaszlépések meghozatalára nyílik lehetőségünk. A Magyar Honvédség a fenti feladatot sugárfelderítés formájában, kiemelten a légi sugárfelderítési feladatok végrehajtását MI-24 harci helikopterekkel oldja meg, melyek fel vannak szerelve egy speciálisan erre a célra kifejlesztett sugárfelderítő konténerrel. A cikk a fenyegetettség bemutatása után a légi sugárfelderítés jelenlegi hazai, katonai állapotát, a folyamat ismertetését tűzte ki célul, átfogó képet adva a légi sugárfelderítő konténeres repülés menetéről.

The security of mankind is depending on the balance of nuclear world-powers. This fragile security is deterred by terrorism which most frightened feature is the unpredictability. We can mention as potential threat the proliferation, the industrial and natural disasters or possibilities of attacks against electric systems. Prevention is one of the most effective part of defend. Information gained in time give possibility to make the best answer. Hungarian Home Defence Force can obtain basic NBC information by NBC reconnaissance, according to the article by airborne NBC reconnaissance. This task is solved by MI-24 combat helicopters and a special appliance called airborne reconnaissance container. The article shows the present situation of Hungarian military NBC air reconnaissance giving a picture about the method of preparing and doing an NBC recce flight.

Kulcsszavak: *ABV felderítés, légi sugárfelderítés, helikopter, speciális képesség ~ NBC reconnaissance, NBC recce flight, helicopter, special capability*

Konfliktusokkal teli világunkban az emberiség biztonsága továbbra is függ a tömegpusztító fegyverekkel rendelkező nagyhatalmak erőegyensúlyától. A kölcsönös félelmen alapuló egyensúlyi játék egy újabb, kíméletlen elemmel bővült, melyre leginkább az jellemző, hogy kiszámíthatatlan, és nem korlátozódik a katonai célpontok elleni hadviselésre. Ez a biztonságot fenyegető veszélyforrás a terrorizmus, melynek legaggasztóbb jellemzője a kiszámíthatatlanság. Az előre nem látható támadások ellen védekezni, azokra felkészülni komoly kihívás a nemzetek számára, ezért szükséges az állandó helyzetértékelő és felderítő rendszerek felállítása, fejlesztése. A terroristák kezében olyan fegyverek, támadásra alkalmas eszközök halmozódnak fel, amik olcsón előállíthatóak, elemei az átlag polgár számára is viszonylag könnyen megszerezhetőek. Ebből adódik a következtetés, hogy igenis számíthatunk vegyi, biológiai, vagy radiológiai eszközök bevetésére.

Az atomfegyverek továbbra is a hatalomgyakorlás és a megfélemlítés alapvető eszközei. Ezek adják a kölcsönös hadászati biztonsági garanciát a nagyhatalmak közötti egyensúly fenntartásához. Békeidőben azonban nem a csapásból származó sugárhelyzet felmérése az elsődleges feladat, hanem a terroristák által létrehozott radiológiai fegyverek, vagy a nukleáris balesetekből származó sugárhelyzet detektálása válik kiemelkedő fontosságúvá. A NATO 1999. évi stratégiai koncepciója kiemelten kezeli az atom, biológiai és vegyi terrorizmusból eredő veszélyeket. Alap koncepciója, hogy elsődleges cél az ABV[1] védelem és az ABV felderítés fejlesztése, hatékonyságának növelése. A megváltozott célkitűzéseket egyébként már az 1998-ban kidolgozott STANAG[2] 2112 is tartalmazza, amely többek között foglalkozik az alacsony szintű sugárzásból adódó ABV események felderítésével.

A Magyar Köztársaság nemzeti biztonsági stratégiája [1] a biztonsági környezet értékelése kapcsán a fenyegetések, kockázati kihívások tekintetében elsők között említi a terrorizmust, a tömegpusztító fegyverek elterjedését és a környezeti hatások fontosságát. A Nemzeti Katonai Stratégia erre alapozva, értelemszerűen szintén potenciális fenyegetésként említi a fentieket, kiegészítve az ipari és természeti katasztrófákkal, valamint az energiaellátó létesítmények elleni támadások lehetőségével. Nem szükséges külön magyarázat ahhoz például, hogy a paksi atomerőmű helyzetét illetően mennyire fontos a téma feldolgozása. A Magyar Köztársaság 1999-ben csatlakozott a NATO-hoz, ezzel az elfogadott "Biztonság és védelempolitikai irányelvek" szerint a Magyar Honvédség feladatrendszere kiegészült. A szerződés 5. cikke szerinti kollektív védelem kötelezettsége mellett kijelölt egységei részt vesznek mind hazai, mind a szövetség határain kívüli békeműveletekben is. Ezen műveletek során a csapatokat a tömegpusztító fegyverek hatásain túl nagyobb valószínűséggel fenyegetik az ipari katasztrófákból (például nukleáris, vegyipari) eredő veszélyek.

Az ABV védelem három pillére (elkerülés, védelem, mentesítés) különböző technikai fejlesztéseket kíván meg. Az elkerülés, vagy pontosabb szóhasználattal a megelőzés a védelem leghatékonyabb eszközei közé tarozik, hiszen az időben megszerzett megfelelő mennyiségű és minőségű információból olyan döntések meghozatalára nyílik lehetőségünk, amelyek alapján elkerülhető a védelemi és mentesítési folyamatok nehézkes végrehajtása. Az információgyűjtés fontos feltétele, hogy gyors legyen, valamint a gyűjtött adatok feldolgozásra kész állapotban kerüljenek a mérést végző egységtől a feldolgozást, majd kiértékelést végző egységen át a döntéshozóig. Mindezek ismeretében kijelenthetjük, hogy a gyalogos, gépjárműves, valamint bármilyen földfelszíni mérési módszer lassúnak és nehézkesnek minősíthető, mivel nem teljesíti az elvárt gyorsasági kritériumot. Továbbá minden légi műveletről kijelenthetjük, hogy mozgékonysági foka, sebessége, a feladathoz

[1] Atom-, Biológiai-, Vegyi-
[2] Standardization Agreement (NATO Egységesítési Egyezmény)

való alkalmazkodási képessége jóval felülmúlja a földfelszíni módszereket. Lényeges feltétel, hogy a mérést végző személyi állomány megfelelően védve legyen a vizsgált anyagok káros hatásaitól. Ezt a célt elérhetjük úgy, hogy olyan eszközzel végezzük a felderítést, mely garantálja a személyi állomány megfelelően hatékony védelmét, vagy alkalmas a szennyezett terület gyors elhagyására bármikor, bármilyen irányban megfelelően nagy sebességgel.

A címben megfogalmazott professzionális válasz nem más, mint hazánk jelenlegi légi sugárfelderítő képessége. A Magyar Honvédség a fentiekben felsorolt kritériumok mindegyikének maradéktalanul megfelelő műszaki és technikai eszközökkel el van látva, a sugárfelderítési feladatok végrehajtásához mindennemű feltétellel rendelkezik. A légi sugárfelderítési feladatokhoz rendelkezésünkre áll a MI-24 harcihelikopter, amely megfelelően gyors ahhoz, hogy az adatgyűjtési időt nagyságrendileg csökkentse a hagyományos módszerekkel szemben, valamint gyorsasága révén a személyi állomány rövidebb ideig legyen kitéve a felderítés alatti káros hatásoknak, továbbá szükség esetén a vizsgálat helyét nagy sebességgel, bármilyen irányban képes elhagyni. A helikopterre felfüggeszthető egy, speciálisan erre a feladatra kifejlesztett sugárfelderítő konténer, amely alkalmas csapásból származó vagy balesetből eredő sugárhelyzet felmérésére, valamint pontszerű radioaktív sugárforrások felderítésére. A gyűjtött adatok kiértékelésére van kiképzett szakszemélyzet, akik el vannak látva megfelelő szoftverrel, melynek eredményeképpen a mérésből származó adathalmaz a kiértékelés után közvetlenül alkalmas a döntéshozó informálására, valamint további hadműveleti tervezőmunkára történő felhasználásra.

A légi sugárfelderítés szükségességét alátámasztó tényezők

A NATO elveinek figyelembe vételével Magyarország, mint tagállam nem törekszik a katonai képességek teljes spektrumának kialakítására, hanem a szükséges területekre összpontosít, szakosodott- és hiányzó képességek életrehívásával igyekszik megfelelni a szövetségi rendszer kihívásainak. Olyan képességeket kell megtartanunk, és lehetőség szerint továbbfejlesztenünk, amelyekhez a fennálló gazdasági és technikai feltételek mellett a legtöbb, már meglévő forrás adott. A cikk egy ilyen képességre, nevezetesen a légi sugárfelderítésre kívánja ráirányítani a figyelmet.

A védelem és biztonság kockázati elemzésekor meg kell határoznunk azon területeket, amelyek a legnagyobb mértékű kockázatot hordozzák magukban, a bekövetkezés lehetősége a más várható eseményekhez képest nagyobb, valamint végrehajtása nem várható el más együttműködő szervtől. Ilyen alapvető feladat lehet a paksi atomerőmű, mint stratégiai jelentőségű veszélyes ipari létesítmény, továbbá a katonai és stratégiai létesítmények védelme.

A bevezető részben felsorolt konkrét tények és indokok alapján, bizonyítottan égető szükség van olyan eszközre, mely haladéktalanul a feltételezett helyszínre érkezhet és megkezdheti felderítő munkáját annak érdekében, hogy mielőbb pontos információkkal rendelkezhessünk a kialakult helyzetről.

Egy másik megközelítésből is átgondolhatjuk a légi felderítés egyedülálló előnyeit: Ha a támadás valamely nukleáris létesítmény ellen irányul, amely lehet atomreaktor, hasadó vagy radioaktív anyagot raktározó hely, szállítóeszköz, akkor nagy valószínűséggel a kiszóródás akár óriási területet szennyezhet be, radioaktív termékekkel kontaminált terepet hozva így létre. A terület nagysága miatt létfontosságú, hogy az előidézett és várható következményeket mielőbb felderíthessük. Gyorsaságunk révén további emberi életeket menthetünk meg, mivel

gyorsan és pontosan tudunk információkat gyűjteni a szennyeződés mértékéről és kiterjedéséről. Ilyen esetben nem a költséghatékonyság az elsődleges feladat, de fontos megemlíteni, hogy egy adott területet egyetlen helikopter is képes igen rövid idő alatt felderíteni, míg ugyanezen feladathoz nagy létszámú földi eszközpark igénybevétele és lényegesen több idő volna szükséges.

Adódik tehát a kérdés: mit tehetnek a nemzetek, szűkebben Magyarország a támadás kivédése, vagy a már bekövetkezett csapás (vagy baleset) gyors helyzetértékelése, felszámolása érdekében?

A Magyar Honvédség lehetőségei

A katonai, vagy katasztrófa-elhárítási műveletek ABV szennyezettségi körülmények között sokrétűvé, bonyolulttá válnak. Lehetnek olyan esetek, amikor a feladatot egyéni vagy kollektív védőeszköz készletben kell végrehajtani. Jelentős probléma a tömegpusztító fegyver első használata, vagy a tragédia után fellépő sokk is. Azokon a területeken, ahol ilyen eset fordul elő, a veszély napokig, sőt hetekig fennállhat a csapás után. Ha ilyen területen kell feladatot végrehajtani, akkor megbízható ismeretek szükségesek arról, hogy mely területek, utak járhatóak, objektumok és infrastruktúra használható, illetve melyek nem.

Az ABV védelem magában foglalja az ABV fegyverek és más forrásból származó szennyeződések hatásai ellen alkalmazott védelmi rendszabályokat, intézkedések létrehozásának és végrehajtásának módszereit, terveit, eljárásait és kiképzési követelményeit. Ez a feladatkör alapvetően a számvetés, előrejelzés és a felderítés speciális eszközeire épül. A hadműveleti tervezéshez, vagy a katasztrófavédelmi feladatok végzéséhez szükséges az aktuális helyzetkép folyamatos ismerete, egy minden pillanatban megbízható adatokat szolgáltató rendszer üzemeltetése. Értelmezni, elemezni és értékelni kell a kialakult helyzetet a lehető legpontosabb felderítési adatok alapján. Ezen rendszerre építve lehetséges válaszlépések sorát, cselekvési változatokat lehet felvázolni a döntéshozás érdekében. Magyarországon polgári és honvédségi vonalon egyaránt működik e célból ABV felderítő-elemző rendszer, melynek vannak közös elemei - mint az AMAR állomások (Automatizált Adatgyűjtő Rendszer) -, valamint a rendszerek, információk átjárhatósága, a koordináció központi szinten is biztosítva van. Azonban jelenleg csak a honvédség rendelkezik légi sugárfelderítő képességgel.

Típusválasztás

A légi sugárfelderítési eljárásmód kiszolgálásához a repülőeszközök közül a helikopterek felelnek meg leginkább. Igen kedvező a repülési sebességtartományuk, nagy előnyük az egy pont feletti függeszkedési képességük és az alacsony repülési magasság. Magyarországon a szakállomány a MI-24 harcihelikopter típus mellett döntött olyan kedvező tulajdonságai miatt, mint: a túlélőképesség, sokoldalúság, hatótávolság, sebesség, illetve a személyzet védelme.

Alapvető bármilyen művelet végrehajtásakor a személyzet, technika túlélőképessége. A MI-24 harcihelikopter jelenleg a világ egyik legjobb típusa többek között ezen a téren is. Hatékony páncélzata, különböző fedélzeti és technikai rendszereinek védelme és azok duplikáltsága miatt a komoly kockázatú, nagy fenyegetettségi fokú területeken is sikeresen és biztonságosan hajtja végre a kijelölt feladatait. Üzembiztonság tekintetében szintén elmondható, hogy a világ élvonalába tartozik. Alátámasztja ezt az a tény is, hogy magyarországi üzemeltetése során nem fordult elő a helikopter meghibásodásából eredő katasztrófa. [2]

A legfőbb ok, ami miatt erre a típusra esett a választás a sugárfelderítési feladatok végrehajtásakor, az előbbieken túl a szerkezeti felépítésében keresendő. Mivel túlnyomásos, hermetizált a tehertér és a kabin, valamint aktív szénszűrővel, fedélzeti sugáradag-mérővel van ellátva, így korlátlan műveleti képességet tudhat magáénak ABV körülmények között üzemeltetve is. Ez a képessége eredményezte azt, hogy a fent említett feladatkörben szerepet kapjon.

Nem csak ipari katasztrófák esetén lehet szükség napjainkban légi sugárfelderítésre, hanem terrorista események kapcsán is, amely terrorista csoportok ellen alkalmazva a típus rendelkezik a szükséges felderítést biztosító képességgel, valamint hatékony fegyverzettel a csoportok megsemmisítésére vagy önvédelemi célokra.

Légi sugárfelderítés konténeres változata

A légi sugárfelderítés végrehajtása a Gamma Műszaki Zrt. által kifejlesztett és 2005 őszén rendszerbe állított konténer segítségével zajlik. Az eszköz képes a csapás vagy baleset következtében kialakult sugárhelyzet gyors felmérésére, valamint pontszerű sugárforrás helyének gyors behatárolására. A konténer helikopterre szerelt változatát az 1. számú ábra szemlélteti.

1. számú ábra
A légi sugárfelderítő konténer függesztve MI-24 harci helikopteren

Természetesen a rendelkezésre álló eszközökkel, mint például az IH-31L légi sugárfelderítő műszerrel folytak ilyen irányú repülések és feladat-végrehajtások korábban is. Meg kell jegyezni azonban, hogy ezen eszközök érzékenysége és pontossága kívánnivalót hagyott maga után, mivel eredetileg földi sugárfelderítésre tervezték ezeket. A környezeti tényezők és a repülés paramétereinek folyamatos változása nagyban befolyásolta a kapott adatok pontosságát és feldolgozhatóságát. Összességében a légi járművek fedélzetén elhelyezett mérőműszerek a repülési magasság függvényében szorzószámokra alapozott eljárással számították ki a földi sugárzásra vonatkoztatott felderítési adatokat, így viszonylag pontatlan eredményeket kaptak.

Jellemzője volt az akkori feladat-végrehajtásnak, hogy a repülőeszköz fedélzetére egy vegyivédelmi szakember is beült. Elsődlegesen a saját szakterületével volt tisztában,

működtette a felderítő berendezést, a kapott mérési adatokat pedig a nála lévő térképen rögzítette. Ez a folyamat azonban nagyarányú figyelmet és koordinációt követelt a hajózó és a vegyivédelmi szakember között. Továbbá a térképen való tájékozódás magas szintjét igényelte, ebből következően igen képzett szakemberek voltak szükségesek a feladat manuális megoldásához.

A már említett IH-31L műszer az 1980-as években került kifejlesztésre. A kor színvonalának megfelelő műszer volt, azonban az érzékenysége csupán atomcsapásból származó sugárzás kimutatására tette képessé. Az akkori elvekkel összhangban a szembenálló felek tömeges atomcsapására készült a vegyivédelmi szolgálati ág, ami után nagy intenzitású radioaktív sugárzás várható. Ezek nagyságrendjének, körülbelüli értékének meghatározásához a korábbi, IH-5 és IH-3M típusú sugárzásmérő műszer érzékenysége is elegendőnek bizonyult. Ezeket a műszereket a repülőeszköz fülkéjében vagy a hajózó, vagy a vegyivédelmi szakember kezelte. A műszerek érzékelő egységét egyes esetekben a repülőeszközök törzsén kívül helyezték el konzolok segítségével.

A felderítő repülések, illetve mérési feladatok végrehajtására a helikopterek közül jobbára a MI-1, MI-2, MI-4, MI-6 típust alkalmazták, míg a rendelkezésre álló repülőgépek közül a PZL-101, Z-37 Csmelák, Super Aeró 45, L-200 Morava, Z-326 és Z-526 kiképző változatait, az AN-2-t vagy esetenként a LI-2 repülőgépet vetették be. Az AN-2 és LI-2 repülőgépek, valamint a MI-4, MI-6 helikopterek kimondottan légi sugárfelderítési feladatok végrehajtására csak a legritkább esetben voltak alkalmazhatók, mivel ezeknek a típusoknak ilyen célra való felhasználása nem volt gazdaságos. Egyéb szállítási feladataik végrehajtása közben azonban – kiegészítő feladatként – megbízhatónak bizonyultak. [3]

A konténer felépítése

A konténerben két nukleáris detektor, GPS-vevő, barometrikus magasságmérő és egy adatgyűjtő található, amely képes fedélzeti adatgyűjtő- és kiértékelő programmal ellátott kézi számítógépnek adatot küldeni, vagy a memóriájába elraktározni.

Az előbbiek alapján a felderítés elvégezhető úgy is, hogy nincs a fedélzeten felderítő személyzet és számítógép. A gyűjtött adatok a felderítés végeztével olvashatók ki az adatgyűjtőből, ilyen esetekben a kiértékelés a földön történik.

A konténerben ki van alakítva a rádióadó helye is arra az esetre, ha földi állomás számítógépe felé kell valós idejű, úgynevezett on-line megoldással küldeni az adatot. További lehetőségként opcionálisan a konténerbe videokamera is beszerelhető, aminek segítségével felvételeket is tárolhat vagy küldhet a konténer a felderíteni kívánt területekről.

Az eszköz érzékelő egysége, a BNS-98 típusú dózisteljesítmény-távadó és az NDI/SK típusú intelligens szcintillációs nukleáris detektor látószöge 45^{o}-ban, kúposan van leárnyékolva ólomköpennyel. Így a berendezés alatt levő területről gyűjt csak célzottan sugárzási adatokat. Ez a megoldás eredményezi azt, hogy 100 méteres repülési magasság esetében a konténer 100 méter széles sávot képes a felszínen felderíteni.

A konténer alkalmazása

A Magyar Honvédség 86. Szolnok Helikopter Bázis egyik végrehajtó alegységénél, a Harcihelikopter zászlóaljnál került rendszeresítésre a sugárfelderítő konténer. A hajózó állománya által kidolgozott számítógépes alkalmazás, egy felhasználói program a szükséges

számításokat a repülési feladatokhoz elvégzi az alapadatok bevitele után. Ezek a bevitt tényezők a felderíteni kívánt terület vonatkozásában: koordináták, pásztázási távköz, terület geometriai jellemzője.

Itt érdemes magyarázatot fűzni ahhoz, hogy miért fontos a terület alakja. A vegyivédelmi szakterület számításaiban a szél sebessége és iránya fontos tényező, ez határozza meg a szennyeződés haladását és terjeszkedését. Amennyiben a szél sebessége 10 km/h alatti, akkor feltételezhetően a szennyező anyag lassan, de minden irányban terjeszkedni fog, ezáltal egy körhöz hasonlatos képet mutat a térképen. Ha azonban 10 km/h feletti szélsebességről van szó, abban az esetben a szennyeződés már haladni fog szélirányban, de terjedni fog oldalirányban is, ezért egy körcikk-szerű képet kapunk. Természetesen az ellipszis vagy téglalap azért szükséges, hogy a matematika nyelvén könnyebben meghatározható és felderíthető célterület-formátumot adjunk meg alapadatnak. Ez univerzálisan használható feladatszabás elrendelésekor.

A terület meghatározása után a repülési feladat alapadatai következnek: föld feletti magasság, föld feletti repülési sebesség, feltöltött üzemanyag mennyisége, számított felszállósúly.

Szükséges még a meteorológiai paraméterek ismerete a terület vonatkozásában repülési szempontból is, úgymint: szélirány, szélsebesség.

A felderítési eljárás első eleme tehát az útvonal megtervezése a kapott koordináták, vagy a célterület ismeretében. A feladat egy meghatározott terület felderítése, Amelynek a határoló vonalait, koordinátáit a vegyivédelmi szakember megadja, ezáltal meghatározva azt a helyet, amelyről információt kíván kapni.

Ettől a ponttól kezdve a hajózók feladata az, hogy a valós végrehajtás módját kidolgozzák. Az aktuális időjárási viszonyoknak természetesen döntő szerepe van. Akár meg is hiúsíthatja a repülést a látási viszonyok drasztikus romlása, vagy a viharos erejű szél. Ha nem ilyen szélsőséges esetet nézünk, abban az esetben is a légmozgásnak meghatározó szerepe van, hiszen a területen uralkodó jellemző szélirány nagyban befolyásolja a helikopter üzemanyag fogyasztási tényezőit, az időtényezőt és a végrehajtás pontosságát is.

A pásztázási vonalak fordulópontjai, a párhuzamos egyenes pályák tartása, lekövetése ugyan a helikopter fedélzetén alkalmazott GPS berendezés segítségével viszonylag pontosan végrehajtható, azonban a szélirány, szélsebesség és főleg a széllökések hatása nehezen kiszűrhető, igen nagy gyakorlatot igényel a hajózó állománytól.

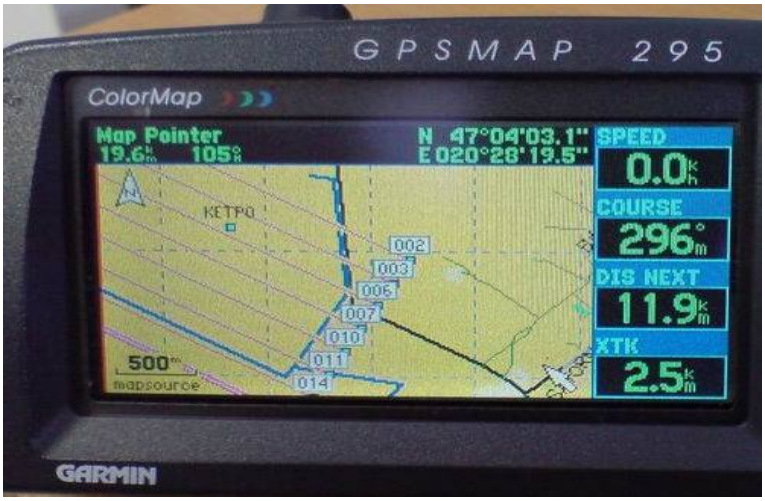
Az uralkodó szélirány ismeretében a pásztázási vonalakat úgy határozzák meg, hogy azok párhuzamosan fussanak a széliránnyal. Így nehézséget csak az jelent, hogy a szélsebességet és a helikopter haladási sebességét folyamatosan figyelemmel kísérje, korrigálja a hajózó. Értelemszerűen széliránnyal szemben haladva a szél sebessége a helikopter „ellen” dolgozik. Nem kell viszont a hajózónak az oldalszélre külön fokozott figyelmet fordítania.

Régebben a terület ismeretében a repülési feladat kidolgozását az adott alakulat vegyivédelmi szakembere és a felderítést végrehajtó hajózó személyzet együtt, több térképen oldotta meg, mivel mindenképpen kellett vegyivédelmi katona a repülőgép fedélzetére a sugárfelderítő berendezés kezelésére, miként erről már szóltunk is néhány bekezdéssel ezelőtt. Az útvonal tervezésekor a vizuálisan jól megkülönböztethető, könnyen látható tereptárgyak adták a sarokpontokat.

Szembetűnő az erőfeszítés, amire a navigáció, terepfelismerés terén kényszerültek a légi felderítést végrehajtó katonák a navigációt segítő olyan berendezések hiányában, mint amilyen napjainkban a GPS.

Ma már a GPS eszközök felhasználásával a tereptárgyak csak megkönnyítik a feladat pontos végrehajtását, de nem alapvető feltételei annak. Ha a meghatározott terület és az elöljáró úgy rendeli, akár a 100 méteres pásztázási távolságot is képes a hajózó személyzet tartani. Így 120 km/h sebességgel, ami a meghatározott paraméter szennyezett terület felderítésekor, óránként 12 km^2-ről készülhet igen nagy pontosságú, valós idejű felderítési eredmény.

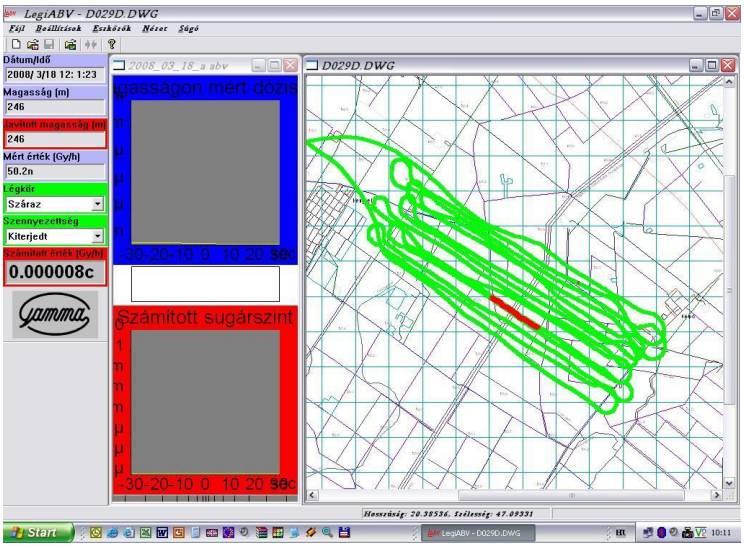
A 2. számú ábra egy GPS kijelzőjén megjelenített, megtervezett útvonalat mutat, ahol a számozott jelek a fordulópontokat mutatják. Halvány rózsaszín árnyalattal pedig a párhuzamos egyenesek kerültek jelölésre, melyek mentén a hajózó a felderítést végzi. Nagy segítség a repülés közbeni tájékozódáshoz a tereptárgyak jelölése is, amit a technika jelen állása már képes megoldani.



2. számú ábra
Felderítési útvonal GPS-be táplálva

A 3. számú ábra az előbbi GPS kijelzőn megjelenített, megtervezett útvonal számítógépen kidolgozott változatát mutatja. Itt az alapadatok bevitelre kerültek, így a fordulópontok felszerkesztése és a térképen való rögzítése is megoldott. A korábban már említett táblázatos alkalmazási programfelület meghatározza ezeket a koordinátákat, majd azok térképen ábrázolhatók és digitálisan a GPS memóriájába tölthetők.

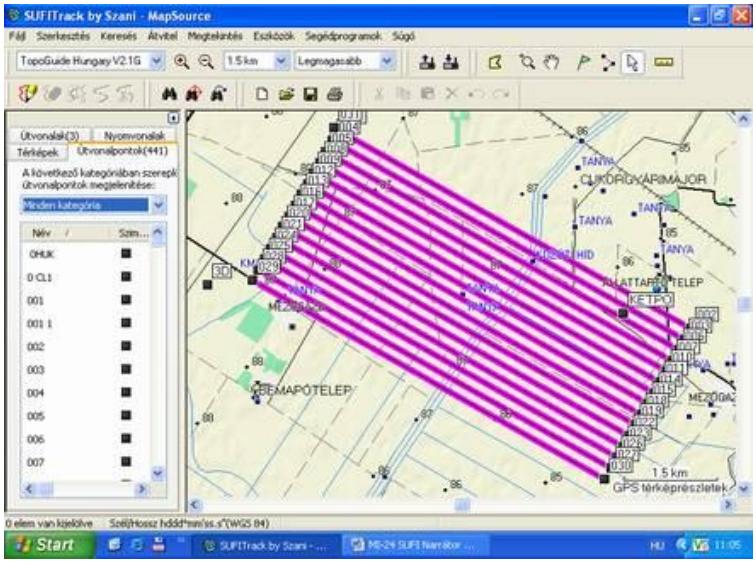
A bemutatott tervek értelemszerűen megadják a vázát a felderítési folyamatnak. Azonban az időjárási körülmények (oldalszél, széllökések) következtében a valós repülési útvonal némiképp eltérést mutat a mértani egyenesektől.



3. számú ábra
Valós, végrehajtott repülési útvonal számítógépes ábrázolása

A 4. számú ábrán egy végrehajtott útvonal mérési eredményei láthatók, ahogyan azt a konténer GPS berendezése rögzítette. A program panel a LégiABV elnevezésű feldolgozó és megjelenítő program felülete, melyet a Gamma Műszaki Zrt. fejlesztett ki a légi sugárfelderítés adatainak további feldolgozásához és térképi megjelenítéséhez.

A felderítési feladat végeztével a térképre dolgozott, valamint a kiértékelő program által mutatott eredmény együttesen a 4. számú ábrán látható. Itt a zöld színnel jelölt vonal a normál háttérsugárzási értéket, a piros színnel kiemelt vonal pedig az ettől eltérő sugárzási szinteket ábrázolja.



4. számú ábra
Felderítési útvonal számítógépen szerkesztve

A Légi Sugárfelderítő Csoport

Az előbbiekben felvázolt feladatot a Magyar Honvédség 86. Szolnok Helikopter Bázis által működtetett Légi Sugárfelderítő Csoport hajtja végre állandó készenléti szolgálat keretein belül. A szolgálatot hajózó és repülőműszaki állomány látja el, feladata a nagykiterjedésű területek légi sugárfelderítésének gyors végrehajtása, a terep sugárszintjének megállapítása, illetve pontszerű sugárforrás(ok) felderítése. A légi sugárfelderítő repülést az állomány a harckiképzési utasítás ide vonatkozó gyakorlataiban foglaltak szerint hajtja végre.

Ezek a gyakorlatok határozzák meg röviden az egyes felderítési, földközeli repülési feladatok végrehajtását. Magukban foglalják a gyakorláshoz szükséges repülési óra számát, idejét, a gyakorlat célját, a végrehajtás feltételeit és a biztonsági intézkedéseket. A hajózó személyzet ezek által szerez jártasságot a későbbi valós felderítő repülésekhez.

Szennyezett terepszakasz felderítése esetén 150-200 m repülési magasság között, valamint 150-180 km/h sebességgel végzik a felderítést. Pontszerű sugárforrás felderítése esetén 100 m alatti repülési magasságon, 100-120km/h közötti sebességgel hajtják végre a feladatukat, amennyiben a vegyivédelmi szakterület ettől eltérően nem határoz.

A hajózó személyzet nukleáris balesetelhárítási védőkészletet visel a hajózó ruhája fölött, ami egy szabvány kezeslábas öltözet csuklyás kialakítással, vékony polietilén anyagból. A védőoverall megfelelő bőrvédelmet biztosít a 0,5 mikrométernél nagyobb átmérővel rendelkező részecskékkel szennyezett területen. A gázálarccal együtt a védőoverall biztosítja a bőr és a légzőszervek védelmét a radioaktív aeroszol részecskékkel szemben, azaz a bőrfelületi kontakt egészségkárosító hatással, és a belégzés útján történő inhalációs hatásokkal szemben.

A szűrőbetét nem az általánosan alkalmazott aktív szénnel kialakított típus, hanem a nagyon apró részecskék kiszűrésére szolgáló változat, amely szintén 0,5 mikrométernél nagyobb átmérőjű részecskék szervezetbe jutása elleni védelemre lett kifejlesztve.

Jelenleg még nincs rendszeresítve a hajózó állomány számára kialakított speciális MEHARA típusú gázálarc, valamint a hatályos légügyi törvények jelenleg nem engedélyezik a gázálarcban történő repülést. A rendszeresíteni kívánt eszköz bevizsgálása megtörtént. A szükséges jegyzőkönyvek elkészültek, így belátható időn belül rendelkezni fog a végrehajtó állomány megfelelő eszközzel a gázálarcos repüléshez.

A feladatok végrehajtása hermetizált fülkében történik, szűrőn keresztüli levegő beáramoltatással, ezáltal a személyzet egészsége nincs kitéve káros hatásoknak. A jelenleg alkalmazható 93M típusú gázálarcot kizárólag csak a kihermetizálás előtt veszik védelmi helyzetbe.

Összegzés

Fontos kiemelni azt a tényt, hogy a létrehozott sugárfelderítő eszköz a kor technikai színvonalához képest is fejlettnek mondható. Állíthatjuk ezt azon okból, hogy mind a hordozó eszköz, mind a mérést végző egység a feladat végrehajtására tökéletesen alkalmas, a technikai igények közül a legtöbb követelménynek megfelel, tehát nem egy átmeneti állapotról, hanem egy működő és egyedülálló képességről van szó! Természetesen a fejlesztéseket mindig érdemes folytatni. Még megoldásra vár a konténer valós idejű elérése, és az on-line adattávadás hatótávolságának növelése. Mindazonáltal kijelenthetjük, hogy hazánkban nincs

még egy olyan légi sugárfelderítő eszköz és eljárás, amely ennyire komplex rendszert alkotna, és az adott szakfeladat végrehajtására ennyire alkalmas lenne. [4]

Az adatgyűjtő rendszer magas színvonalán túl a kiértékelés folyamata is minden igényt kielégítő. A kapott adatok, azáltal, hogy grafikusan történnek megjelenítésre egy térképi felületen, minden szakág által egyszerűen értelmezhetőek és kezelhetőek. Ez azért fontos előrelépés, mert a szaktevékenység már nem egymást követő tevékenységek sorozata, hanem egyszerre képes dolgozni az adatokkal a vegyivédelmi, a hadműveleti, és a repülést tervező szakember is.

Nagy előny az is, hogy a konténer által gyűjtött adatsor a vegyivédelmi szakág adatforgalmában szabványosított karakteres formában is kinyerhető, így az közvetlenül továbbítható a Magyar Honvédség Atom-, Biológiai-, Vegyi Riasztási és Értesítési Rendszer elemein keresztül a forrásszinttől a Nemzeti ABV Központba. Ez a fajta adatsor a NATO bármely tagállamában alkalmazható.

Az adatokat feldolgozó szoftver maradéktalanul alkalmas a kialakult helyzet értékelésére. A helyzetmegítélés folyamán, térképen kerül rögzítésre a hadműveleti tervezést befolyásoló minden lényeges adat. A szoftver képes előrejelzést készíteni, így a bekövetkezendő események előtt lehetséges az adott veszélyeztetett területen tartózkodók riasztása.

Tisztán leszűrhető az a megállapítás, hogy ABV eseményeknél a gyorsaság, reagáló képesség, a korrekt számvetések készítése döntő jelentőségű. Ebben kiemelt szerepe van úgy a repülést végrehajtó és kiszolgáló szakszemélyzetnek, mint a fejlesztések eredményeként meglévő ABV felderítő technikának. Előre megjósolható, hogy az elkövetkező évek alacsony szintű védelmi költségvetése és a világgazdasági válság továbbra sem teszik lehetővé - az ország elé célul tűzött és felvállalt - haderő-modernizációs feladatok maradéktalan végrehajtását. Pedig a javaslatok döntő része azon területeket favorizálja (például: ABV védelem), amelyek a védelmi felülvizsgálati reformtervben is elsőbbséget élveztek, és ténylegesen szükségesek lennének ahhoz, hogy képességfejlesztésben az áttörés bekövetkezzék. [5] Tény, hogy a XXI. század hajnalán egyértelműen ebben az irányban kell keresni az előrelépés lehetőségeit. Informatikai társadalmunknak az élet minden terén alapadatokra, információkra van szüksége. Ezek begyűjtése mindinkább elektronikus eszközök alkalmazásával valósul meg (AMAR állomások, légi sugárfelderítő konténer…). Így tehát ezek korszerűsítése az egyik fő fejlődési irány.

A sugárzásmérő eszközök területén a csernobili katasztrófa után elkezdett intenzív hazai fejlesztések olyan eredményeket hoztak - az alacsony szintű radioaktivitás méréstechnikájában is – ami által jelentős előnnyel rendelkezünk több NATO országgal szemben.

A Gamma Művek Zrt. - a légi sugárfelderítő konténer megalkotója - jelentős kapacitást fordít olyan vegyifelderítő eszköz megalkotására, melyet a már meglévő légi sugárfelderítő konténerbe integrálva további fejlődést eredményez. Szintén ők azok, akik a konténer elektronikus adatgyűjtőjét rádiós egységgel szerelik fel, illetve kamerát helyeznek el benne. Így valós idejű adatátvitelt, ezáltal valós idejű, azonnali helyzetértékelést tesznek lehetővé. Az új elképzeléseket az 5. számú ábra mutatja.

Másik fejlődési irány, illetve előrelépési lehetőség a MI-24 helikoptertípus hadrendben tartása az összes lehetséges eszközzel. Ez alatt nagyjavítások végrehajtása, újabb

modifikációk megvásárlása vagy esetleges gépbeszerzések értendők a fent bemutatott igen kedvező tulajdonságai miatt.

5. számú ábra
A légi sugárfelderítő konténer adattovábbító antennával, kamerával

A már említett Nemzeti Katonai Stratégia [6] képességalapú haderőfejlesztést említ. Ennek elemei között szól helikopterek modernizációjáról és újak beszerzéséről. Amennyiben ez megvalósul, relatívan kis összegből - amibe a sugárfelderítő konténerek legyártása kerül - világszínvonalú képesség alakítható ki, NATO tagságunk, illetve nemzetközi megítélésünk mérlegét kedvezőbbé téve. A NATO vegyivédelmi szakembereinek figyelmét annyira megragadta a szabványos, NATO keretein belül alkalmazott NBC jelentések készítésére is alkalmas, kiértékelő szoftverrel felügyelt rendszer, hogy javasolták a magyar felajánlások közé felvenni ezt a képességet.

Hivatkozások

[1] A Magyar Köztársaság Nemzeti Biztonsági Stratégiája (2073/2004. (III.31.) Kormány Határozat)

[2] Orosz Zoltán – Rolkó Zoltán: A MI-24 harcihelikopter hosszú távú alkalmazása. In: 2236/2003. (X.1.) kormányhatározat a Magyar Honvédség számára megfogalmazott feladatok tükrében. Repüléstudományi közlemények on-line tudományos folyóirat, "Fél évszázad forgószárnyakon a magyar katonai repülésben " című konferencia kiadványa, 2005. április 15. (http://www.szrfk.hu/rtk/kulonszamok/2005_cikkek/orosz_zoltan_rolko_zoltan.pdf)

[3] A terep légi sugárfelderítése (Vv/32). Bp.: Zrínyi Nyomda, 1959.

[4] Zelenák János — Nagy Gábor — Csurgai József — Molnár László— Pintér István — Baumler Ede — Solymosi József: A légi sugárfelderítés képességei

alkalmazhatóságának vizsgálata elveszett vagy ellopott sugárforrások felkutatása, illetve szennyezett terepszakaszok felderítése során. Hadmérnök, 2009. március (http://hadmernok.hu/2009_1_zelenak.pdf)

[5] Szenes Zoltán: Magyar Honvédség a NATO-ban. Mit várunk Rigától? In: Hadtudomány, 2006. (16. évf.) 4. sz. 23. old.

[6] A Magyar Köztársaság Nemzeti Katonai Stratégiája (1009/2009. (I. 30.) Kormány határozat) In: Magyar Közlöny, 2009. 12. sz. 4125. old.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. szeptember

Bakosné Diószegi Mónika
dioszegi.monika@bgk.uni-obuda.hu

Solymosi József
Solymosi.Jozsef@zmne.hu

NÖVÉNYTERMESZTÉSI ÉS ÁLLATTENYÉSZTÉSI „VEGYES" GAZDASÁGOK HULLADÉKAINAK ENERGETIKAI HASZNOSÍTÁSA

Absztrakt

Hazánk energia kiszolgáltatottsága igen nagyfokú. Az energiabiztonság növeléséről nem csak beszélni kell. Számos intézkedéssel erősíteni, különböző támogatási rendszerrel pedig ösztönözni kell az energiaszektorban beruházni kívánókat. Serkenteni kell a kihasználatlan, és éppen ezért napjainkban csak egyfajta „tartalékként" jelen lévő kapacitások kiaknázását. Cél a minél többféle energiaforrásra támaszkodó gazdaságok kiépítése, az alternatív energiaforrások felhasználásának fejlesztése. 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 és állattenyésztési hulladék biogázként hasznosítható energetikai lehetőségekről.

Hungary is definitely exposed to the energy market. Not only should lip service be paid to increasing energy security. Potential investors in the energy sector should be strengthened by a variety of measures and encouraged by various support schemes. Exploitation of now unused"reserve" capacities should be stimulated. The objective is to build economies relying on the largest number of energy resources possible. Owing to Hungary's outstanding natural endowments and its livestock breeding history of several centuries, there are extremely promising openings for biomass energy. This publication provides a brief overview of the opportunities in energetic for using the great amount of agricultural and livestock breeding waste generated in Hungary as biogas.

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

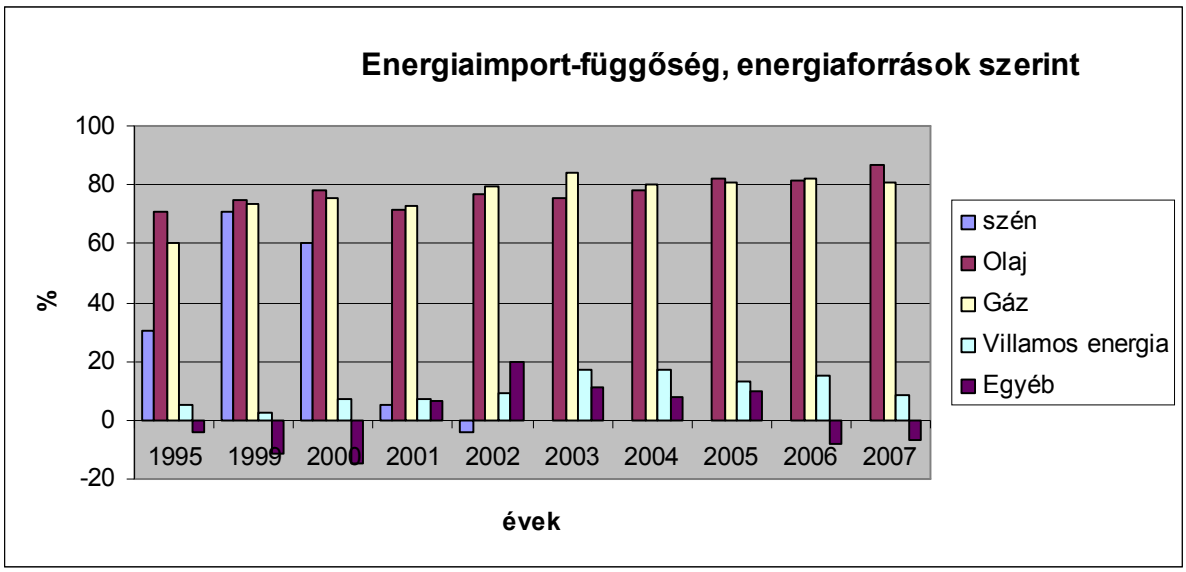
ENERGIAFÜGGŐSÉG

Az Európai Unió energiafelhasználásának több mint fele importból származik. 2008-ban a 27 tagállam energiafelhasználásának 53,8%-a származott külső forrásból. Nettó exportőr ezen időszakban csupán Dánia volt. [1] A kőolaj és a földgáz tette ki a behozatal legnagyobb részét. Legfontosabb beszállítók Oroszország ahonnan az import kőolaj 30%-a, és a földgáz 40%-a érkezett, továbbá Norvégia, ami 16%, illetve 23%-kal részesedett az uniós energiaimportból. [2]

Magyarország energiaigényét tekintve a tagállamok között a középmezőnyben foglal helyet, ugyanakkor energiafüggősége átlag feletti (1. táblázat). 2007-ben és 2008-ban az energiafelhasználás több mint 60%- a importból származott.

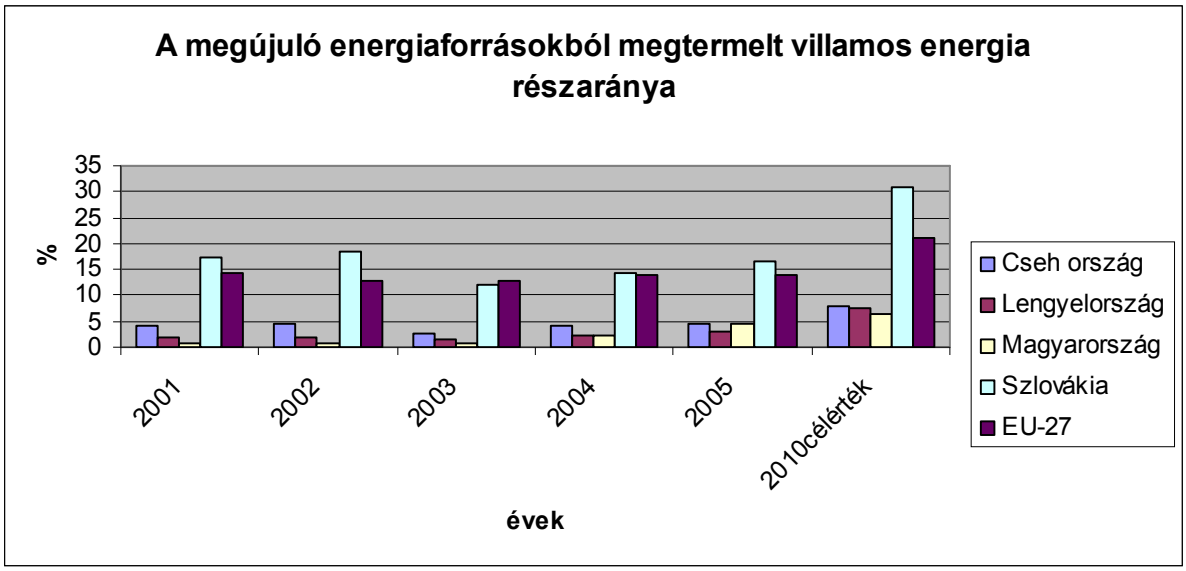
Energiaimport-függőség %-ban meghatározva										
Évek	1995	1999	2000	2001	2002	2003	2004	2005	2006	2007
összesen	47,8	53,2	55,2	53,3	57,2	62,1	61,1	63,5	63,1	62,8

1. táblázat Magyarország energiaimport változása az elmúlt években [2]



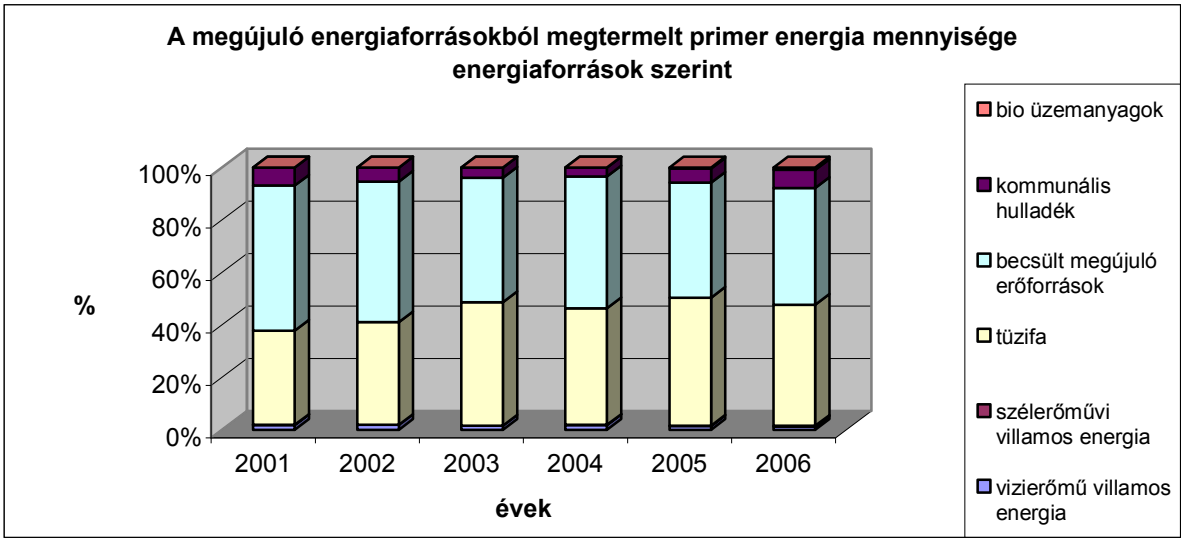
1. ábra Az energiafüggőség indikátora: nettó import mennyiség elosztva a bruttó belföldi energia felhasználással [3]

A honi energiafogyasztás fedezetének hiánya főként az olaj és a földgáz nagyfokú felhasználásából adódik. Az 1990-es évek elején kezdődött gázprogram hatásra mind a közületek, mind a lakosság jelentős mértékben állt át földgázfogyasztásra. Ennek köszönhető az 1995-től kezdődő gáz „függőség" további több mint 20%-os hiány növekedése (1. ábra). Az így megnövekedett nyersanyagigény magával hozta a gáz nagy mennyiségű importját, ami kiszolgáltatottá tette hazánkat a térség szeszélyes kül- és belpolitikai viszonyainak. A készletek csökkenése, egyre dráguló kiaknázása és szállítása miatt a földgáz ára az utóbbi években drasztikus növekedést mutatott. Ehhez járult hozzá az ország gyengülő gazdasága és nagy költségvetési hiánya miatt megszűnő fogyasztói gázár támogatás.



2. ábra A megújuló energiaforrásokból megtermelt villamos energia részaránya %- os értékben [3]

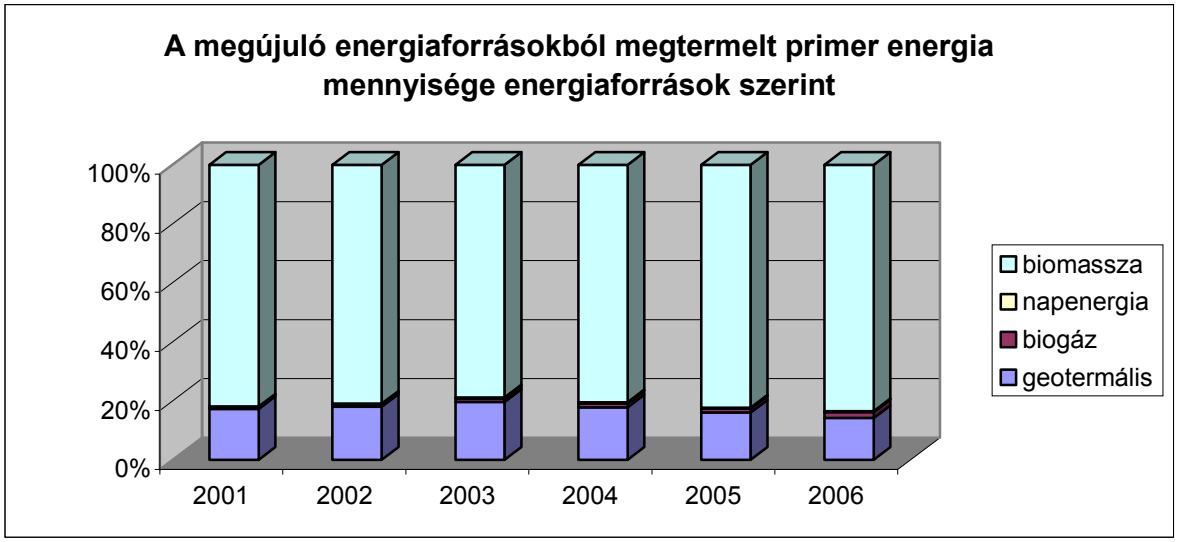
A világ villamos energia előállításának kb. 90%-a fosszilis energia segítségével történik. Magyarországon ez az arány az atomenergia nagyobb részarányának köszönhetően 60 % körüli. Az egyre növekvő energiaéhség és az ezzel együtt járó villamos energiatermelés iránti növekvő igény komoly környezeti terhelést jelent környezetünkre, valamint előre vetíti a fosszilis energiaforrások kimerülésének felgyorsulását. Ennek védelmében az EU stratégiai célkitűzése a megújuló energiák részarányának jelentős növelése a villamos energia előállításában is (2. ábra).



3. ábra A megújuló energiaforrásokból megtermelt primer energia mennyisége energiaforrások szerint, kilótonna olajegyenértékben[4]

A megújuló energiaforrásokból megtermelt primer energia javarészt tűzifa és további biomassza felhasználásával került előállításra (3. ábra).

Ezen belül is a biogázzal megtermelt primer energia mennyisége növekedett - közel 5-szörösével- a legnagyobb mértékben az elmúlt években 2,6%-ról 12,6%-ra (4. ábra).



4. ábra A megújuló energiaforrásokból megtermelt primer energia mennyisége energiaforrások szerint, kilótonna olajegyenértékben [4]

ALTERNATÍV LEHETŐSÉGEK

Az alternatív energiákra való igény drasztikusan emelkedett az elmúlt években. Ennek oka a legelterjedtebb energiahordozók készletének kimerülése és emiatt azok magas árai. Fejlett társadalmakban kialakulóban van, az un. tudatosabb környezetvédelmi életmód, amelynek felhívásaival nap, mint nap találkozik az ember a médiákban vagy rendezvényeken, kampányokon keresztül. Az „új" energiahordozók bevezetése- mivel az ilyen rendszerek kiépítése igen nagy költséggel jár- természetesen állami szerepvállalás nélkül elképzelhetetlen. A régmúlt időkben alkalmazott módszerek mára már új technológia segítségével, nagyobb hatásfokkal alkalmazhatók. Gondoljunk csak bele a korszerű víz- vagy szélerőművek teljesítményébe, melynél még a csapágyazás kialakításánál is figyelembe veszik a felesleges súrlódási energia – mint veszteség- csökkentését. Ide sorolható a modern tüzelési technikák –faelgázosító kazánok – bevezetése, aminek köszönhetően az eltüzelt biomasszából nyerhető energia hatásfoka jelentősen emelkedett a régi kályhák vagy kandallókéhoz képest.

A minket körülvevő természet számtalan hasznosítható energiát tartogat a számunkra. A fejlett társadalmak feladata ezek feltárása, kiaknázása anélkül, hogy azzal maradandó károkat okoznánk egyre sebezhetőbb bolygónkon.

Megnevezés		Energia PJ/év
Dendro massza		
	tűzifa	20-22
	energiaerdő	30-32
	vágási hulladék	5…7
Növényi biomassza		
	gabonatermékek melléktermékei	10…12
	egyéb növényi melléktermékek	30-50
	termesztett energianövények	30-40
	bio- hajtóanyagok	4…6
Másodlagos biomasszák		
	hígtrágya	0,7…0

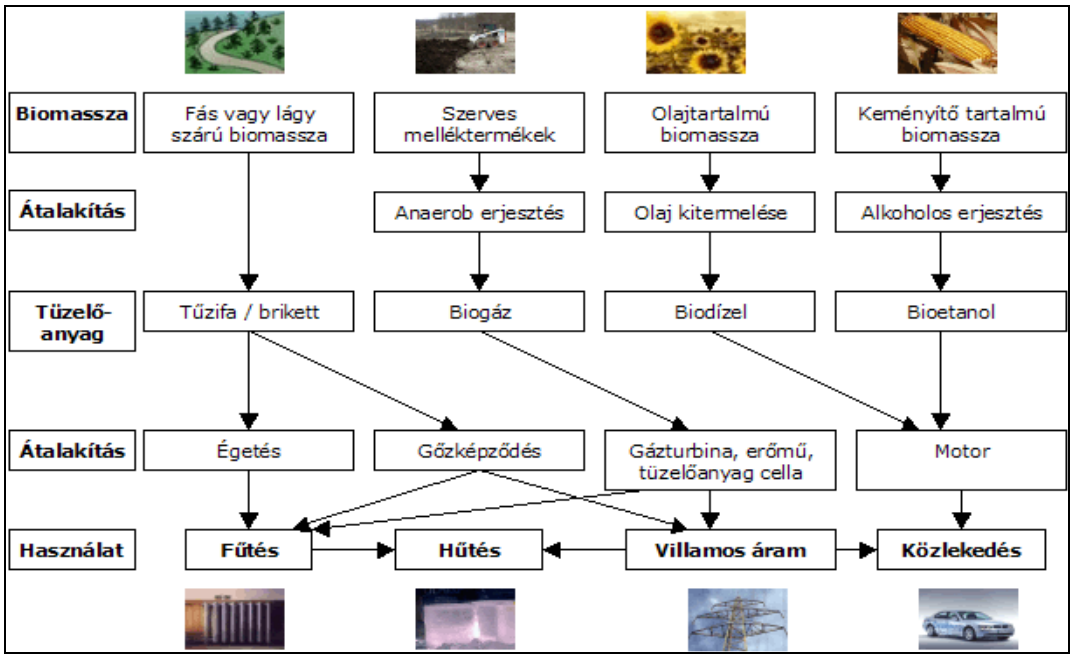
	állati hulladékok, melléktermékek	1,3…5
	feldolgozási hulladékok	5…7
Harmadlagos biomasszák		
	élelmiszeripari hulladékok	3…5
	élelmezési hulladékok	6…9
	szennyvízkezelés iszapjai	15-40
	kommunális bio hulladék	30-80
összesen		200-320

2. táblázat Biomassza potenciál Magyarországon [3]

Magyarország biomassza készlete szerteágazó és emiatt nehezen meghatározható. A KEOP (Környezet és Energia Operatív Program) előzetes felmérései és becslése alapján az 2. táblázat tartalma szerint Magyarország biomassza tartaléka jelentős. Ha figyelembe vesszük az ország 2007-es összes energiafogyasztását (1115PJ), akkor látható, hogy annak legrosszabb esetben is az 1/5-ét képes lenne fedezni.

Az értekezésünk kizárólag olyan energia hasznosítására terjed ki, ami a megújuló energiák, azon belül pedig a biomassza csoportjába tartozik. Kutatásunk emiatt egy szűkebb körének hasznosítására korlátozódik, mely nem főtermékként termesztett növényzet vagy tartott állat, hanem mezőgazdasági, állattenyésztési, vagy ipari főtevékenység hulladékaként áll rendelkezésre.

Vizsgáljuk meg a biomasszát, mint potenciális energiaforrást!



5. ábra A biomassza hasznosíthatósága energia nyersanyagként [5]

A csoportosításból remekül észrevehető, hogy a rendelkezésünkre álló biomassza energiává történő átalakítása igen sokrétű. Azt, hogy melyik módszert alkalmazzuk- égetés, rothasztás, erjesztés vagy olajkitermelés- mindig az ésszerűség dönti el.

Egy tisztán mezőgazdasági terület vagy erdőgazdaság a tevékenysége során keletkezett melléktermékét valószínűleg égetési eljárással fogja hasznosítani.

Általános tanyasi gazdaságot vizsgálva - ahol növénytermesztés mellett nagy szerepet kap az állattenyésztés is - ugyanakkor nem csak növényi eredetű hulladék képződik. Számolni kell fás vagy lágyszárú hulladékkal, keménytő tartalmú növényzettel, állati trágyával, állati

hulladékkal. Olyan eljárást kell alkalmazni, ami e vegyes hulladékban rejlő energiát maradéktalanul kiaknázza.

Az alapanyag összetételére érzékenyen, változó hatásfokkal reagál a tüzelési eljárás. Nem beszélve az olaj kitermelésről vagy az alkoholos erjesztésről, ahol a kívánt hatásfokhoz előírás az alapanyag homogenitása, valamint magas olaj és keményítő tartalma.

A biogáz előállításánál alkalmazott anaerob erjesztés, azaz eljárás, ami megfelel e vegyes összetételű hulladék energiává történő átalakításának.

BIOGÁZ, MINT MEGOLDÁS

A megújuló energetikai eljárások között különleges helyet foglal el a biogáz előállítása. Ezzel az anaerob technológiai eljárással sikeresen lehet „kezelni" a szennyezések szerves frakcióját. A hulladék kialakulását nem szünteti meg, ugyanakkor arra kiválóan alkalmas, hogy környezetbe kerülését megakadályozza, lehetőséget nyújtva közben „zöld energia" előállítására. Ily módon, a környezetre káros anyag felhasználásával számunkra fontos termék - energia - nyerhető.

A szerves anyagokban lekötött szén elgázosodása a biogáz. Mindenből nyerhető biogáz, aminek az alapja szerves anyag (szénhidrát, szerves zsír, fehérje).

A biogáz alapanyagai:

1. fás vagy lágyszárú növényzet
2. mezőgazdasági hulladék
3. állati trágya
4. állati hulladék (tetem)
5. szennyvíz

Bárhol, a természetben található szerves anyag bomlása közben keletkezik biogáz. A folyamat - ami a mesterségesen létrehozott biogáz telepen zajlik le - csupán biztosítja és egyenletesebbé teszi a természet útján amúgy is bekövetkező kémiai reakció egyenletességét és jó hatásfokát.

A szerves anyag lebontását a metánbaktériumok végzik. Ezek optimális működéséhez az alábbi feltételek szükségesek:

1. oxigénmentes környezet
2. állandó 20-30 ^{0}C feletti hőmérséklet, sötétség
3. 50% feletti nedvességtartalom
4. 7-7, 5 pH érték
5. elegendő Nitrogén tartalom

Ezeknek a követelményeknek egy tartály tesz eleget (un. fermentor).

A különböző alapanyagokat aprítás és homogenizálás után juttatják el a speciális tartályba. Állandó hőmérsékleten tartva folyamatos keverés mellett az anyag az anaerob térben lebomlik 2/3 részt metánra és 1/3 részt széndioxidra.

A metán %-os értéke adja a biogáz értékét, energiatartalmát. A földgázhoz képest, ami csaknem 100%-os metántartalmú a biogáz kb. 55-70%-os metántartalommal rendelkezik. A metán tartalom nagyban függ az alapanyag összetételétől. A minőséget, ill. az energiahozamot lehet növelni, un. elő - ill. utó fermentorok sorba állításával Az előbbi a kb. 30-35 ^{0}C-os mezofil fermentor, az utóbbi az 50-55 ^{0}C-os termofil fermentor.

Biogáz főként baktériumok aktivitása során keletkezik, habár néhány gomba illetve alacsonyabb rendű állati szervezet is részt vesz az anyagok lebontásában. A mikrobák szaporodása és a biogáz képződése a természetben igen lassan megy végbe. A bomlási-átalakulási folyamat minden egyes anyagnál más és más ütemben zajlik. A cellulóz alapú anyagok lebomlási ideje nagyon hosszú: 40-50 nap, míg az állati eredetű anyagoké csupán

8-20 nap. A gáztermelés is hasonlóan alakul, mint a folyamat időtartama. A gyorsan lebomló anyag arányos idő alatt nagyobb mennyiségű gázt termel. Nagyon fontos tehát, hogy a hulladékokat úgy válogassák össze, hogy a leghatékonyabb legyen a biogáz üzem működése. Csak több komponensű biomasszával biztosítható a kiegyensúlyozottabb gáztermelés.

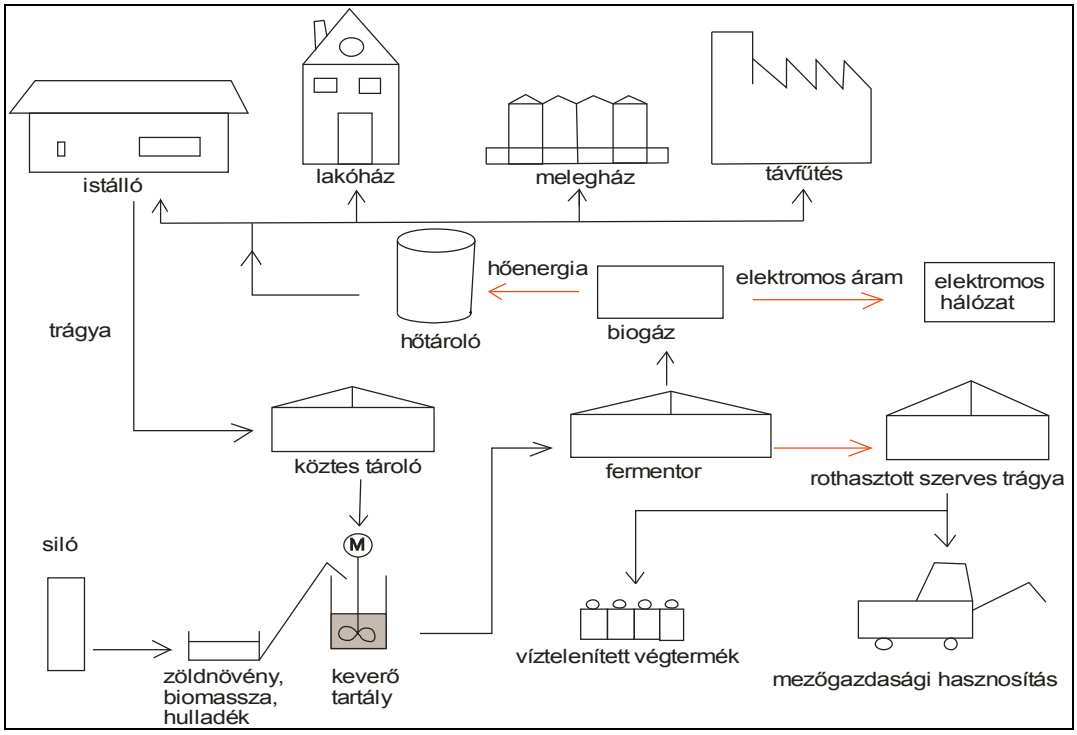
Bár minden szerves anyag lebomlásakor nyerhető metán gáz, természetesen a különböző széntartalmú anyagok különböző metántartalommal bírnak gázosításukkor.
Az alábbi táblázat tartalmaz néhány alapanyagra vonatkozó értéket.

		Biogáz (l/kg)			Hasznosítható
		alsó	felső	átlag	biogáz (l/kg)
Állati trágya	sertés	340	550	445	338
	szarvasmarha	90	310	200	152
	baromfi (csirke)	310	620	465	353
	baromfi (pulyka, liba)	455	505	480	365
	ló	200	300	250	190
	istálló almos trágya	175	280	225	171
	juh	90	310	200	152
	nyúl	380	464	422	321
	Prémes állatok	347	413	380	289
Hazai m.g-i	búzaszalma	200	300	250	190
melléktermék	rozsszalma	200	300	250	190
	zabszalma	290	310	300	228
	kukoricaszár, csutka	380	460	420	319
	napraforgószár	279	321	300	228
	repceszalma	180	220	200	152
	rizs szalma	170	280	225	171
	burgonyaszár	280	490	385	293
	paradicsomszár	361	385	373	283
	vágott cukorrépafej	400	500	450	342
Használt ker-	fű	280	550	415	315
tészeti növény-	elefántfű	430	560	495	376
	nád-káka	170	260	215	163
	lóhere	430	490	460	350
	zöldséghulladék	330	360	345	262
	palántamaradék	602	638	620	471
	lomb	210	290	250	190
	vegyes mg-i hulladék	310	430	370	281
Szennyvíz iszap		310	740	525	399

3. táblázat Különböző alapanyagokból nyerhető biogáz mennyiség [5]

A 6. ábra ismerteti egy sematikus biogáz telepen zajló gázképződés fő lépéseinek folyamatát, állomásait és berendezéseit. Az állattenyésztésből és a növénytermesztésből visszamaradó szerves „hulladék” külön- külön történő tárolása és aprítása után homogenizálásuk következik. Ezt követően kerül az energia alapanyag az előzőekben említett fermentorba. A 6. ábrán egy fermentoros telepet tüntettünk fel, de mint már korábban ismertettük, a lehetőségeknek megfelelően ebből kettő különböző hőfokú fermentort is lehet sorba kötve alkalmazni a hatásfok növelése érdekében. A fermentorban képződött gáz a gépházba érve gázmotor segítségével hő és villamos energiává alakul. A hőenergiát hasznosíthatják a gazdálkodó telep egységei, esetleg egy közeli lakótelep. A villamos energia a törvényben előírt módon, kötelező átvételi áron, előzetesen kötött szerződés alapján az országos rendszerbe kerül.

A fermentorból elvezetett, tovább nem bontható anyagot kapunk végtermékül a kitűnő minőségű biotrágyát. Ez egy gyűjtő tározóból – a trágyázási idénynek megfelelően - visszakerül a gazdálkodó mezőgazdasági területeire, vagy a felesleg további értékesítésre, mint értékes mezőgazdasági tápanyag.



6. ábra Biogáz-telep sematikus vázlata

Az anaerob kezelés ezáltal kulcseljárás lehet a szennyezések eltávolításában, lebontásában, újrafelhasználásában, megújuló energia előállításában, egyéb technológiákkal kombinálva, pedig további értékes melléktermékek nyerhetőek. Ez az eljárás igen sokféle termék (biogáz, „bio földgáz”, elektromos áram, szén-dioxid, használati melegvíz, hajtóanyag, biotrágya) előállítására képes, ezek egyikének (a „zöld” villamos áram) átvételét pedig kedvező és évente szabályozott áron garantálja az állam.

SZABÁLYOZÁSOK ÉS TÁMOGATÁSOK TÜKRÉBEN

Tanulmányunk elején kitértünk arra, hogy a fejlett országok tudatos környezet és energiapolitikája egyre nagyobb hangsúlyt kap. Ennek oka az energiafüggőség, valamint az időjárás egyre szembetűnőbb szélsőséges ingadozása, melyet nagymértékben az ember okozta levegő, talaj és vízkészlet szennyezése vált ki. A legtöbb Európai ország olaj és gázfüggősége

nagyon magas. Néhány helyen, köztük Magyarország is, elérheti a 70-75 %-ot is. Stratégiai szempontból ennek az aránynak a csökkentése égetően sürgős és fontos feladat.

Az alábbiakban összefoglaltuk a szabályozásokat, célkitűzéseket és kötelezettségeket, amik az alternatív energia felhasználását szorgalmazzák.

Az Európai Unió 2010-ig előírt célkitűzései mind a két problémát - környezetszennyezés és energiafüggőség- próbálják orvosolni.

Közösségi akciójavaslat az EU bizottságának kiadásában az un. Fehér Könyv (1997): a megújulókból származó energia arányának növelése 2010-re érje el a 12%-ot.

2003/70/EK Irányelv: Az EU megújított stratégiája (SDS) konkrét célkitűzéseket fogalmaz meg a megújuló energiaforrások részarányának növelésére, miszerint 2010-re átlagosan az energiafogyasztás 12%-ának, továbbá közös, de differenciált célkitűzésként a villamosenergia-fogyasztás 21%-ának megújuló energiaforrásból kell származnia, és emellett vizsgálni kell ezen arányok 2015-ig 15%-ra való emelésének a lehetőségét.

2003/30/EK Irányelv: az összes forgalomba hozott közlekedési célú benzin és dízelüzemanyag vonatkozásában 2010-ig a bio üzemanyagok aránya érje el legalább az 5, 75%-ot.

Kifejezetten az energiafüggőség csökkentését kívánja előtérbe helyezni a 2006-os „Európai stratégia az energiaellátás fenntarthatóságáért, versenyképességéért és biztonságáért” című un. Zöld Könyv. Célként tűzi ki az alacsony széntartalmú energiaforrásokból származó villamos energiatermelés támogatását, a belföldi megújuló energia szerepének növelésével. Fontos cél továbbá az „Energiahatékonysági Akcióterv”, az 1%-os energiacsökkentés elérése.

Támogatásként az EU 1973/2003/EK rendelete az energetikai célú növénytermesztést 45 EUR/ha díjazza.

Az országban 2007-2013-as időszakra vonatkozó energiapolitikai elképzelések szerint 2010-re 6, 5% (ez meg is valósul), 2013-ra 11,4% megújuló részesedést kell elérni a villamos energiatermelésben. Míg az összes megújuló energiák részaránya 2010-ben legalább 8,2%-t kell, hogy kitegyen.

Itt fontos megemlíteni, hogy a 63/2005/OGY –en megállapított támogatások között szerepel a „zöld” villamos energia kötelező átvétele a törvényben meghatározott fix áron. Valamint a biogáz telephez kapcsolódóan- szintén ezen OGY eredményeként- szorgalmazza elősegíteni annak rácsatlakozását a meglévő gázrendszerbe.

Kötelezettsége van országunknak továbbá, a Kiotói egyezményben rögzített üvegházhatású gáz kibocsátás csökkentésére az 1990-es bázisévhez viszonyítva.

2010-es időszakon túlmenően - a GKM (volt Gazdasági és Közlekedési Minisztérium) által kidolgozott terv betartása esetén – cél, hogy 2013-ra a megújuló energiaforrás az országos villamos energia-felhasználás 11, 4%-át, az összes energia- felhasználás pedig 14%-át fedezze.

A szabályozások és iránymutatások ösztönzésére és betartatására természetesen a legjobb biztosíték az anyagi támogatás. Az alábbiakban a teljesség igénye nélkül ragadtunk ki egy párat.

A fenntartható fejlődés uniós irányelve szempontjából a 2007-2013 közötti Új Magyarország Fejlesztési Terv egyik kiemelkedően fontos része a Környezet és Energia Operatív Program (KEOP), amely az élhető környezeti megoldásoktól kezdve, a megújuló energiaforrások lehetőségein át vizeink védelmén keresztül számos programcsomagot tartalmaz.

A KEOP akciótervének egyik fő pontja a biogázra vonatkozik:

„A növényi eredetű és hulladék alapú, valamint az állattartó telepeken keletkező trágyából és a szennyvíztisztító képződő szennyvíziszapból előállított biogáz hasznosítása hulladékkezelés és energiatermelés szempontjából is előnyös, hő- és villamos-energiatermelésre is felhasználható” (regionális biogáz üzemek kialakítását, kisméretű egyedi

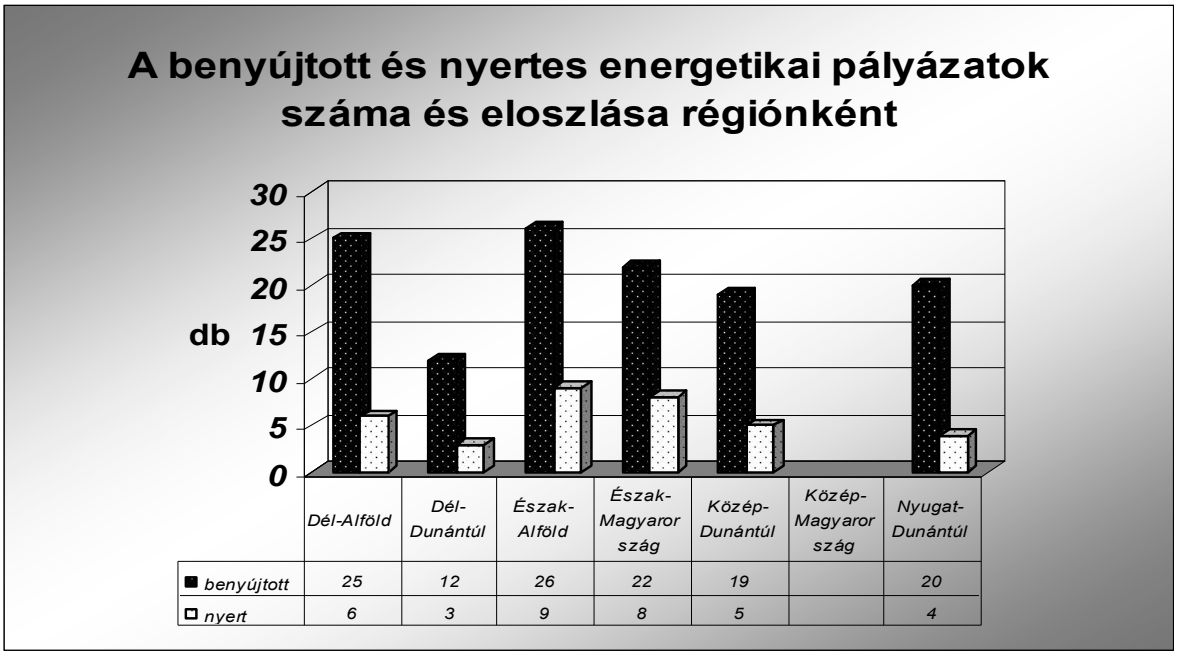
fogyasztói biogáz üzemek létesítését, a szennyvíziszap energetikai és mezőgazdasági hasznosítását szorgalmazza).

Rámutat arra, hogy előtérbe kell helyezni a hő és villamos energia előállítás támogatását konstrukción belüli támogatott tevékenységek, biológiai felhasználás esetén. Növényi és állati eredetű hulladékból, kommunális hulladékból, illetve szennyvíztisztító telepeken képződő szennyvíziszapból előállított biogáz alapú közvetlen hőtermelést, közvetlen vagy kapcsolt villamos energiatermelést:- regionális biogáz hasznosítók vagy

- kisméretű eredetű egyedi fogyasztói biogáz-hasznosítók kialakításával.

A biomassza és természetesen a biogáz hasznosítás jövőjét nagymértékben befolyásolják a kiépítését, ill. üzemeltetését segítő támogatások. Az EU-s források főleg az AVOP- on (Agrár- és Vidékfejlesztés Operatív Program) keresztül támogatták az ilyen irányú törekvéseket.

A gazdálkodók energetikai célú növénytermesztését a 25/2006. FVM rendelet szerint területalapú támogatásokkal ösztönözte az állam.



7. ábra A KEOP 4.1benyújtott és nyertes energetikai pályázatok száma és eloszlása régiónként[3]

KEOP: Környezet és Energia Operatív Program (UMFT)

Az un „Zöld áram" termelésének ösztönzését a többször módosított 2001.évi CX. Villamos Energia törvény szabályozza. Ez a rendszer vegyes: egyszerre alkalmaz átvételi kvótákat és fix átvételi árat is. Sajnos ezt 2006-ban csökkentette az állam, aminek hatása azonnal érződött az átvétel mennyiségén (4,17%-ról 3,8%-ra csökkent).

A KEOP 4.1. keretein belül van lehetőség anyagi támogatás igénylésére olyan erőmű létesítésére, ami megújuló energiaforrásból hő- és/vagy villamos energia előállítására képes. E támogatás célja: a hazai energiahordozó forrásszerkezet kedvező befolyásolása a hagyományos energiaforrásoktól a megújuló energiaforrások irányába való elmozdulás elősegítésével. Támogatás formája vissza nem térítendő, mértéke: 30 %- max. 50 %(minimum összege: 1 000 000. - HUF, maximum összege: 800.000.000. - HUF, 2007-es adat)

A benyújtott pályázatok száma régiónként igen eltérő. (7. ábra) Közép Magyarországi részről egyetlen ilyen irányú (KEOP 4.1) pályázat sem került beadásra 2007-ig. Elmondható, hogy a beadott pályázatok körülbelül egynegyede sikeres, nyertes pályázatként lett elbírálva.

Összesen a megújuló energiaforrásból előállított hő és villamosenergia-támosatására 2007-ig országos szinten 3793 Millió HUF fizettek ki.

ENERGETIKAI LEHETŐSÉGEK RÉGIÓNKÉNT

Magyarország mezőgazdasági területeinek hulladékait az egyes gazdaságok túlnyomó részt helyi szinten felhasználják. A növényzet tárolása, kiszárítása és elégetése után a nyert hőenergiát a gazdaság melléképületei, istállói, melegházai, tárolói, nagyobb mennyiségben pedig a környezetében épülő lakóépületek tudják hasznosítani. Számottevő ugyanakkor az ország azon gazdálkodóinak száma, ahol állattenyésztéssel is foglakoznak. Az alábbi táblázat (4. táblázat) mutatja régiónként az állattartó gazdaságok és a „vegyes" (állattartó és növénytermesztő) gazdaságok számát régiónként.

Területi egység	Állattartó gazdaságok	Vegyes gazdaságok	Összesen
Közép-Magyarország	**22 470**	**13 419**	**35 889**
Közép-Dunántúl	10 766	14 063	24 829
Nyugat-Dunántúl	9 687	17 166	26 853
Dél-Dunántúl	15 228	22 977	38 205
Dunántúl	**35 681**	**54 206**	**89 887**
Észak-Magyarország	23 181	16 939	40 120
Észak-Alföld	36 951	46 470	83 421
Dél-Alföld	43 541	48 266	91 807
Alföld és Észak-Magyarország	**103 673**	**111 675**	**215 348**
Ország összesen	**161 824**	**179 300**	**341 124**

4. táblázat Állattartó és vegyes gazdaságok az ország egyes területei tekintetében [6]

Külön kiemelhető az országnak az a három területe, ahol legnagyobb számban lelhetők: Dél- Dunántúl, Észak- Alföld, Dél- Alföld. Az ország összes vegyes gazdaságát tekintve 341124- ből 63 %-át pontosan: 213433 darabot ezeken a részeken találunk.

E területek mezőgazdasági energia felhasználása a legjelentősebb, amit az alábbi táblázat (5. táblázat) tartalmaz. Az összes energiafogyasztás - ezeken a területeken- közel 10%-át a mezőgazdaságra fordított energia teszi ki.

Régiók	Összes energia felhasználás2007 [TJ]	A mezőgazdaság energia felhasználása [TJ]
Dél-Alföld	54480.0	5499
Dél-Dunántúl	36287.0	3245
Észak-Alföld	65154.0	4985
Észak-Magyarország	78991.0	2431
Közép-Dunántúl	92235.0	3343
Közép-Magyarország	158307.0	1482
Nyugat-Dunántúl	42033.0	2152
Összesen	527487.0	23137.0

5. táblázat Mezőgazdasági energia felhasználása régiónként [6]

Az ország e területein nagy mennyiségű állati és növényi hulladék, fel nem használható termék halmozódik fel. Ezek egy része, ha nem megfelelő- sokszor költséges- kezelést alkalmaz a gazdálkodó egység veszélyes is lehet a környezetre. A vegyes hulladék csupán egy töredékét lehetne elégetéssel hasznosítani, azt is csak megfelelő tárolás esetleg még több energiát igénylő szárítás, aprítás után.

A biogáz telephelyi telepítése, nem csak a gazdaság épületeinek melléképületeinek fűtését oldhatná meg a téli hónapokban. A biogáz gázmotorban történő elégetésével még értékesebb energia, villamos energia előállítása válna lehetővé. Ezt kisebb mennyiségben a gazdaság, nagyobb mennyiségben az országos hálózat tudná hasznosítani.

A megújuló kategórián belül a szennyvízkezelő létesítményből, illetve a hulladéklerakóból származó gázt felhasználó erőművek által értékesített mennyiség egyelőre nem számottevő csupán 2,7 illetve 16,4 GWh. Az előző évihez viszonyítva egyik kategóriában sem jelent meg új kapacitás. A két kategória együttes teljesítménye így továbbra is 5 MW. (Ezek az értékek a KÁT rendszerén belül értendők!) [7]

Megújuló erőművek, beépített teljesítmény (ország régiói) [MW]						
Régiók	Biogáz-erőmű	Biomassza bázisú erőművek	Hulladékégető	Szélerőmű	Vízerőmű	Összesen
Dél-Alföld régió	0.82					0.82
Dél-Dunántúl régió	0	49.9				49.9
Észak-Alföld régió	7.004	3.6		3	11.4	25.004
Észak-Magyarország régió		117.08		2.85	33.44	153.37
Közép-Dunántúl régió	2.322	103.01	.8	8.655		114.787
Közép-Magyarország régió	1.33	1.36	24		2	28.69
Nyugat-Dunántúl régió	.83			105.8	6.154	112.784
Összesen	12.306	274.95	24.8	120.305	52.994	485.355

6. táblázat Megújuló erőművek régiók szerinti csoportosításban [3]

A biogáz üzem telepítés valóságos helyzetét az alábbi táblázat tartalmazza. Az érintett régiók közül az Észak-Alföldön létesítettek jelentős kapacitással rendelkező biogáz erőművet. Dél-Dunántúlon 50 MW Észak- Alföldön 3,6 MW teljesítményű biomassza bázisú erőmű működik. Ugyanakkor a Dél-Alföldi régióban sem biomassza bázisú jelentős teljesítményű, sem biogáz erőmű nem létesült.

Az egyre többet emlegetett energiafüggőség problémájának megoldása itthoni nyersanyagainkban van. Létezik a hazai energiaforrás csak keresni kell! Ha megtaláltuk, akkor nagy körültekintéssel a lehető legoptimálisabb körülmények között kötelességünk hasznosítani. A fenti összefoglalóból egyértelműen látszik, hogy a Dél-Alföldi és a Dél-Dunántúli régiókban nagy létjogosultsága van biogáz erőmű telepítésének.

NÖVÉNYTERMESZTÉSI ÉS ÁLLATTENYÉSZTÉSI „VEGYES" GAZDASÁGOK HULLADÉKAINAK ENERGETIKAI HASZNOSÍTÁSÁNAK GLOBÁLIS ÉRTÉKELÉSE

A biomassza energetikai hasznosításának legfontosabb feltételei Magyarország tekintetében adottak. Fejlett ország lévén biztosítani tudja a technikai és szellemi hátteret, az EU tagállamaként ez irányú fejlesztésekhez anyagi támogatást kaphat, valamint –talán a legfontosabb elemként – kitűnő mezőgazdasági alapjaira építve nagy mennyiségű nyersanyaggal rendelkezik.

A biomassza energetikai hasznosításának gazdasági értékelésekor sokszor csak a hagyományos „költség – jövedelem – beruházás" jellegű módszert alkalmazzák [8]. A magasabb energiaárak tükrében, a ma még gazdaságtalannak tűnő energiaforrások kihasználása hamar gazdaságossá válhat, és akkor az lesz lépéselőnyben, aki már most is ebben az irányban halad.

A vegyes gazdaságokban rejlő növényi és állati hulladékok vizsgálatánál jóval körüllátóbbnak kell lenni. Fontos szempont hogy, a nap, mint nap keletkező szerves energia nyersanyag tárolása, ártalmatlanítása sokszor problémás és költséges. Szakszerű körülményekkel biztosított tárolása és lebomlása közben azonban értékes biogázt nyerhetünk belőle. Gázmotorral történő elégetésénél termelt villamos energia helyben felhasznosítható vagy az országos hálózatra csatlakozva kedvezményes áron leadható. A folyamat közben keletkező hőenergiát pedig nem csak a mezőgazdasági vállalkozás, hanem a környék lakóházai- telepei is hasznosíthatják. Növényi és állati hulladékok megfelelő kezelésének számos gazdasági indoka van, melynek értéke pénzben nehezen becsülhető meg. Példaként említve a mezőgazdasági területek versenyképességét, új munkahelyek keletkezését vagy az ezekkel együtt járó helyi infrastruktúra és életszínvonal fejlődését. Szintén, pénzben nem meghatározható a környezetkímélőbb tüzelés során levegőbe jutott jóval kevesebb kén-dioxid és nitrogén-oxidok mértéke, a fosszilis tüzelőanyagokéhoz képest. Továbbá nem szabad elfelejteni azt az ésszerű és megkérdőjelezhetetlen törekvés szükségszerűségét, ami a hazai energiaellátás kiszolgáltatottságának csökkentésére irányul.

Általánosan megállapítható, hogy a biomasszahulladék-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 (2010.06.06.)

[2] Statisztikai Tükör: Energiaárak alakulása 2004-2009, IV. évfolyam 58-as szám, 2010/58 Összeállította a KSH http://www.energiakozpont.hu/index.php?p=230, (2010.06.06.)

[3] T-STAR teljes nevéből - Település Statisztikai Rendszer Budapest, 2007 http://www.energiakozpont.hu/index.php?p=230, http://adatbank (2010.05.29.)

[4] A fenntartható fejlődés indikátorai Magyarországon, Központi Statisztikai Hivatal, Budapest (2007)

[5] Magyar Biogáz Egyesület, biogas.hu, (2010.04.21.)

[6] Magyarország mezőgazdasága, Központi Statisztikai Hivatal, Budapest 2007, http://portal.ksh.hu/portal/page?_pageid=37,115776&_dad=portal&_schema=PORTAL,

2007,http://portal.ksh.hu/portal/page?_pageid=37,115776&_dad=portal&_schema=PORTAL,(2010.03.01.)

[7] Az átvételi kötelezettség keretében megvalósult villamosenergia-értékesítés főbb mutatói 2009. évben http://www.eh.gov.hu/gcpdocs/201004/kat_2009_ev.pdf (2010.06.06)

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

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Tamási Béla
btamasihu2002@yahoo.com

Földi László
foldi.laszlo@zmne.hu

A KÖZÚTI VESZÉLYES ANYAGSZÁLLÍTÁS 2009. ÉVI TAPASZTALATAI SOMOGY MEGYÉBEN

Absztrakt

A térségi közúti veszélyes anyagszállítások száma az M7 autópálya országhatárig történt meghosszabbításával jelentősen megnőtt. A közúti veszélyes anyagszállításra vonatkozó szabályzók változásai nagymértékben segítik az ellenőrző tevékenységet. A veszélyes anyagszállítást koordináló és ellenőrző tevékenységet folytató szervek alapvető feladata a szállítmányokra vonatkozó előírások rendszeres ellenőrzése, a hiányosságok feltárása és a szükséges intézkedések megtétele. Tevékenységükkel hatékonyan elősegítik a lakosság és a környezet védelmét. A cikk célja, hogy bemutassa a veszélyes áru szállítmányok ellenőrzésének elmúlt évi eredményeit és tapasztalatait Somogy megyében.

The number of road transportation of dangerous goods in our county grew up significantly with lengthening the M7 hihgwayto the frontier. The changes in the regulations concerning road transportation of dangerous goods help the controlling activities. The fundamental tasks of the coordinating and controlling organs of dangerous goods transportation are frequent checks of regulations concerning dangerous cargo, revelation of deficiencies and taking necessary actions. Their activity greatly helps the protection of the population and the environment. The aim of this paper is to present the controlling results and experiences concerning road transportation of dangerous goods in Somogy County last year.

Kulcsszavak: *közúti veszélyes anyagszállítás, ellenőrzés, hiányosságok feltárása, intézkedések megtétele, lakosság- és környezetvédelem ~ road transportation of dangerous goods, control, revelation of deficiencies, taking actions, population and environment protection*

BEVEZETÉS

Somogy megye geográfiai elhelyezkedése mellett, az M7 autópálya országhatárt elérő megépítése, a veszélyes anyagok közúti szállításának számszerű emelkedését eredményezte, elsősorban a nemzetközi (tranzit) szállítások esetében. A közúti veszélyes anyagok szállítások (továbbiakban ADR[1]) jelentős növekedése és a szállítás összetett kockázati viszonyai, szorosabb hatósági felügyeletet igényelnek, mely igény mind társadalmi, mind kormányzati szinten jelentkezik. A Somogy Megyei Katasztrófavédelmi Igazgatóság és a Nemzeti Közlekedési Hatóság Dél-Dunántúli Régió Somogy Megyei Kirendeltsége kiemelt figyelmet fordított ez irányú tevékenységére Ezt támasztja alá a 2009. évben végzett hatékony felkészülési és ellenőrzési tevékenység, melyekre az eddigieknél még fokozottabb igény jelentkezett.

I. A VESZÉLYES ÁRUK KÖZÚTI SZÁLLÍTÁSÁVAL KAPCSOLATOS JOGI SZABÁLYOZÁS 2009. ÉVI VÁLTOZÁSAI

2009-ben jelentős változás történt a veszélyes áruk közúti szállításának ellenőrzésével kapcsolatos jogi szabályozás területén. A módosítás az ADR szabályzat mintegy 15%-át érintette és módosítás mind a kilenc részben található. Legjelentősebb ezek közül a környezetre veszélyes árut szállító járművek jelölésének kiegészítése, az új mentességi forma az „Excepted Quantities” és vannak olyan változások is, melyek az eddigi előírásokat tovább szigorítják, mint az LQ[2]-s szállításoknál a jelölés vagy a fuvarokmányban való feltüntetés.

A közúti közlekedésről szóló **1988. évi I. törvény** (továbbiakban Kkt.) a katasztrófavédelmet legérzékenyebben érintő módosítása, hogy 2010. január 1-jét követően a beszedett bírság már nem az eljáró hatóságot (többek között a katasztrófavédelmi hatóságot) illeti, hanem a központi költségvetés központosított bevételét képezi.

A Kkt. egyik újdonsága, hogy nincs helye bírság kiszabásának, ha a jogsértő cselekmény elkövetése óta egy év eltelt (egy éves elévülési határidő került alkalmazásra). Pontosítja a törvény, hogy a bírságot a rendelkezés megsértéséért felelősnek kell megfizetnie és amennyiben többen felelősek, úgy felelősségük arányában szankcionálják őket, ha pedig ez az arány nem állapítható meg, a bírságon egyenlő arányban osztoznak. Szintén új elem, hogy mentesül a felelősség alól a bírságfizetésre kötelezett, ha a szabálysértés a működési körén kívül eső elháríthatatlan ok, vagy olyan esemény miatt következett be, amelyet nem látott, vagy láthatott előre. A módosítás eredményeként megszűnt a magyar járművek visszatartási lehetősége a bírságfizetés kikényszerítésére, ez a lehetőség csak a külföldi járművek esetében alkalmazható.

Változások következtek be a bírságolás rendjét szabályozó jogszabály (az **57/2007 (III.31) Korm. rendelet**), a bírságolás rendjéről szóló rendelet vonatkozásában, miután hatályon kívül helyezték és helyette 2009. augusztus 01-től a 156/2009 (VII.29) Korm. rendeletben, részben átalakított formában és tartalommal megjelent az új szabályozás. Az új bírságrendelet a korábbiakhoz képest több területet eltérően, illetve részletesebben szabályoz. Meghatározza a veszélyes áruk szállításával kapcsolatos azon jogszabályokat, melyek be nem tartása, a későbbiekben sorolt bírságtételek valamelyikének kiszabását vonhatja maga után. Megállapítja továbbá az egyes bírságolással érintett cselekmények elkövetéséért felelőssé tehetők körét, illetve – 1 millió forintban – maximalizálja a „halmazati bírságok” összegét, azaz az egy ellenőrzés során feltárt több jogsértő cselekmény esetében együttesen kiszabható bírság mértékét. Az új bírságrendelet szerint az augusztus 1-jét megelőzően elkövetett szabályszegések esetében is az új bírságrendelet előírásait kell alkalmazni, amennyiben a

[1] **A**ccord Européen Relatif au Transport International des Marchandises **D**angereuses par **R**oute
[2] Limited Quantity

bírság mértéke, illetve a bírság legmagasabb mértéke tekintetében az új rendelkezés kedvezőbb rendelkezést állapít meg, mint a korábbi bírságrendelet.

A hatósági munkában nagy változásokat, és emellett többlet feladatokat hozott a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló **2004. évi CXL.tv.** (továbbiakban Ket.) módosítása. A Ket megszünteti az „udvarias levél" kategóriáját. Ennek megfelelően a hatóság döntése kétféle lehet: az ügy érdemében határozatot hoz, vagy az eljárás során felmerült minden más kérdésben végzést bocsát ki.

A Ket. áttér a határidők munkanapokban történő számítására, így például az ügyintézési határidő 22 munkanap lett, mely az eljárás megindításának napján kezdődik, és meghosszabbítani 1 alkalommal 22 munkanappal lehet. Az ügyintézési határidőn belül a hatóságnak nem csupán a döntést kell meghoznia, hanem intézkednie is kell a döntés közlése iránt. Az ügyintézési határidő túllépése esetén az eljárás lefolytatásáért fizetett illetéket a hatóság megfizeti az ügyfélnek – ha illetékmentességben részesült az ügyfél, a hatóság a meg nem fizetett illetéket a központi költségvetésnek fizeti meg – saját költségvetése terhére. Az új Ket. értelmében már nincs mérlegelési lehetősége a hatóságnak, ha az ügyfél nem fizeti be az eljárási illetéket felhívás ellenére sem, az eljárást köteles megszüntetni.

A módosítás óta az elsőfokú hatóság feladata dönteni a fellebbezéssel együtt benyújtott, a fellebbezési eljárásban való költségmentességre irányuló kérelemről, mellyel összefüggésben az elsőfokú hatóság vizsgálja a fellebbezési eljárási illeték meglétét is, és az elkésett fellebbezést érdemi vizsgálat nélkül végzéssel köteles elutasítani. Az elkésett fellebbezés miatt előterjesztett igazolási kérelem elbírálása szintén az elsőfokú hatóság feladata.

A fentieken túl jelentős még a két legutóbbi változás, a **KRESZ** módosítása, illetve a Ket. módosítása nyomán kiadott **80/2009.(XII.29) KHEM** rendelet.

A KRESZ módosítása mindenki számára nyilvánvaló módon rendezte a katasztrófavédelmi hatóság jogkörét a járművek megállítása, illetve a közúti forgalom irányítása tekintetében. A KRESZ a forgalom irányítására és a közúti jelzések, és forgalmi szabályok felülbírálására vonatkozó (KRESZ 6.§ (1)-(3) bekezdés) jogosultságokat kiterjesztette a katasztrófavédelmi hatóság közúti ellenőreire.

A 80/2009.(XII.29) KHEM rendelet a Ket. módosításában testet öltött azon kormányzati szándék, amely a kis hibák tekintetében az első alkalommal mulasztók esetén kellően „toleráns". Ennek megfelelően a Ket. 94.§ (1) bekezdés a) pontja taglalja a figyelmeztetés jogintézményét, míg a Ket. 94.§ (2) bekezdése meghatározza azokat az eseteket, amikor kizárt e jogintézmény alkalmazása. A Ket. 94.§ (2) bekezdés b) pontja alapján kiadott 80/2009.(XII.29) KHEM rendelet – a 2.§ (5) bekezdés b) pontjában – ennek megfelelően szabályozta a veszélyes áruk közúti szállítása során elkövetett szabálytalanságok tekintetében azon mulasztások körét, melyeknél az eljáró hatóság nem mérlegelhet, és szankcióként nem élhet figyelmeztetéssel, kizárólag bírságot szabhat ki. Ezek a már említett új bírságrendelet (156/2009. (VII.29.) Korm. rendelet) 5. mellékletének 1-33. sorában foglalt (azaz a régóta ismert és alkalmazott 1/2002 (I.11.) Korm. rendelet I. és II. kockázati kategóriájába tartozó) mulasztások.

Az ADR ellenőrzések és bírságolások során a jogalkalmazási és a bírósági tapasztalatoknak megfelelően a területi szervek számára folyamatosan aktualizálni kell a belső szabályzókat a módszertani és eljárási gyakorlat egységes kezelése érdekében, illetve a jogalkotók felé jelezni szükséges a jogszabály módosítására vonatkozó javaslatainkat.[6]

II. A KÖZÚTI VESZÉLYES ÁRU SZÁLLÍTÁS ELLENŐRZÉSE

A Somogy Megyei Katasztrófavédelmi Igazgatóság a 2009. évben a korábbi évekhez hasonlóan – a Nemzeti Közlekedési Hatóság Dél-Dunántúli Régió Somogy Megyei Kirendeltségével, a rendőrség, illetve a vámhatóság illetékes szervével egyeztetve, valamint önállóan is – folyamatosan tervezték és hajtották végre az ellenőrzéseket. Az igazgatóság szakemberei az elmúlt év során 54 alkalommal vettek részt közúti ellenőrzésen, ami az előző évhez képest növekedésnek mondható.

A közutakon történő megjelenés növekedésében szerepet játszottak a bevezetett hatékonyságnövelő intézkedések, az ellenőrzési lehetőségek növekedése, valamint az igazgatóság munkatársai ellenőrzési gyakorlatának bővülése, továbbá a törvényi változásig, a beszedett bírságok felhasználhatóságának ösztönző ereje.

Közúti szállítmányok ellenőrzése

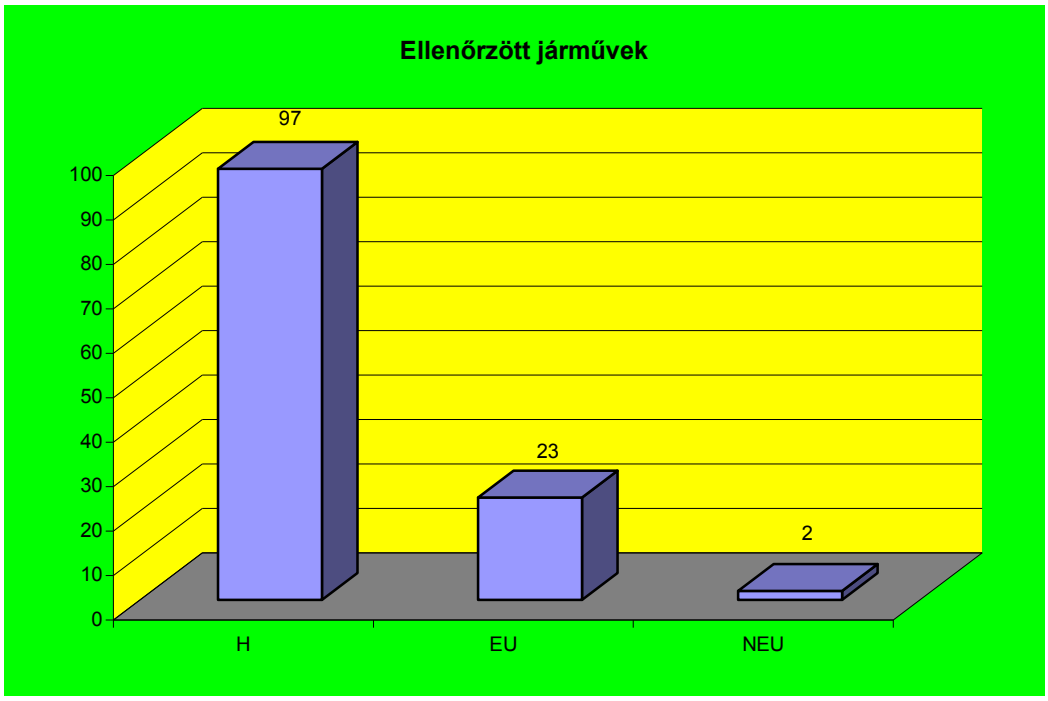
A Somogy Megyei Katasztrófavédelmi Igazgatóság szakemberei jelentős erőfeszítéseket tettek az ellenőrzések rendszeresebbé tételére, az ellenőrzések mennyiségének növelésére.
Az ellenőrzési alkalmak számának növekedése mellett, az összes ellenőrzött gépjárművek száma szintén emelkedést mutat. 2009-ben 122 db veszélyes árút szállító gépjárművet ellenőriztek, mely a közutak biztonsága szempontjából jelentős mértékű. (lásd 1. sz. ábra) Az adatok a veszélyes árut szállító járművekre vonatkoznak, ezen túlmenően azonban az úgynevezett fekete fuvarok kiszűrése érdekében az elmúlt évben mennyiségében közel 300 db olyan, nem jelölt járművet is ellenőriztek, melyek nem szállítottak veszélyes árut. A nem jelölt járművek vizsgálata során több esetben került feltárásra olyan szállítás, ahol veszélyes árut szállítottak a vonatkozó előírások betartása, illetve annak mindennemű szándéka nélkül.

Az ellenőrzések hatékonyságát többek között befolyásolja az ellenőrzés helyének, idejének megválasztása, a forgalom nagysága. Előfordul, hogy az ellenőrzés ideje alatt nem, vagy csak kevés számú veszélyes árut szállító jármű közlekedik, kevés ellenőrzésre alkalmas helyszín van, amit a szállító cégek elkerülnek, mihelyst tudomást szereznek az ellenőrzésről. Ezt kiküszöbölni csak az ellenőrzések gyakoriságának növelésével, illetve az ellenőrzés helyszínének gyors, többszöri változtatásával lehetséges.

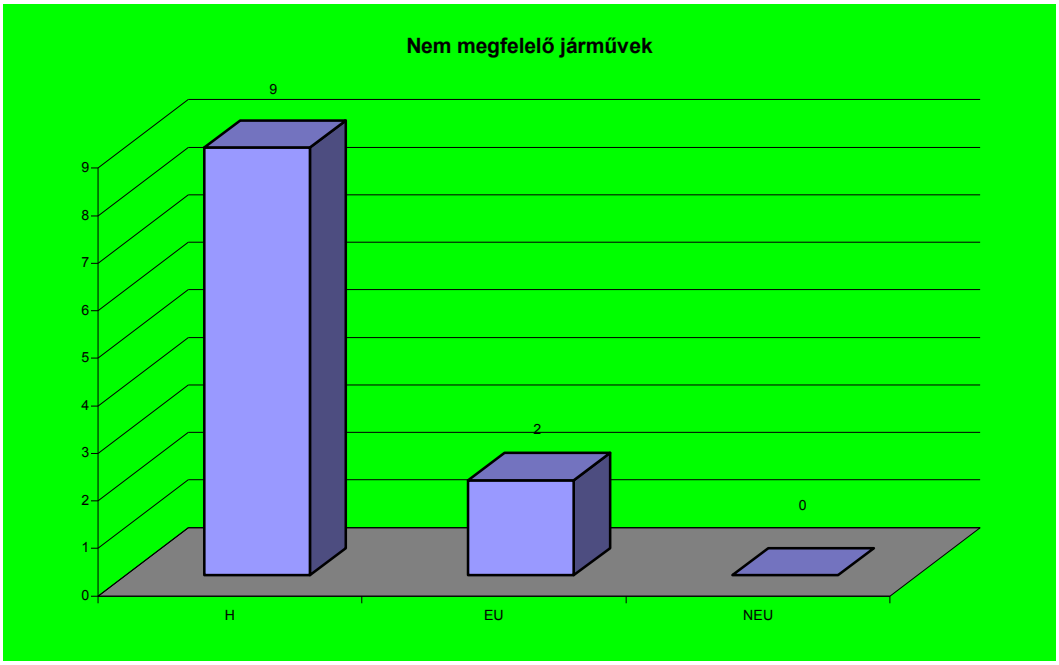
A katasztrófavédelmi ellenőrzések jelenléte a közutakon a továbbiakban is kiemelkedően fontos feladatot jelent, amely nagymértékben hozzájárul a közlekedés biztonságának növeléséhez. (lásd 2. sz. ábra)

Az ellenőrzött 122 gépjármű közül – melyek nemzetiség szerinti aránya 80% belföldi, 17,5% EU tagállam és 2,5% nem EU tagállam– közel 3,5%-nál tártak fel a szakemberek hiányosságot. A magyar szállítók 9%-a, a külföldi szállítók 1,1%-a nem felelt meg valamilyen szempontból az előírásoknak [1].

Az elmúlt évekhez képest csökkent a tapasztalt hiányosságok száma mind a belföldi, mind a külföldi szállítók körében.



1.sz .ábra
2009-ben ellenőrzött járművek száma Somogy megyében
Forrás: SMKI[3]

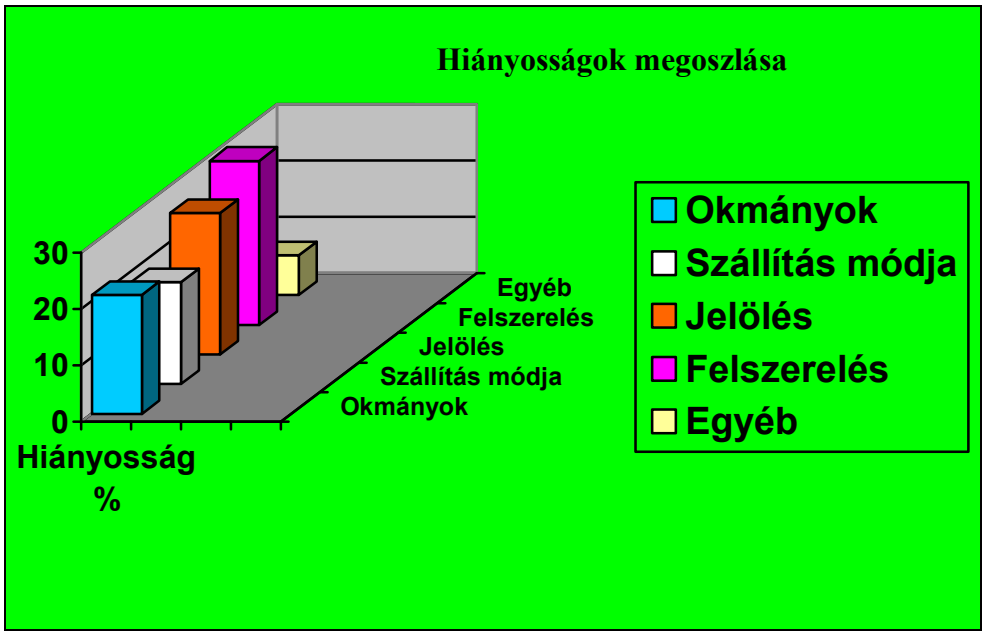


2.sz. ábra
A veszélyes anyagot szállító járművek „Nem megfelelősége ” Somogy megyében,
2009-ben Forrás: SMKI

[3] Somogy Megyei Katasztrófavédelmi Igazgatóság

Az elemzések szerint a nemzetközi fuvarozásban résztvevő nagyobb hazai cégek és vállalatok veszélyes árut szállító járművei az ADR szabályainak és előírásainak többnyire megfelelnek, jelölésük szabályos, kiegészítő felszerelésekkel, tűzvédelmi eszközökkel rendelkeznek. A 2009. évben tapasztaltak alapján – hasonlóan az előző évhez – a legtöbb hiányosság a belföldi fuvarozást vállaló kisebb hazai vállalatok, illetve az Európai Unióból származó külföldi cégek gépjárműveinél fordult elő. Számos hiányosság volt a mentességi határ alatti mennyiséggel szállítók körében. Ezen esetekben a szállítók rendszeresen úgy végezték a szállítást, mintha egyáltalán nem vonatkozna rájuk semmilyen ADR szabály. A hibák sokszor halmozottan jelentkeztek.

A szabálytalan szállítások számának stagnálása arra vezethető vissza, hogy a közlekedési morál, a szállítói fegyelem ugyan mutat pozitív változást, viszont a növekvő jelenlét a közutakon, a hatékonyság növelő intézkedések, valamint a nem jelölt járművek fokozottabb ellenőrzése előhozza azokat a látens hibákat, hiányosságokat is, amelyek eddig nem kerültek az ellenőrök látókörébe.



3.sz. ábra
A hiányosságok százalékos megoszlása Somogy megyében, 2009-ben
Forrás: SMKI

A leggyakrabban előforduló hibák (lásd 3.sz. ábra):

- a fuvarokmányok nem megfelelő vezetése,
- a tűzoltó készülékek hiánya vagy érvényességi idejének lejárta,
- a rakományrögzítéssel kapcsolatos hiányosságok,
- az írásbeli utasítás hiánya,
- a járművek, illetve a küldeménydarabok nem szabályos jelölése, bárcázása,
- a védőfelszerelések és a figyelmeztető jelzőeszközök hiánya,
- utas szállítása

Regionális ellenőrzések

A több megyében – az elkerülő útvonalakon is – egyszerre tartott ellenőrzések a korábbiakhoz képest növekvő számban kerültek végrehajtásra. Az ellenőrzéseken részt vettek az érintett régiók katasztrófavédelmi igazgatóságai, a Nemzeti Közlekedési Hatóság regionális szervei, a

megyei rendőr-főkapitányságok területileg illetékes szervei, az Autópálya Rendőrség, valamint esetenként a vám- és pénzügyőrség és a hivatásos önkormányzati tűzoltóságok szakemberei.

Az elvégzett regionális jellegű ellenőrzések tapasztalatai egyértelműen azt jelzik, hogy még a társszervek részvétele nélkül is indokolt ilyen jellegű ellenőrzések sűrűbbé tétele, miután ellenőrizetlen elkerülő út nem lévén, több olyan veszélyes áru szállítmány került ellenőrzés alá, mely az ADR egyetlen előírását sem tartotta be. A regionális jellegű összehangolt ellenőrzések hatékonysága a közúti közlekedés biztonsága szempontjából megkérdőjelezhetetlen, ezért a közös ellenőrzéseket a későbbiek során is célszerű szorgalmazni és rendszeressé tenni.

Telephelyi ellenőrzések

Somogyban az év folyamán telephelyi ellenőrzésre 15 esetben került sor és egyben a telephelyeken lévő gépjárművek ellenőrzése is végrehajtásra került. Bebizonyosodott, hogy a telephelyi ellenőrzésekkel a szabálytalanságok nagy része megelőzhető, ezért a telephelyi ellenőrzések fokozása szükséges.

A telephelyi ellenőrzéseket az is indokolja, hogy feltehetően a SEVESO szabályozás hatálya alóli mentesítés érdekében az üzemeltetők egy része veszélyes anyagaikat rendezetlen helyzetű ipari parkokban és kisebb telephelyeken igyekeznek elhelyezni.

A hatékonyság növelése érdekében szükséges a veszélyes áruszállításban részt vevők (feladók, szállítók, csomagolók) felmérése, melynek kiindulási alapjául részben a saját adatbázisaink (veszélyes hulladékszállítók, SEVESO-s üzemek, ellenőrzött járművek üzemeltetői, feladók), illetve részben a társhatóságok (közlekedési hatóság, környezetvédelmi hatóság) adatbázisai szolgálhatnak.

III.SZANKCIONÁLÁSI TEVÉKENYSÉG

A 2009. évben a Somogy Megyei Katasztrófavédelmi Igazgatóság a korábbiakhoz képest, jóval nagyobb tapasztalattal bírt a veszélyes áruszállítással kapcsolatban végrehajtott önálló ellenőrzés és szankcionálás (bírságolás) területén. A 2009. augusztusában bevezetett jogszabályváltozásokkal a kiszabható bírság maximális összegét ügyfelenként egymillió forintban korlátozták.

A 2009. év során Somogy megyében összesen 6 db bírsággal összekapcsolt határozat került kiadásra. A bírságolások következtében 1 500 000 Ft bírság került megfizetésre. [2]

IV.VESZÉLYES HULLADÉKOK ORSZÁGHATÁRT ÁTLÉPŐ SZÁLLÍTÁSA

Az országhatárt átlépő hulladékszállításról szóló 180/2007. (VII. 3.) Korm. Rendelet előírása szerint a hulladékok behozatala, kivitele és átszállítása során hatóságként az Országos Környezetvédelmi, Természetvédelmi és Vízügyi Főfelügyelőség jár el. A főfelügyelőség a Somogy megyén áthaladó veszélyes hulladék behozatala, kivitele és átszállítása esetén a hulladék szállítására vonatkozó eljárásáról értesítette a Somogy Megyei Katasztrófavédelmi Igazgatóságot. A legnagyobb mennyiségben akkumulátorokat, illetve szerves oldószereket, lúgokat szállítottak. A szállítások során végrehajtott ellenőrzések hiányosságot nem tártak fel.

V. VESZÉLYES ÁRU SZÁLLÍTÁS SORÁN BEKÖVETKEZETT BALESETEK

A területi szervek részére pontosabb és az egyes részletekre is kiterjedő konkrét szabályozást ad az Országos Katasztrófavédelmi Főigazgatóság belső intézkedése annak érdekében, hogy a veszélyes áruszállítási ellenőrök az esetlegesen bekövetkezett balesetekről megfelelő módon és időben értesüljenek, illetve a balesetek kivizsgálása szabályszerűen megtörténjen. 2009. évben, Somogy megyében veszélyes anyag szállítás során baleset nem következett be. [3] [4] [5] [6]

ÖSSZEGZÉS

A 2009. évre vonatkozó ADR ellenőrzések Somogy megyei tapasztalata, hogy emelkedett az ellenőrzött gépjárművek száma és javult az ellenőrzések során a hibafeltárás hatékonysága. Az elmúlt évek statisztikai adatait figyelembe véve megállapítható, hogy a magyar és külföldi szállítók esetében sem a hibás szállítások, sem az egy gépjárműre vetített szabálytalanságok aránya nem változott jelentős mértékben, amely az ellenőrző hatóságok határozott fellépésének és a szállításban résztvevők önkéntes jogkövetésének eredménye. Tapasztalat, hogy egyre kevésbé lehet elkerülni az ellenőrzéseket, így a hiányosságok egyre inkább a hatóságok látókörébe kerülnek. Ezért a hatósági tevékenység végrehajtása során további hatékonyságnövelő intézkedések bevezetése szükséges. Ezeket két alapvető területen látom szükségszerűnek.

A **személyi állomány ismeretének bővítése**, az ellenőrzések feldolgozása, a nemzetközi törzsekben eredményesen alkalmazott „Tapasztalat Feldolgozó Rendszer” átvételével növelhető. A rendszer, az ellenőrzések tapasztalatainak „űrlapon” történő rögzítését követően számítógépes hálózaton keresztül valamennyi katasztrófavédelmi igazgatóság részére rendelkezésre áll. Ehhez kapcsolódik a megfelelően feltöltött, időszakosan frissített, az igazgatóságok és a környező országok bevonásával „Adattár” elkészítése.

A **technikai, technológiai fejlesztés** elengedhetetlen. Sajnos napjaink világválsága csökkenti a modernebb technikai eszközök beszerzését. Ennek ellenére, az ADR bírságokból befolyt összeget a K+F projektekbe kell fektetni. A nemzetközi piac, vevő a tárgyban fellelhető újdonságokra, kutatási, technikai és technológiai eredményekre.

A jogi szabályzók a 2009-es év során több alkalommal változtak, nem éppen a tevékenységet ösztönző irányába. Ennek ellenére a jövőben is a legfontosabb feladat, hogy az ellenőrzési számok mellett azonos súlyt kell kapnia az ellenőrzések minőségének, a hiányosságok feltárásának és a hatékonyság fokozásának. Ezeknek a lehetősége Somogy megyében biztosítottnak látszik.

Hivatkozások:

[1] Dr Vass Gyula tü. ezds: A katasztrófavédelmi szervek veszélyes áru szállításának ellenőrzésével kapcsolatos tapasztalatai a 2009. évre vonatkozóan. http://www.vedelem.hu/files/UserFiles/File/konf2010/adr/ADR_ell_%20tapasztalatok_2009.pdf *Letöltve: 2010. május 10.*

[2] Dr Hoffman Imre: A 2009. évi katasztrófavédelmi ADR ellenőrzések és bírságolások végrehajtásának tapasztalatai
http://www.vedelem.hu/letoltes/tanulmany/tan247.pdf *Letöltve: 2010. május 25.*

[3] Somogy Megyei Katasztrófavédelmi Igazgatóság: Jelentés a veszélyes áru szállítások ellenőrzéséről 2009/I.negyedév

[4] Somogy Megyei Katasztrófavédelmi Igazgatóság: Jelentés a veszélyes áru szállítások ellenőrzéséről 2009/II. negyedév

[5] Somogy Megyei Katasztrófavédelmi Igazgatóság: Jelentés a veszélyes áru szállítások ellenőrzéséről 2009/III.negyedév

[6] Somogy Megyei Katasztrófavédelmi Igazgatóság: Jelentés a veszélyes áru szállítások ellenőrzéséről 2009/IV. negyedév

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Jobbágy Szabolcs
jobbagyszabolcs@citromail.hu

HAZAI ÉS EU ENERGIABIZTONSÁG ÉS A MEGÚJULÓ ENERGIAFORRÁSOK

Absztrakt

Értékelő elemzésében egy általános képet szeretnék nyújtani az energiabiztonsággal kapcsolatos kérdéskörről, megvilágítva legfontosabb alappilléreit. A teljesség igénye nélkül, az energiapiac összefüggéseit tanulmányozva, magyarázatot kívánok adni egyfajta megközelítésben a biztonság, és annak egyik meghatározó szegmense az energiabiztonság fogalmára. Ismeretbővítés céljából általánosságban át szeretném tekinteni az energiabiztonság alapját képező fosszilis és egyéb nem megújuló, valamint a megújuló-alternatív energiahordozók-energiaforrások tárházát, alkalmazásuk lehetőségét, majd az elemzés zárásaként összefüggéseket keresve, átfogó módon, értelmezni kívánom az Európai Unió és Magyarország energiabiztonságának a kérdéskörét. Az értékelő elemzés egyfajta összefüggéseken alapuló általános kitekintés, mint sem konkrét elemzése a téma valamely specifikus részterületének.

In my evaluative analysis I would like to give you a general overwiev about questions of energy security highlighting the most important basic principle. Without the need of completeness, studying coherency of energy market I would like to give you explanations for the concept of security and its main segments for the concept of energy security. With the aim of insight, generaly I wish to overwiev the repertoire of fossil and other non-renewable-alternative energy sources, application possibilities. Eventualy closing the evaluation, searching relationships in a comprehensive way I wish to clarify the issues of energy security of EU and Hungary. The evaluation analysis is a kind of general overwiev based on relationships, as not a concrate evaluation of a specific part of this topic.

Kulcsszavak: *biztonság, energiabiztonság, energiaforrás, diverzifikáció, alternatívenergia ~ security, energy security, energy source, diversification, alternative energy.*

ELŐSZÓ

A világ, amelyben élünk egy globalizált világ[1]. Biztonságát számos tényező veszélyezteti. A kockázati tényezők tárházában, a klasszikus értelemben vett háborúk, az erőszak, a nukleáris fenyegetettség, az új típusú kihívások, mint a terrorizmus, az információs hadviselés[2] [1] [2] [3], a kritikus infrastruktúra védelme[3] [4], az illegális migráció[4] [5], a globális felmelegedés mellett, napjainkban egy markáns „veszélyforrás", az energia, az energiabiztonság, az erőforrásokért folytatott harc is képviselteti magát.

Egy olyan világban élünk, melynek alapvető mozgatórugója a különböző energiaforrások kiaknázása. Azonban Földünk energiaforrás készletei végesek. A források földrajzi eloszlása egyenlőtlen. Az energia egy mindenki számára nélkülözhetetlen szegmens, az energia hatalom. A geopolitikai feszültségek, a közvetlen konfrontáció megelőzése, az „energiaéhség" kielégítése, az alternatív-megújuló energiaforrásokra való áttérés lehetőségeinek, megoldásainak kidolgozása és megvalósítása érdekében, nagy hangsúlyt kell helyezni az energia, az energiabiztonság, mint a biztonságot alapvetően meghatározó tényező kérdésének megoldására, hazai és nemzetközi szinten egyaránt.

A BIZTONSÁG, AZ ENERGIABIZTONSÁG FOGALMA

A biztonság szó a latin securus szóból ered, mely többek között gond nélküli, gondtalan, biztonságos jelentéssel bír. A Hadtudományi Lexikon megfogalmazásában a biztonság nem jelent mást, mint az „.....egyéneknek, csoportoknak, országoknak, régióknak, szövetségesi rendszereknek a maguk reális képességein és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete és annak tudati tükröződése, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak az ellene való eredményes védekezés feltételei." [6]

A biztonság egy komplex fogalom, melynek magyarázatára, kategorizálására a szakirodalomban számos megfogalmazás található. A vonatkozó magyarázatokból nyilvánvalóvá válik, hogy a biztonság fogalma vitatott, nincs egységes értelmezése, az idők folyamán folyamatosan változott, átalakult, új elemekkel bővült. Nem lehet leszűkíteni csupán a katonai jellegű fenyegetésekre és az azokra adott válaszokra.

A hidegháború időszakában a legfontosabb biztonsági kihívás, elsőrendű kockázati tényező a nukleáris háború elkerülése, a Szovjetunió térnyerésének, expanziós politikájának a megakadályozása volt. Ezt követően, az egykori szuperhatalom széthullásával, a bipoláris világrend megszűnésével, új kihívásokkal kellett és kell szembenézni, mint az etnikai

---

[1] *Globalizált világ:* A globalizáció ma már mindenki számára ismert, és gyakran használt, rendkívül összetett fogalom. A globalizáció egy olyan társadalmi, gazdasági folyamat, átalakulás, amelyben többféle „erő" hatására az országhatárok több szempontból is átjárhatóbbá válnak. A globalizációnak társadalmi, gazdasági és kulturális vonatkozásai vannak. Segítségével egymástól földrajzilag jelentős távolságban lévő emberek, közösségek is kapcsolatba kerülhetnek egymással. A globalizáció igyekszik a világot minden szempontból egységessé tenni. Olyan kölcsönös függőségi viszonyokat teremt, illetve olyan szabályokat érvényesít, amelyek bizonyos országok kormányai számára nem feltétlenül elfogadhatóak.

[2] *Információs hadviselés:* A fogalom az első öbölháború óta létezik. Az információs hadviselés a hadviselés egy új formája, amikor is az információ, illetve a támadások az információ, illetve az információs rendszerek ellen a hadviselés eszközeivé válnak.

[3] *Kritikus infrastruktúra:* Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában. Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

[4] *Migráció:* Egy demográfiai, népmozgási folyamat. A migráció a személyek, és ezzel együtt az anyagi javak, a szakértelem, a magatartásformák mozgása és kölcsönhatása is.

villongások-konfliktusok, a tömeges migráció, a terrorizmus, a kritikus infrastruktúra védelme, az erőforrásokért folytatott harc, a globális felmelegedés. Ebből adódóan a hidegháború lezárulásával megnőtt az igény a biztonság fogalmának kiszélesítésére. Barry Buzan híres angol politológus megfogalmazása alapján „…….a biztonság a túlélés és a fennmaradás lehetősége és képessége a létet fenyegető veszélyekkel szemben." [7] Többek között ő volt az első, aki kísérletet tett a biztonság különböző kategóriáinak megkülönböztetésére. Munkássága eredményeképpen a biztonság öt fő szektorát különítette el, melyek a katonai, politikai, gazdasági, társadalmi és környezeti szektorok. A Hadtudományi Lexikon megfogalmazásában is megtalálhatóak ezek az alapvető szektorok, kiegészülve a humanitárius, a környezetvédelmi és katasztrófa-elhárítási szektorokkal. [6]

Ezen a ponton kapcsolható össze az energiabiztonság kérdése a biztonság fogalmával, hiszen a gazdasági biztonság egyik meghatározó szegmense az energiától, az alapanyagoktól való függés. A fejlett országok, többek között az Európai Unió tagállamainak a fizikai túlélése, jóléte és annak növelése, nem kis mértékben függ az energiahordozókhoz való hozzáféréstől, mely energiahordozókkal olykor legnagyobb mennyiségben az instabil államszerkezettel, bizonytalan politikai berendezkedéssel bíró, fejlődő országok rendelkeznek. Az energiához való hozzáférés biztosítása, visszatekintve a történelem viharos időszakaira, mindig is kiemelt helyet foglalt el a háborút kirobbantó esetleges okok között. [8] Az energiahordozókért folytatott „harc" napjainkban is meghatározó tényezője a geopolitikai, gazdaságpolitikai csatározásoknak. A harc egyre inkább kiélesedni látszik a készletek végessége, kimerülése és a földrajzi elhelyezkedése miatt.

Az energiabiztonság szempontjából legnagyobb jelentőséggel a kőolaj és a földgáz bír, melyek egyrészt a fogyasztói társadalmak alappillérei, másrészt figyelembe véve a jelenlegi felhasználási adatokat, a növekvő igényt és a készletek állapotát, előrejelzések alapján még ebben az évszázadban könnyen egy globális összeomlást eredményezhetnek. Mint korábban említettem volt, a rendelkezésre álló készletek elfogyása egyre inkább leszűkíti a beszerzési forrásokat, geopolitikailag előnyös helyzetbe hozva a forrás és tranzit országokat, az energia piac meghatározó szereplőivé téve őket, és egyre kiszolgáltatottabb helyzetbe, függő állapotba sodorja a fogyasztó-importáló nemzeteket. Azonban a cél, az energiabiztonság, egy stabil energiapolitikai helyzet megteremtése mind a három fél számára közös érdek. Adódik ez abból, hogy a kitermelő, exportáló országoknak érdeke a biztos felvevőpiac, a piacokhoz való eljutást biztosító szállítási infrastruktúra megléte. A tranzit országok előnyös földrajzi fekvésüknek köszönhetően jelentős hasznot húzhatnak a területükön áthaladó szállítási útvonalakból, így azok megléte, illetve bővítése elsődleges érdekük. Ugyanakkor az energiára éhező, energiaforrásokkal nem vagy nem elegendő mennyiségben rendelkező országok is egy stabil, kiszámítható hozzáférési volumen, és szintén a megbízható, megfelelő kapacitással bíró szállítási útvonalak meglétét tartják ideális állapotnak. Ebből az aspektusból az exportáló, a tranzit és az importáló országok közötti kompromisszumokon alapuló kommunikáció kiemelkedő fontosságú. [8] [9] Az elhangzottak alapján, konklúzióként az energiabiztonság fogalma egyfajta megközelítésben értelmezhető úgy, mint „…….a kritikus energia, energetikai infrastruktúra normál állapota fenntartása feltételeinek összessége." [10] Egy másik megközelítés alapján, pedig az energiabiztonság nem más, mint „…….a lakosság ellátásához, és a gazdaság folyamatos működéséhez szükséges energiahordozók folyamatos, elérhető áron történő biztosítása." [8] A fent említett két definíció magában hordozza az energiabiztonság értelmezéséhez nélkülözhetetlen három legfontosabb tényezőt, melyek a jelentkező kereslet kielégítése – az energiahordozóknak a szükséges formában, mennyiségben, időben és helyen történő biztosítása -, a szükségletek kielégítésének folyamatossága, és az árak igazodása az energiaéhséggel küszködő piaci szereplők jövedelmi viszonyaihoz.

ENERGIAFORRÁSOK

Kőolaj a „fekete arany”

Annak ellenére, hogy a kőolaj, mint energiaforrás kényelmetlenebb, mint a villamos energia, környezetszennyezőbb, mint a földgáz, drága és politikai kockázatokkal terhelt, mindennapjaink egyik legmeghatározóbb energiaforrása, melynek a felhasználásától a világ jelentős mértékben függ. A számos próbálkozás, kísérlet és alternatív megoldás alkalmazása ellenére úgy tűnik, hogy a készletek teljes kiapadásáig alapvető energiaforrásként fog szerepelni a világ szinte minden régiójában.

A Nemzetközi Energiaügynökség (NEÜ)[5] kimutatása szerint, az energiaszektorban a kőolaj egy tetemes 40%-os részesedést birtokol. A 2008-as adatokat alapul véve, az európai régió a globális kőolaj felhasználásból mintegy 41,3%-ot tudhat magáénak. Számszerűsítve az adatokat, napi 80 millió hordós kitermelésről beszélhetünk, amelyen felül az előrejelzések szerint 2015-ig, mintegy 37,5 millió hordó többlet kitermelésre lesz szükség a fogyasztási tendenciák növekedését figyelembe véve. Ugyanakkor a Nemzetközi Energiaügynökség prognózisa szerint, pontosan a készletek véges mivolta miatt, 2015-re mintegy 12,5 millió hordós szakadék fog kialakulni a termelés és a fogyasztás között, amely tovább fogja mélyíteni az „olajéhség” okozta feszültségeket.

A kőolaj ily mértékű túlzott felhasználása a készletek kiapadására, a túlzott függőség kialakulására, a környezetszennyezésre, az alternatív megoldások keresésére hívja fel a figyelmet. Azonban az alternatív megoldásokra való áttérés egy hosszú folyamat eredménye lesz, ugyanis jelen pillanatban az új technológiák ára és hatékonysága jelentősen elmarad a kőolajban rejlő lehetőségektől, nem beszélve az alternatív technológiákra való áttéréshez szükséges tőkebefektetésről.

Többek között a kőolajjal kapcsolatos világméretű problémák kezelésére hivatott egyik legfontosabb szervezet tehát, a Nemzetközi Energiaügynökség, mely napjainkra már jelentős mértékben túlnőtt, és túllépett eredeti, alapításbeli célján és rendeltetésén. Az ügynökség az OECD[6] tagállamainak autonóm energetikai szervezete. Az ügynökséget a tagállamok az első olajárrobbanást követően, 1974-ben hozták létre az egységes fellépés érdekében. Alapdokumentuma a Nemzetközi Energia Programról szóló Egyezmény. Létrehozásának célja az intézményesített olajválság kezelő feladatkör volt. Napjainkban, pedig hosszú távú feladatként vállalta a tagországok energetikai problémáinak kezelését úgy, mint az olajellátás zavarait csökkentő rendszer fenntartását, a rendkívüli helyzetre való felkészülést, az energiaellátás, az energiahatékonyság növelését, és az alternatív energiaforrások kifejlesztését, az olaj és egyéb energiahordozó piacokról való állandó információs rendszer működtetését, stb. Az ügynökség legfontosabb döntéshozó szerve a Kormányzó Tanács (GB Governing Board), mely kétévente miniszteri szinten tartja üléseit. Magyarország 1997-től tagja az ügynökségnek. [11]

Földgáz

Ahhoz, hogy a túlzott mértékű kőolajon alapuló energiafelhasználásról át lehessen térni az alternatív megoldásokra, a szakemberek egybehangzó véleménye szerint szükséges egy átmeneti energiagazdaság kialakítása. Ennek a szektornak az egyik legmeghatározóbb szegmense a földgáz, azon egyszerű okból kifolyólag, hogy a kőolajhoz képest a rendelkezésre álló készletek mennyisége számottevően nagyobb, az ára valamelyest kedvezőbb, egy kényelmes energiaforrás, a felhasználás szempontjából, pedig viszonylag

[5] *Nemzetközi Energiaügynökség (NEÜ):* International Energy Agency (IEA)

[6] *OECD:* Organisation for Economic Co-Operation and Development – Gazdasági Együttműködés és Fejlesztés Szervezete, mely egy 1961-től működő nemzetközi szervezet, amely az 1948-ban megalapított OEEC (Organisation for European Economic Cooperation – Európai Gazdasági Együttműködés Szervezete) utódja. A fejlett országok gazdaságpolitikai fóruma, melynek Magyarország 1996-tól tagja. Tagjai közül néhányat megemlítve: Egyesült Államok, Anglia, Kanada, Franciaország, Belgium, Csehország, Finnország, Görögország, Hollandia, Japán, Németország, Olaszország, Spanyolország, Svájc, Szlovákia, stb.

magas tisztaság jellemzi. Azonban a kőolajhoz hasonlóan legfőbb hátránya abban rejlik, hogy földrajzilag egyenlőtlen eloszlást mutat, hiszen a termelés jelentős hányadát, mintegy 60%-át Észak-Amerika, Oroszország és a volt Független Államok Közösségének tagországai biztosítják. Ezen okból kifolyólag a korábban említett, az importáló országokra jellemző függő, az exportáló és a tranzit országoknak kiszolgáltatott helyzeten nem képes gyökeresen változtatni.

A 2008-as adatokat figyelembe véve, a világ energiafelhasználásának mintegy 25%-át a földgáz teszi ki. Európa elég kiszolgáltatott helyzetben van, hiszen a világ fogyasztásának körülbelül 25%-a ebben a régióban realizálódik, és a kőolajhoz hasonlatosan a lokális készletek hiányában ennek a mértékű fogyasztásnak a legnagyobb hányada ugyancsak import bázison nyugszik. Néhányat megemlítvén a legnagyobb importőrök közül, olyan országok találhatóak a felsorolásban a teljesség igénye nélkül, mint Oroszország, Algéria, Irán, Dánia, Norvégia, Türkmenisztán, stb. [11]

Mint az Európai Unió tagállama, Magyarország is erőteljesen importfüggő ország a földgázfelhasználás szempontjából, mely függőség a hazai kitermelés folyamatos csökkenése és a fogyasztás folyamatos növekedése miatt egyre inkább erősödik. A 2007-es kimutatások szerint az ország elsődleges energiafelhasználásának mintegy 45%-át a földgáz teszi ki, melynek elenyésző része származik csak a hazai kitermelésből. 2007-ben ez a mennyiség mintegy 13,1 $Mrdm^3$ volt, amelyből 2,6 $Mrdm^3$-t biztosított csak az ország a saját forrásaiból, a fennmaradó 10,5 $Mrdm^3$-t, pedig importforrásból. Előrejelzések szerint ez a mennyiség 2015-re el fogja érni a 16 $Mrdm^3$ körüli értéket. Az egyre nagyobb mértékben növekvő fogyasztási igények kielégítése érdekében szükséges a források és a felhasználási területek közötti szállítása útvonalak kibővítése, kiépítése, diverzifikálása, a szállítási kapacitások növelése, illetve az új forrásokkal történő kapcsolatfelvétel. [8] [12]

Kőszén

A kőszén, különböző formákban, mint a fekete kőszén, a barnakőszén, a lignit, a tőzeg, már nagyon régóta része az energiatermelésnek, melynek oka, hogy viszonylag könnyen bányászható, és elégethető. A korábban említett két nem megújuló fosszilis energiaforrással[7] szemben, a kőszén nagy előnye az olcsó kitermelhetőségében, az általa olcsón előállítható elektromos energiában, az évszázadokra becsülhető rendelkezésre állásában, a könnyű szállíthatóságban, a jó tárolhatóságban és abban rejlik, hogy az Európai régióban is viszonylag nagy mennyiségben található meg. A kőszén szállítása egyszerűen megoldható az egyéb más nyersanyagok és késztermékek szállítására hivatott infrastruktúra alkalmazása révén. A fogyasztó által felhasznált mennyiség, alapvetően a kitermelő országban kerül felhasználásra, mivel a helyi gazdaság fokozatosan ráépült a kitermelhető szénvagyonra. Továbbá a jelentős szénkészlettel rendelkező országok többlettermeléséből viszonylag szabad piac alakult ki, melyre nem jellemző a kartellesedés, egyetlen piaci szereplő sem képes alapvetően befolyásolni az árakat, a kitermelési volument, így egy sem juthat olyan előnyös helyzetbe, amelynek segítségével, az energiaforrással való rendelkezését egyéb érdekeinek az érvényesítésére használhatná fel globális szinten. [8] Ugyanakkor a szakemberek egybehangzó véleménye alapján az egyik legszennyezőbb energiaforrásnak tekinthető.

A kőszén a világ villamosenergia-termelésében, globális szinten, mintegy 40%-os részesedéssel bír. Magyarország vonatkozásában megállapítható, hogy az ország primer energiaszükségletének mintegy 16%-át a kőszén fedezi, és a 2015-ig előrevetített statisztikai adatokat figyelembe véve, ez az arány folyamatosan csökkenő tendenciát fog mutatni a globális szinten jellemző földgáz és kőolajfüggőség egyre nagyobb mértékű térhódításával. Abban az esetben, ha kézzelfogható megoldások fognak realizálódni a környezetszennyezés mértékének, illetve a túlzott széndioxid kibocsátás mennyiségének a csökkentésével

[7] *Fosszilis energiaforrás:* Fosszilis energiaforrások alatt a bányászott szenet, a ként és a szénhidrogéneket (kőolaj, földgáz) értjük, melyek elhalt és lebomlott növények és állatok maradványai. Energiaforrásként történő felhasználásuk elégetésükkel lehetséges, mely folyamat során jelentős mennyiségű szennyező anyag kerül a légkörbe, növelve az üvegházhatást, elősegítve a globális felmelegedést.

kapcsolatban, a földgázhoz hasonlóan, a kőszén is, a már korábban említett átmeneti energiagazdaság egyik meghatározó energiaforrása lehet. [11] [12]

Nukleáris energia

Az atomenergia napjaink egyik legvitatottabb energiaforrása, mellyel kapcsolatban, több szempontból is jelentős mértékben megoszlik a szakemberek és a közvélemény álláspontja. Egyrészt magasztalják, mint a világ energiaproblémájának megoldását, másrészt elvetik, mint az energiatermelés legveszélyesebb módját. Sokakban a biztonságos felhasználás kételye merül fel elsőként, rettegvén egy, a Csernobili atomerőműben bekövetkezett hasonló atomkatasztrófától, ismervén többek között azt a tényt, hogy napjainkban is még nem egy, ehhez az atomerőműhöz hasonló erőmű funkcionál, de említhetnénk a Three Mile Island-i balesetet[8] is. [13] Ezek hatására, globális szinten elég jelentős mértékben felerősödött az össztársadalmi tiltakozás, a politikai és társadalmi elfogadottság redukálódása. Vannak országok, ahol megállt a reaktorok építése, mint például az Egyesült Államokban, ahol 1978. óta nincs megrendelés új atomreaktorokra, vagy például Svédország, ahol népszavazás döntött arról, hogy 2010-re le kell állítani az atomenergia termelést. A Nemzetközi Atomenergia Ügynökség (NAÜ)[9] kimutatása szerint is egyre inkább csökkenő tendenciát mutat ennek az energiaforrásnak az alkalmazása. Mindezek ellenére az európai régióban a villamosenergia-termelés közel 1/3-a ennek az energiaforrásnak az alkalmazásából származik, mely a legnagyobb európai szénmentes energiaforrás. [14] Magyarországra levetítve a statisztikát, az ország primer energiafelhasználásának, pedig mintegy 13%-át szolgáltatja az atomenergia. [12] A statisztikai adatokban természetesen az is benne foglaltatik, hogy az atomenergiában rejlő előnyök felülmúlják a hátrányait, és globális szinten nem egységes a megítélése, mivel a fokozódó energiaigény a felhasználásának a fokozódását vetíti előre. A rengeteg érv és ellenérv mellett sokak szerint a nukleáris energia a reneszánszát éli napjainkban, annak következtében, hogy az egyetlen környezetbarát lehetőség, nagy mennyiségű villamosenergia-előállítására. Ennek bizonyítéka Franciaország, Kína, Brazília, Japán, Pakisztán, Oroszország vagy éppen India fokozódó igénye ezen energiaforrás alkalmazására, amely országokban vagy tervezik, vagy már folyamatban van nukleáris erőművek építése. [15]

Az Európai Unión belül a tagállamoknak megadatik a döntés joga az atomenergia felhasználásával kapcsolatban, de abban az esetben, ha a mellőzése mellett döntenek, akkor mindenképpen alacsony szénkibocsátású energiaforrásokat kell az energiatermelés szolgálatába állítaniuk, az üvegházhatású gázok kibocsátásnak a csökkentése érdekében. [14]

Ugyanakkor a túlzott kőolaj függőség állapotából való kizökkenésen nem túl sokat segíthet az eltérő felhasználási területből adódóan, hiszen a kőolaj egyik elsődleges alkalmazási területe a közlekedés, míg az atomerőművek alkalmazásával, pedig villamos energiát termelnek. További jelentős probléma az atomenergia energiaforrásként való felhasználásával kapcsolatban, a kőszénhez hasonlóan, a környezetszennyezés, gondoljunk csak az atomhulladék biztonságos elhelyezésére, hiszen ezeknek a radioaktív anyagoknak a felezési, lebomlási ideje nagyon hosszú években mérhető. Ugyanakkor viszont az is igaz, hogy a termelési folyamat során viszont kevesebb járulékos ipari hulladék keletkezik, mint más erőművekben. Maradván a környezetszennyezés problematikájánál, a jelenleg alkalmazott technológiák miatt, az urán dúsításához, széntüzelésű erőművek alkalmazására van szükség, mely tovább növeli a zöldek tiltakozását, a környezetszennyezés oldalára billentve a mérleg serpenyőjét. A negatívumok sorában kell megemlíteni az atomerőművek létesítésével és üzemeltetésével kapcsolatos jelentős költségvonzattal járó, időigényes beruházást is, valamint az urán egyre növekvő világpiaci árát. A biztonság aspektusából megvizsgálván az

[8] *Three Mile Island-i baleset:* 1979. március 28-án, a Pennsylvania állambeli Harrisburg városkától nem messze található atomerőműben bekövetkezett súlyos baleset, melynek során a csernobili tragédiával ellentétben nem következett be a környezet radioaktív sugárzással történő szennyeződése. Szakértői vélemények szerint az ok tervezési hiba és a nem megfelelően elvégzett karbantartási munkálatok voltak, melynek következtében elháríthatatlan üzemzavar keletkezett, a hőelvezetés megszűnt, a reaktor bizonyos részeiben jelentős nyomás és hőmérsékletnövekedés következett be.

[9] *Nemzetközi Atomenergia Ügynökség (NAÜ):* International Atomic Energy Agency (IAEA)

atomenergiát, pedig egy újabb negatívumot róhatunk fel rovására, hiszen ebben a globalizált világban, az új típusú kihívások egyik legmeghatározóbb alkotóeleme, a terrorizmus szempontjából sem egy biztonságos alternatíva. A terrorizmus fanatikus követői körében egyrészt egy atomerőmű nagyon könnyen elsődleges, stratégiai célponttá válhat, másrészt az energiatermelési folyamat során, a hatékonyság növelése érekében, a fűtőanyag urán tartalmának egy részét plutóniummá alakítják, mely illetéktelen kezekbe jutva alkalmas lehet atomfegyver előállítására. [14]

Mindezen aggodalmak ellenére, sokan a jövő egyik nagy lehetőségét látják benne hatékonysága és relatíve tiszta energiaforrás létéből adódóan. A korábban felsorakoztatott energiaforrásokkal szemben kategóriákkal nagyobb mennyiségű energia előállítására alkalmas, mint a mechanikai erőn alapuló energiaforrások (szél, vízenergia) vagy az ipari forradalom vívmányaként, az ember szolgálatába állított, különböző kémiai reakciók (égési folyamatok, elektrokémiai reakciók). Az atomerőművek gazdasági szempontból fel tudják venni a versenyt az energiapiac többi szereplőjével szemben, mivel a „nukleáris üzemanyag" nagy energiasűrűségű, és jól tartalékolható, az atomerőművek üzemeltetetési költsége a nagy beruházási költségek és az urán növekvő világpiaci ára ellenére alacsony, ebből adódóan az általuk termelt villamos energia, kedvező áron értékesíthető a piacon, és a technológia alkalmazása nem fokozza az üvegházhatású gázok kibocsátásának mértékét. Továbbá kiemelendően jelentős szempont, hogy a nukleáris energiaforrás a kőolajjal és a földgázzal ellentétben, nem a föld politikailag, társadalmilag instabil berendezkedéssel bíró régióiból származik. [14]

Az aggodalmak, kételyek és a globális energiaproblémát megoldani képes érvek és ellenérvek között lévő összhang, talán egyetlen lehetséges módja a nemzetközi szabályozás és a szigorú biztonsági intézkedések bevezetése, új, úgynevezett 4. generációs atomreaktorok[10] építése, és alkalmazása, melyek segítségével a már használhatatlannak tűnő kiégett fűtőanyagok újra, illetve tovább hasznosíthatóak, megoldást találva átmenetileg a nukleáris hulladék tárolási problematikájára. [15] Erre hivatott többek között a Nemzetközi Atomenergia Ügynökség (NAÜ), mely egy független kormányközi ENSZ szervezet. Az ügynökség 1957-ben jött létre, és jelenleg 144 tagja van, mely tagok között Magyarország is képviselteti magát, mint alapító tag. Legfőbb döntéshozatali szerve a tagállamok évente ülésező Általános Konferenciája. Az ügynökség tevékenysége három nagy területet foglal magába, melyek a nukleáris energia és más nukleáris technológiák békés célú felhasználásának segítése és támogatása, a nukleáris biztonság erősítése, továbbá a nukleáris tevékenység békés jellegének ellenőrzése, az úgynevezett biztosítéki rendszer keretében.

A MEGÚJULÓ ENERGIAFORRÁSOK

Az energiafogyasztás szakadatlan növekedése az 1970-es évek derekán rádöbbentette a világot arra, hogy az ipari fejlődésnek gátat szabhat az energiaforrások kimerülése, mely napjainkban egyre nagyobb mértéket ölt. Szakértői, borúlátó vélemények alapján a Föld fosszilis energiaforrás készletei körülbelül 50-60 évre elegendőek még. Nagyjából erre az időszakra tehető az alternatív vagy megújuló energiaforrások iránti érdeklődés felébredése is, melyeknek egyre hatékonyabb és szélesebb körű alkalmazása megoldást jelenthet a kimerülő energiaforrások kiváltására.

A megújuló energiaforrás egyrészt olyan energiaforrás, amely a természeti folyamatok során folyamatosan rendelkezésre áll, másrészt olyan természeti jelenség, amelyből úgy nyerhető ki energia, hogy az, jelentősebb emberi beavatkozás nélkül, néhány éven belül újratermelődik. A megújuló energiaforrások közzé sorolandó többek között a napenergia, a szélenergia, a vízenergia, a biomassza, a geotermikus energia, stb. Olyan természeti

[10] *4. generációs atomreaktor:* nagyobb hőmérsékleten, magasabb hatásfokkal működő reaktorok, mint a termikus elven működő reaktorok, amelyek azoktól eltérően, nagyobb hatásfokú láncreakciók eredményeképpen, az urán fűtőanyag sokkal nagyobb hányadát hasznosítják, csökkentve a nukleáris hulladék mennyiségét, egy áttekinthetőbb biztonsági rendszert és egy kevésbé kifinomult vezérlést lehetővé téve. A láncreakció lényege az urán 235-ös izotópjának gyors neutronokkal történő bombázása a hasadás nagyobb hatásfoka érdekében.

erőforrások tehát, amelyek hasznosításával az emberiség a szükségleteit az adott gazdasági fejlettség szintjén kielégítheti, és használatuk ellenére természetes úton újratermelődnek. Az alternatív energiaforrások egyik legelőnyösebb tulajdonsága, hogy környezetkárosító hatásuk elenyésző, a fosszilis energiaforrásokhoz képest folyamatosan, akár generációkon át kinyerhetőek a természetből, és összhangban vannak a fenntartható fejlődés alapelveivel.

A fenntartható fejlődés fogalma az 1980-as évek elején jelent meg a nemzetközi szakirodalomban. Általános ismertségét Lester R. Brown[11]-nak a fenntartható társadalom kialakításával kapcsolatos műve alapozta meg, melyben a szerző összekapcsolta a népességnövekedést a természeti erőforrások hasznosításával, és mindezt úgy kívánta megvalósítani, hogy a lehető legkisebb legyen a természeti környezet minőségi és mennyiségi romlása. A fenntartható fejlődés fogalmát az ENSZ Környezet és Fejlődés Világbizottsága fogalmazta meg az 1987-ben kiadott „Közös Jövőnk" című jelentésében. Ebben a jelentésben a gazdasági növekedés egy új korszakának lehetőségét vázolta fel, amely a fenntartható fejlődés globális megvalósítására épít, megőrzi a természeti erőforrásokat, és amely megoldás lehetne a fejlődő országokban elhatalmasodó, egyre nagyobb szegénységre. A jelentés értelmében a fenntartható fejlődés fogalma nem más, mint egy „…….olyan fejlődés, amely kielégíti a jelen szükségleteit anélkül, hogy veszélyeztetné a jövő nemzedék esélyét arra, hogy ők is kielégíthessék a szükségleteiket." A fenntartható fejlődés három alappilléren nyugszik, melyek a szociális, a gazdasági és a környezeti alappillérek. [16]

Napenergia

Mindenki előtt ismert tény, hogy a Nap a földi élet elsődleges energiaforrása. Ez a hatalmas fúziós erőmű már több milliárd éve működik. A Napban hidrogénatomok alakulnak át héliumatomokká, óriási gravitációs nyomáson és rendkívül magas hőmérsékleten. A nap hatalmas tömegében, amely a naprendszer mintegy 99%-át teszi ki, az évmilliárdos működés ellenére még mindig több mint 70% hidrogén található, amely ilyen szempontból szinte kimeríthetetlen energiaforrásként értelmezhető. Ezen aspektusból az egyik legígéretesebbnek tűnő, megújuló energiaforrás, melynek segítségével, napkollektorok és napelemek alkalmazása révén, villamos energia és hőenergia állítható elő. Tehát az aktív energiatermelés szempontjából két eltérő módon is felhasználható.

A fosszilis energiaforrásokkal szemben hosszú távú megoldást jelenthet a globális energiaszükségletek kielégítésére, hiszen a megújuló energiaforrások egyik legfőbb ismérvének megfelelően, folyamatosan rendelkezésre áll, illetve egy szénhidrogénmentes energia előállítás valósítható meg felhasználásával, jelentős mértékben csökkentve ennek következtében a légköri-környezetszennyezést. További nagy előnye a nem megújuló energiaforrásokkal szemben, hogy segítségével egy decentralizált energiarendszer lenne megvalósítható, mely az energiapiac résztvevői-fogyasztói számára lehetővé tenné a saját energia előállítást, csökkentve ily módon az energiapiac szolgáltatói-forrás szektorától való függőséget. Azonban nagy hátránya a fosszilis energiaforrásokkal szemben, hogy még mindig sokkal költségesebben lehet vele energiát előállítani, mondjuk egy széntüzelésű hőerőműhöz képest, elsősorban a magas beruházási költségek miatt, melyek megtérülése viszonylag hosszú idő, mintegy 20-22 évre tehető. Hátrányos ismérveként kell megemlítenünk azt a tényt is, hogy a folyamatos fejlesztések ellenére, még mindig viszonylag kis hatékonysággal képes a villamosenergia-előállítására, illetve a földrajzi viszonyok is jelentős hatást gyakorolnak alkalmazhatóságára a napsütéses órák számát figyelembe véve. Napjainkban, a Föld napsütésben bővelkedő területein is, a működési idő mindösszesen 22%-ban alkalmas

[11] *Lester R. Brown:* Az Earth Policy Institute (Földpolitikai Intézet) elnöke, akit a Washington Post a világ egyik legbefolyásosabb gondolkodójának tart. A szervezetet 2001. májusában alapította azzal a céllal, hogy terveket dolgozzon ki, és tegyen közzé a fenntartható jövő kialakításáról. Többek között az ő nevéhez kapcsolódik a fenntartható fejlődés fogalmának a megalkotása. Ő volt egy másik jelentős szervezet, a World Watch Institute (Világfigyelő Intézet) szervezetnek ugyancsak az alapítója, amelynek a létrehozását követő 26 éven keresztül ő volt az elnöke. Pályafutását gazdálkodóként kezdte, majd munkásságának eredményeképpen több mint 50 könyv fűződik a nevéhez szerzőként vagy társszerzőként, melyek több mint 40 nyelven jelentek meg. Tudományos tevékenységének köszönhetően 24 egyetem is tiszteletbeli doktorává fogadta.

energiatermelésre, egy hőerőmű ily szempontból 90%-os hatékonyságával szemben. Továbbá, mivel egy viszonylag új technológiáról van szó, a hozzá kapcsolódó iparág fellendülése, az új munkahelyek teremtése, az elszigetelt földrajzi helyek energiaellátásának megoldása, mint pozitív jellemző mellett, felvetődik a napelemek, napkollektorok életciklusának a végén jelentkező, jövőbeni hulladékkezelésnek a problematikája is. Mindezek ellenére a folyamatos fejlesztések eredményeképpen a jövő egyik legkecsegtetőbb alternatív energiaforrásainak egyike lehet. [11] [17]

Szélenergia

A szélenergia ipar napjaink legdinamikusabban fejlődő, megújuló energiát alkalmazó, tiszta energiatermelő technológiája. Globális szinten történő alkalmazása a környezetvédelmi és a költségelőnyei miatt egyre nagyobb teret hódít, egy nagyon jó alternatív megoldást kínálva a fosszilis energiahordozókat mellőző, villamosenergia-termelésimód megvalósítására.

Az elv messzemenőkig egyszerű, a légtömeg mozgásából „forgó" energiát nyerni, majd ezt a mozgási energiát generátorok segítségével elektromos energiává alakítani. A szélenergia kitermelésének modern formája tehát a szélturbina lapátjainak forgási energiáját alakítja át elektromos energiává, mely ily módon alkalmas hálózatba integrálható villamosenergia-előállítására, komplex „szélfarmok" vagy kisebb „széltelepek" keretébe szervezve a berendezéseket. Ugyanakkor a napenergiához hasonlóan, ez az energiaforrás is alkalmas egyéni energiatermelésre (nemzeti vagy akár konkrét fogyasztói szinten), mely lehetőség megoldást jelenthet a fosszilis, nem megújuló energiaforrásokhoz való hozzáférés okozta piaci kiszolgáltatottságra, függőségre. Az alkalmazott eszközök legfontosabb jellemzője a magas műszaki színvonal és a csekély karbantartási igény.

Alkalmazásával kapcsolatban azonban problémák is felvetődnek, melyek többek között a szélturbinák méretéből adódó nagy térigény, valamint a kis megbízhatóság, hiszen a működési idő nagy részében jóval a maximális teljesítmény alatt működnek. A szélenergia jelentős mértékben ki van szolgáltatva az időjárási körülményeknek, melyek alapvetően meghatározzák a primer energia, a szél rendelkezésre állását és „minőségét", mely utóbbi tényező alatt elsősorban a szélerősség, szélsebesség kérdése értendő. [18] Továbbá gondot jelenhet a telepítési hely körültekintő megválasztása is, mely egyrészt összefüggésben van az imént említett földrajzi – környezeti – időjárási tényezővel, másrészt a szélturbinák működési elvéből adódó, zavaró hatású, zaj és fénytényezőkkel. Ezen okokból kifolyólag a telepítési helyszínek általában nagy távolságokra helyezkednek el a felhasználás helyszínétől, melynek következtében a szélerőművek által termelt elektromos energiát viszonylag nagy távolságokra kell elszállítani, ami növeli az alkalmazás járulékos költségeit. Ez alatt elsősorban a szállítási infrastruktúra kiépítésével kapcsolatos költségeket kell érteni, illetve azoknak a beruházásoknak a költségeit, amelyek egyfajta tárolókapacitásként szolgálnak a szélenergia, környezeti tényezők által befolyásolt, rendelkezésre állása okozta, energia kimaradások kiküszöbölésére, a villamosenergia-hálózat egyensúlyának megteremtése érdekében.

A szélenergia felhasználással kapcsolatos kutatások és fejlesztések terén többek között Németország, Spanyolország, valamint Dánia jár az élen. A folyamatos kutatás-fejlesztés eredményeképpen, egyre nagyobb kapacitású, egyre jobb hatékonyságú szélturbinák előállítására és alkalmazására nyílik lehetőség, egyre nagyobb szerephez jutva, a fosszilis energiahordozókon alapuló villamosenergia-termelés szektorában.

A szélenergia alkalmazásában hazánk is képviselteti magát a Mosonmagyaróváron vagy a Somogy megyei Öreglak térségében telepített szélparkkal, melyek a villamosenergia-termelésre hivatott szélerőművek két különböző családját – az előbbi betáplálja a megtermelt energiát a villamos energiarendszerbe, míg az utóbbi a helyben történő felhasználásra termel energiát – testesítik meg. [11] [14] [17]

Vízenergia

A vízenergia alkalmazása történelmi múltra tekint vissza. Már a régi kultúrákban is, mint például Mezopotámiában, Kínában vagy Egyiptomban is hasznosították, elsősorban a

vízkerekek alkalmazásával, többek között a mezőgazdasági művelés alá vont területek öntözésére, illetve az ivóvíz ellátás biztosítására. Ezt követően a római birodalomban kezdték el használni elsőként a vízimalmokat, illetve a hajókra épített úszómalmokat, a gabona őrlésére. Továbbá alkalmazták a vízkerekek energiáját a kovácsműhelyekben a fém megmunkálására vagy a fűrészüzemekben darabolásra.

Az egyik leggazdaságosabb energiaforrás, melynek segítségével a víztömeg mozgási energiáját átalakítva villamos energia nyerhető. Viszont alkalmazásának lehetőségét jelentős mértékben befolyásolja, a nap vagy a szélenergiához hasonlóan, a természetföldrajzi környezet. Ebben a tekintetben Magyarország nincs éppen a legelőnyösebb helyzetben, ugyanis gazdaságossági szempontból, az energetikai kihasználhatósága alacsony hatásfokú, nem úgy, mint például az Alpokban vagy a Skandinávfélszigeten. Ugyanakkor környezetvédelmi szempontból sem az egyik legkedvezőbb alternatív energiaforrás, a vízerőművek, a duzzasztógátak által okozott negatív környezeti következményekből adódóan, gondolván az érintett folyók, folyóparti területek élővilágára és ökoszisztémájára gyakorolt hatásukról. [11]

Bioenergia

A bioenergia vagy más néven a biomassza fogalma általánosságban nem jelent mást, mint a Földön lévő összes élő tömeg, egy adott élettérben, egy adott pillanatban jelen lévő szerves anyagok és élőlények összessége.

Napjaink globalizált világában a bioenergia az alábbi nemzetgazdasági forrásokból származhat: a növénytermesztésben és erdészetben keletkező melléktermékek, az állattenyésztés, az élelmiszeripar (itt elsősorban a növényolaj-iparra kell gondolnunk), valamint a kommunális és ipari hulladékok. Mindezeket figyelembe véve, a biomassza, a keletkezése alapján három nagy csoportba kategorizálható. Az elsődleges kategóriába tartoznak a természetes vegetáció alkotóelemei, melyek alatt a mezőgazdasági növényeket, az erdőket, a mezőket, a réteket, a legelőket, a kertészeti és vízben élő növényeket értjük. A második nagy kategóriát az állatvilág, illetve az állattenyésztés fő és melléktermékei, valamint hulladékai alkotják. A harmadlagos biomassza csoportba, pedig a feldolgozóiparok és az emberi életműködés melléktermékei sorolhatóak.

A biomasszák legnagyobb előnye abban rejlik, hogy felhasználásuk által a fosszilis energiahordozók kiválthatóak, megtakaríthatóak, megvalósítva ily módon a fenntartható energiafelhasználást, a fenntartható fejlődést, csökkentve a levegő szennyezettségét és az általa okozott globális problémák sorát, mint az üvegházhatás és a felmelegedés. Megújuló energiaforrásnak tekinthetőek, hiszen megfelelő kezelés révén, rövid életciklusok során, általában egy éven belül újratermelődnek.

A biomassza, a fosszilis energiaforrások, a kőolaj, a szén és a földgáz után, a világon a negyedik legnagyobb energiaforrás, mely elsősorban villamos energia és hőenergia termelésre hasznosítható. Globális szinten a felhasznált energia mintegy 14%-át, de a fejlődő országokban több mint a 35%-át ennek a típusú bioenergia forrásnak a felhasználása biztosítja.

A biomasszákat a felhasználási területnek megfelelően az alábbi kategóriákba sorolhatjuk: tüzelhető, elgázosítható és gépjármű üzemanyagként hasznosító biomasszák, mely csoportok egyértelműen utalnak arra, hogy elsődlegesen a hőtermelésre, a hőenergia előállítására, illetve a gépjárművek meghajtására kínálnak alternatív megoldásokat.

A tüzelhető biomasszák alapvetően viszonylag kis nedvességtartalmúak, és ennek megfelelően magas fűtőértékkel rendelkeznek. A velük szemben támasztott legfontosabb követelmény többek között az, hogy az égési folyamat melléktermékeként keletkező hamu olyan vegyi összetételű legyen, hogy az ne károsítsa a különböző fűtőberendezéseket, illetve ne okozzon jelentős levegőszennyezést. A legtipikusabb tüzelhető biomassza fajták a tűzifa apríték, a fűrészpor, a szalma, az energiafű, illetve az ezekből előállított pellet[12].

[12] *Pellet:* olyan nagy nyomáson préselt szálas, rostos anyag, amelyet vagy a saját anyaga vagy a belekevert kötőanyag tart egyben.

Az elgázosítható biomasszák, a tüzelhető biomasszákhoz képest, nagyobb nedvességtartalmú növényi vagy állati hulladékból állnak, mint például a cukortartalmú növények, a zöld növényi hulladék, az állati szennyvíziszap, a trágya, stb. E típusú biomasszák egyik kiemelkedő megvalósulási formája a biogáz[13]. A biogáz alkalmazása elsősorban a környezetvédelem szempontjából jelentős, hiszen többek között például meggátolja a háztartási, állattartási hulladékokból spontán felszabaduló metánnak a légkörbe jutását.

Az üzemanyagként hasznosítható biomasszákat két nagy csoportba sorolhatjuk, a benzin és a diesel üzemanyagként hasznosítható biomasszák. Az első kategóriába elsősorban a magas cukor (cukorrépa, cukornád) vagy magas keményítő (kukorica, burgonya, búza) vagy a magas cellulóztartalmú növények (szalma, fa, nád, energiafű) sorolhatóak, amelyekből különböző kémiai eljárásokkal etanol[14] gyártható. Az utóbbi típusú biomassza esetében, pedig elsősorban az olajtartalmú növényekre (repce, olíva, napraforgó, stb.) kell gondolnunk, amelyekből az olaj kisajtolható, és különböző eljárások révén, egyszerűbb vegyszeres kezeléseket követően, a diesel üzemanyaghoz hasonló olaj nyerhető belőlük.

A biomasszában rejlő lehetőségek a fosszilis energiaforrások kiváltása érdekében Magyarországon kedvező reményekkel kecsegtetnek. Országunkban a mezőgazdaság, a növénytermesztés és az állattartás szerepe mindig is kiemelt helyet foglalt el, köszönhetően az ország kedvező földrajzi adottságainak. A mezőgazdaság, pedig mint az korábban elhangzott, a biomassza megjelenésének egyik legfőbb forrása. Ennek a típusú megújuló energiaforrásnak az egyre fokozottabb alkalmazására történő áttérés segítségével, az ország elektromos és hőenergia szükségletének egyre jelentősebb része lenne biztosítható, csökkentve hazánk importfüggőségét és energiapiaci kiszolgáltatottságát. [18] [19]

Geotermikus energia

A geotermikus kifejezés görög eredetű kifejezés, melynek jelentése földi hő, vagyis a Föld belső hőjéből származó energia. A geotermikus energia a magmából ered, és a földkéreg közvetíti a felszín felé. A föld hő egyik legfontosabb jellemzője a korábban említett megújuló energiaforrásokkal szemben, hogy állandóan, folyamatosan, a kitermelés helyén áll rendelkezésre, rugalmasan alkalmazható, és a meteorológiai viszonyok nem befolyásolják. A korábban említett napenergiához hasonlóan szintén korlátlan, és ugyancsak a környezetet nem szennyező energiahordozóról van szó, amely nálunk csak egyes helyeken koncentrálódó, helyi energiaforrás, mely viszonylag alacsony energiaszinttel rendelkezik.

A geotermikus források felfedezése a történelmi múltba, a római kor idejéig nyúlik vissza. Elsőként a termálvizet alkalmazták elsősorban gyógyászati célokra. A 19. században vált lehetővé elsőként, a technikai új vívmányainak köszönhetően, a földfelszín alatt rejlő termikus erőforrások felfedezése és feltárása, majd a 20. században meginduló villamosenergia-termelés eredményeképpen ebben a szektorban is megjelent. Napjainkban is, globális szinten, elsősorban villamos és hőenergia előállítására használják.

A Kárpát-medence, de főleg Magyarország területe alatt a földkéreg az átlagosnál vékonyabb, ezért országunk geotermikus adottságai igen jók. A geotermikus energia hordozója ebben a régióban elsősorban a termálvíz. Hazánkban a geotermikus energia hasznosítása a hő hasznosításban, illetve a balneológiában[15] nyilvánul meg. A hő hasznosítás egyrészt szezonális jellegű, másrészt egyoldalú és extenzív[16] jellegű, az elhasznált melegvizet nem nyomják vissza, hanem országosan a felszín alatti víztározókba vagy az élővizekbe engedik, ezen okból kifolyólag a felhasználók nagy többsége a tárolt vízkészletekhez, direkt

---

[13] *Biogáz:* A biogáz a szerves anyagoknak a baktériumok segítségével történő lebontása anaerob (oldott oxigénben és kémiailag kötött oxigénben szegény környezet) körülmények között, mely körülbelül 45-70% metánt (CH_4), 30-55% szén-dioxidot (CO_2), nitrogént (N_2), hidrogént (H2), kénhidrogént (H_2S) és egyéb maradványgázokat tartalmaz (pl. metil-merkaptánt (CH_3SH)).

[14] *Etanol:* A benzint helyettesítő vagy annak adalékaként szolgáló bioüzemanyag.

[15] *Balneológia:* Gyógyvíztudományt jelent. A balneológiások kezelések a gyógyvizek kémiai összetételen alapulnak.

[16] *Extenzív:* Kifelé haladó, terjeszkedő.

módon tud hozzájutni. A hő hasznosítás műszaki színvonala még viszonylag alacsony színvonalú és hatékonyságú, valamint a geotermikus alapú villamos energiatermelés még nem nagyon jellemző felhasználási mód.

A HAZAI ÉS AZ EU ENERGIABIZTONSÁG

Meglátásom szerint az energiabiztonság, a biztonság fogalmához hasonlóan egy összetett fogalom, komplex kérdéskör. Véleményem szerint, összefüggéseiben figyelembe véve a fent elhangzottakat, az energiabiztonság kérdése nem csupán az energiaforrásokhoz való hozzájutást, azoknak a kimerülését, és az ebből következő feszültségeket és problémákat jelenti. Mindezeken túlmenően, szoros összefüggésben van az alkalmazott energiatermelési mód biztonsági kockázataival és a környezetre gyakorolt hatásaival is, a nukleáris fenyegetettség vagy az új típusú kihívások, mint a terrorizmus, a globális felmelegedés és a klímaváltozás egyre égetőbb kérdése miatt, mely, pedig a biztonság e szektorának szerves részévé teszi az alternatív-megújuló energiaforrások alkalmazására való áttérésben rejlő, megoldásra váró kérdéseket és nehézségeket is.

Napjainkban az energiabiztonság egyre inkább stratégiai kérdéssé válik mind az Európai Unió mind, pedig a NATO számára. Nem végződhet úgy csúcstalálkozó, konferencia, hogy a napirendi pontok között ne szerepeljen az energia, mint a biztonság szempontjából egyre nagyobb jelentőséggel bíró kockázati tényező. Adódik ez azon egyszerű okból kifolyólag egyrészt, hogy az energiahordozókból Európa az egyre inkább növekvő szükségleteihez képest nem rendelkezik elegendő mennyiségű saját készlettel, így a hiányzó részt földrajzilag is egyre távolabb eső forrásokból kell beszereznie, pótolnia, kiszolgáltatott, importfüggő helyzetbe kerülve így az energiapiac egyéb, energiahordozókkal rendelkező szereplőihez képest. Természetesen globális szinten is egyre inkább növekszik a korábban említett „energiaéhség”, párhuzamosan azzal, hogy a véges energiakészletek, a könnyen kitermelhető energiaforrások mennyisége folyamatosan csökken, földrajzilag egyre inkább behatárolódik. Ez az ellentét magával hoz egyfajta versenyhelyzetet, melyben a világ különböző gazdasági-politikai centrumainak versenybe kell szállniuk egymással az energiaforrásokért. Mint korábban mondottam volt, az energia hatalom, így ebből a versenyből győztesen kikerülő fél, előnyös helyzetét, fel tudja használni majd egyéb érdekeinek az érvényesítésére is. [8] Ezt a túlsúlyt, fölényes helyzetet, mint például a Gazprom monopol helyzetét azonban nem szabad engedni, kompromisszum kész megoldások felvázolásával, az energiapiac szereplőit, kölcsönösen érdekelt, és legfőbbképpen egyenrangú félként kell bevonni a probléma megoldásába.

Mint azt korábban említettem, az energiabiztonság szempontjából az egyik leginkább meghatározó tényező a kőolaj és a földgázellátás helyzete, mely nem megújuló energiaforrásoknak a beszerzési forrásait, a szállítási útvonalait stabilizálni és diverzifikálni kell. Ez a biztonság megteremtésének egyik alapvető kritériuma. Különösen igaz ez az európai régióra, annak is a keleti részére, így Magyarországra, aki ebben a tekintetben eléggé kiszolgáltatott helyzetben van, hiszen például a földgázimport vonatkozásában, legnagyobb mértékben Oroszországtól függ. Sokáig nagy reményeket fűztek a Makó térségében található földgázlelőhelyhez, melynek feltárása során fokozatosan vált nyilvánvalóvá, hogy az ott rendelkezésre álló készletek elég mélyen vannak, valamint nagyon magas a kénszennyezettségük, melynek következtében a kitermelés és a felhasználható tisztaságúvá alakítás jelentős tőkebefektetést igényelne, melyet az ország nem képes vállalni. [8] Az európai legfőbb import irányok, az orosz forrás mellett, az Északi-tengeri, valamint az Észak-Afrikai régió, mely utóbbi, elsősorban az észak olasz iparvidék energiaszükségletének a kielégítésére hivatott. A forrásokhoz való szélesebb körű hozzájutást, diverzifikálást biztosítanák az újonnan megépítésre kerülő vezetékek, mint például a Nabucco, amely Közép-Ázsiából szállítana gázt a régióba Oroszország megkerülésével vagy a Déli Áramlat. A MOL csoport tagjaként a Magyarországi Földgázszállító (FGSZ) élen jár a források és a szállítási útvonalak diverzifikálásában. Jelen pillanatban Magyarország területére egy keleti és egy nyugati beszállítás ponton keresztül érkezik földgáz, a HAG vezetéken keresztül Ausztriából

Mosonmagyaróvár belépési ponttal mintegy 4,4 $Mrdm^3$ éves, 12 Mm^3 napi kapacitással, valamint a Testvériség földgázvezetéken keresztül Beregdaróc belépési ponttal Ukrajna felől 10 $Mrdm^3$ éves, 30 Mm^3 napi csúcskapacitással. A hazai termelésből 3,5 $Mrdm^3$ éves, 11,2 Mm^3 napi csúcskapacitás származik, melynek növelése lehetőségeinkhez mérten a jövő távlati célkitűzése. A fejlesztések több irányúak, mely jelenti egyrészt a hazai vezetékszakaszok kibővítését a föld alatti tározók kibővítése, illetve az ország jövőbeni várható tranzitország-szerepének elősegítése érdekében, valamint a különböző összekötő vezetékek megépítését a szomszédos országok irányából érkező földgázvezetékek csatlakoztatása érdekében, mely szolgálja egyben a saját szükségletek kielégítését és szintén a tranzitvezetékek áthaladását országunk területén. [12]

A napjainkra jellemző, egyrészt előnyös gazdasági fejlődés, szoros velejárója tehát a globális energiaigény fokozódása, mely, ha a fejlődés jelenlegi trendje nem változik, szakértői előrejelzések alapján 2030-ra mintegy 50%-al fog növekedni. A földgáz vonatkozásában az Európai Unió Energia és Közlekedési Főigazgatóságának az előrejelzése szerint 2030-ra mintegy 84%-ot is elérheti a gázimport mértéke. A források diverzifikálása és stabilizálása mellett, bárkiben jogosan vetődhet fel a kérdés, hogy rendelkezésre fognak e állni egyáltalán megfelelő mennyiségben a szükséges energiaforrások, a fogyasztók mennyire férhetnek hozzá biztonságosan a forrásokhoz, továbbá hogyan és milyen mértékben lehet helyettesíteni a hagyományos értelemben vett energiahordozókat az alternatív, megújuló energiahordozókkal. Az alapvető probléma egyrészt abban rejlik, hogy a forrásokkal rendelkező országok demokratikus berendezkedése, bel és külpolitikai helyzete nagyon sérülékeny, gondoljunk itt elsősorban Azerbajdzsánra, Türkmenisztánra, Kazahsztánra vagy Oroszország bizonytalan és kiszámíthatatlan külpolitikai helyzetére. Azonban minden bizonnyal az Európai Unió növekvő gázfüggőségének egyik legnagyobb haszonélvezője ennek ellenére Oroszország lesz, akinek ugyancsak szüksége lesz az európai piacokra. Alternatív forrásként jöhet szóba a Kaszpi-tenger térségéből érkező földgáz és kőolaj import, mellyel kapcsolatban két fő probléma merül fel. Egyrészt a forrásokat olyan demokratikus tekintélyuralmi rendszerek ellenőrzik, melyek nem tudnak önállóan, Oroszországtól függetlenül megjelenni az európai piacon, másrészt gondot jelenthet a tranzitútvonalak biztonsága, a szállítási útvonalak védelme, az energiahordozók biztonságos eljuttatása a fogyasztó nemzetekhez. A szakértők véleménye azonban az, hogy az energiabiztonság megteremtéséből ki kellene zárni a politikát, abban elsősorban a szabad piacnak, a különböző cégek közötti megállapodásoknak kellene a legfőbb szerepet játszani. Ily módon a kisebb ellátási problémák könnyen kezelhetőek lehetnének, az országok közötti megállapodások, a kiépített vezetékek és a tározók segítségével.

A diverzifikáció másik lehetséges módja az alternatív, megújuló energiaforrásokra való, egyre szélesebb körű áttérés lehetőségeinek a kiaknázása. Az Európai Uniónak egy közös összefogás eredményeképpen, egyre nagyobb hangsúlyt kell helyeznie ezen energiahordozókban rejlő lehetőségek kiaknázására, minimálisra redukálva alkalmazásuk által, a fosszilis energiahordozóktól való túlzott függést, a környezetszennyezést, illetve oldva az általuk okozott gazdasági-politikai feszültségeket.

A kérdés időszerűsége nem vitatott, hiszen az Európai Unió nagyon szigorú követelményeket és elvárásokat fogalmaz meg a tagállamok részére a szén-dioxid és egyéb üvegházhatású gázok kibocsátási mértékével kapcsolatban, melynek alapja többek között a Kiotói jegyzőkönyv, melynek értelmében, a „B" függelékében feltűntetett országok, vállalták, hogy 2008 és 2012 között, öt év átlagában meghatározott mértékben, az 1990-es kibocsátási szint alá csökkentik az üvegházhatású gázok kibocsátásának a mértékét. Ebben a jegyzőkönyvben az Európai Unió vállalta, hogy a nevezett időintervallumban mintegy 8,2 %-al csökkenti a környezetszennyező gázok kibocsátásnak a mértékét. Az Unió, a megújuló energiaforrások 2020-ra elérendő részarányát 20%-ban határozta meg, mely Magyarország vonatkozásában mintegy 13%-os részarányt ír elő, céloz meg, az energiatermelés egyéb módjainak részarányához képest.

Mindezeknek a vállalásoknak a teljesítéséhez természetesen mind Uniós mind, pedig nemzeti szinten jelentős támogatásra és tőkeinvesztícióra van szükség a kutatás-fejlesztés és a

gyakorlatba való átültetés terén. Ennek kiemelkedő példája Magyarország vonatkozásában a Kormány 2008. szeptember 3-án elfogadott „Stratégia a magyarországi megújuló energiaforrások felhasználásának növelésére 2008-2012 között" című KHEM[17] előterjesztés, mely elsősorban a villamosenergia-termelésben alkalmazandó alternatív energiaforrásokkal foglalkozik, mint a biomassza, a geotermikus energia és a szélenergia. A folyamatos kutatások és fejlesztések eredményeképpen egyre nagyobb hatásfokú, kapacitású, egyre költségtakarékosabb, megbízhatóbb technológiák kifejlesztésére nyílik lehetőség, mely magával hozza a fosszilis és egyéb nem megújuló energiaforrásokkal szemben, az alternatív megoldások részarányának a növekedését az energiatermelésben. [14]

A biztonság harmadik általam megjelölt szegmensének, a jelenleg is alkalmazott energiatermelési módokban rejlő kockázatoknak és kihívásoknak a vonatkozásában, pedig elsősorban a nukleáris energia tekintetében kell vizsgálódnunk. Az atomenergia vonatkozásában a legfőbb megoldásra váró kérdés, az új típusú, úgynevezett 4. generációs atomerőművek kifejlesztése és tökéletesítése, melyek kis túlzással minden, ebben az energiatermelési szektorban jelentkező problémát orvosolni képesek. Ezek alatt értendő többek között a technológia folyamat során keletkező plutónium részarányának a lecsökkentése, a nukleáris fűtőanyagok és hasadási termékek proliferációjának a megakadályozása, kiküszöbölve az elvi és gyakorlati lehetőségét egy esetleges atomfegyver előállításának, a nukleáris erőművek biztonságosabbá tétele, a reaktorbalesetek elkerülése, és egy súlyos probléma, a környezetet és az emberiséget veszélyeztető, szennyező nukleáris, radioaktív hulladék keletkezési és tárolási a problémájának a megoldása. Az új fejlesztéseknek köszönhetően ez az energiatermelési szektor, mely gyakorlatilag kimeríthetetlen tartalékokkal rendelkezik, a jövőben is fenntartható lesz oly módon, hogy nem fog hozzájárulni a kedvezőtlen környezeti hatásokhoz, a klímaváltozáshoz, a globális felmelegedéshez. [19]

KONKLÚZIÓ

Korunkban az energiatermelés legnagyobb hányadában még mindig a fosszilis energiahordozókra épül, melyek meghatározó szerepet játszanak az üvegházhatású gázok kibocsátásában, előidézve, fokozva a környezetszennyezést, a globális felmelegedést, a klímaváltozást. Az energiahatékonyság növelése, az alternatív, megújuló energiaforrásokra történő áttérés megvalósításával talán már el is késtünk, de minden bizonnyal halasztást nem tűrő probléma globális szinten, mivel a fosszilis energiaforrások alkalmazásával járó negatív hatások már réges régen beindították az éghajlatváltozásnak a földi létre gyakorolt kedvezőtlen folyamatait.

A globalizáció, a gazdasági fejlődés előrehaladtával a világ meghatározó gazdasági centrumainak az energiaigénye fokozatosan növekszik, mellyel párhuzamosan az energiapiac függőségi, kiszolgáltatott, feszültségekkel teli viszonyai is fokozódnak, felerősödnek.

Napjainkra az energia a geopolitikai első számú faktoraként, a változások fő hajtóerejét képezi. Újra kell gondolni jó néhány geopolitikai elméletet, többek között azt az elképzelést, hogy a globalizációnak köszönhetően a határok értelmüket veszítik, az információ és a tudás a legfontosabb és, hogy az energiaforrások szabadon mozognak. A fent elhangzottakból mindenki számára egyértelművé válik, hogy az energiaforrásokban gazdag földrajzi területek értéke, napjainkban, óriási mértékben felértékelődött, az elhelyezkedés jelentősége, az energiaalapú világ miatt, Adódik ez azon egyszerű okból kifolyólag, hogy amelyik ország kedvezőbb földrajzi fekvéssel bír, sokkal nagyobb az esélye a természeti erőforrásokhoz, az energiahordozókhoz való hozzájutásra, az energiapiac meghatározó, domináns szereplőjévé válásra, különösen a földgáz és a kőolajlelőhelyek tekintetében.

Az energiabiztonság kérdését komplex módon kell kezelni, melyben globális szinten a Föld minden országának, az energiatermelési szektor minden résztvevőjének jelentős feladata van.

[17] *KHEM:* Környezetvédelmi, Hírközlési és Energiaügyi Minisztérium

HIVATKOZÁSOK

[1] Az információs hadviselés hazai kormányzati kihívásai. Tanulmány kivonat. – p. 1-6. (Forrás:http://www.enoadvisory.com/doc/Informacios_Hadviseles_Tanulmany_EXTRACT_ENO_Advisory.pdf /letöltés ideje: 2009.10.24./)

[2] Szabó András: Az információs hadviselés és a hadtudomány. – In: Hadtudomány A Magyar Hadtudományi Társaság folyóirata, 1998. december, VIII. évfolyam 4. szám (elektronikus). (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/1998/ht-1998-4-5.html /letöltés ideje: 2009.10.24./)

[3] Nemzetközi Hírközlési és Informatikai Tanács - Információs Társadalom Technológia Távlatai - Körkép 2007. Szeptember Október. – p. 1-25. (Forrás: http://www.nhit-it3.hu/it3-cd/IT3_korkep_07szept_okt.pdf /letöltés ideje: 2009.10.24./)

[4] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. – p. 1-22.
(Forrás:http://www.bm.hu/web/jog_terv.nsf/0/19659F03FD726909C12574C20034751C/$FILE/2080_2008_Korm-hat.pdf /letöltés ideje: 2009. 10.23./)

[5] Glatz Ferenc: Migráció a kibővített Európai Unióban. – p. 400-407. (Forrás: http://www.glatzferenc.hu/upload/file/Kotetek/5K-50.pdf /letöltés ideje: 2009.10.24./)

[6] Magyar Hadtudományi Társaság: Hadtudományi Lexikon I. kötet. Szabó József (főszerk.). – Budapest, 1995. – ISBN 963 04 5227 8

[7] Matus János: A biztonság és a védelem problémái a változó nemzetközi rendszerben. – In: Hadtudomány A Magyar Hadtudományi Társaság folyóirata, 2005. december, XV. évfolyam 4. szám (elektronikus). (Forrás: http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_24.html /letöltés ideje: 2009.10.24./)

[8] Fodor Péter: A NATO és energiabiztonság. – In: Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2009. szeptember, IV évfolyam 3. szám (elektronikus) – p. 168-179. (Forrás: http://www.hadmernok.hu/2009_3_fodor.pdf /letöltés ideje: 2009.10.31./)

[9] Biztonságpolitikai szemle Corvinus Külügyi és Kulturális Egyesület. – Corvinák. – 1. A biztonsági kihívások új felfogása. - Az új típusú biztonsági kihívások új elméleti keretben. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid=1 /letöltés ideje: 2009.10.24./)

[10] Dr. Nagy Károly: Energiabiztonsági központok. – In: Hadmérnök a ZMNE Bólyai János Katonai Műszaki Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2008. március, III. évfolyam 1. szám (elektronikus) – p. 165.-171. (Forrás: http://www.zmne.hu/hadmernok/archivum/2008/1/2008_1_nagy.pdf /letöltés ideje: 2009.10.24./)

[11] Biztonságpolitikai szemle Corvinus Külügyi és Kulturális Egyesület. – Corvinák. – 2. Új típusú biztonsági kihívások – Energiabiztonság. (Forrás: http://bizpol.playhold.hu/?module=corvinak&module_id=4&cid=19&scid=27 /letöltés ideje: 2009.10.24./)

[12] Dr. Zsuga János: Földgázszállítás – Powerpoint előadás – 2009. Budapest.

[13] World Nuclear Association – Three Mile Island Accident (2001 march). (Forrás: http://www.world-nuclear.org/info/inf36.html /letöltés ideje: 2009.10.29./)

[14] Körmendi Krisztina, Solymosi József: A villamosenergia termelés környezetre gyakorolt hatása, a szén-dioxid kibocsátással nem járó villamosenergia termelés lehetőségei és korlátai. – In: Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2009. szeptember, IV évfolyam 3. szám (elektronikus) – p. 11-127. (Forrás: http://www.hadmernok.hu/2009_3_kormendi.pdf /letöltés ideje: 2009.10.31./)

[15] Halász László, Hanka László, Vincze Árpád: A nukleáris erőművek negyedik generációjának és egy korszerűbb reprocesszálási eljárás jövőbeni alkalmazásának lehetősége a nukleáris hulladékok növekvő mennyiségének és elhelyezési problémájának tükrében. - Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2008. szeptember, III évfolyam 3. szám (elektronikus) – p. 25-48. (Forrás: http://www.hadmernok.hu/archivum/2008/3/2008_3_hanka.pdf /letöltés ideje: 2009.11.01./)

[16] Magyar UNESCO Bizottság – A fenntartható fejlődés fogalma, célkitűzése. (Forrás: http://www.unesco.hu/index.php?type=node&id=131 /letöltés ideje: 2009.10.27./)

[17] Kasza Anett: A napenergia és a szélenergia alkalmazásának lehetőségei hazánkban. – Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2009. június, IV évfolyam 2. szám (elektronikus) – p. 29-40. (Forrás: http://www.hadmernok.hu/2009_2_kasza.pdf /letöltés ideje: 2009.10.31./)

[18] Bakosné Diószegi Mónika: Hazai energiabiztonság növelésének lehetőségei. – Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2009. június, IV évfolyam 2. szám (elektronikus) – p. 5-18. (Forrás: http://www.hadmernok.hu/2009_2_bakosne.pdf /letöltés ideje: 2009.10.31./)

[19] Bakosné Diószegi Mónika, Solymosi József: Lágyszárú mezőgazdasági növényből előállított pellet vizsgálata, az energiabiztonság növelését szolgáló lehetőség szemszögéből. - Hadmérnök A ZMNE Bólyai János Hadtudományi Kar és a Katonai Műszaki Doktori Iskola On-Line Tudományos Kiadványa, 2008. szeptember, III évfolyam 3. szám (elektronikus) – p. 14-24. (Forrás: http://www.hadmernok.hu/archivum/2008/3/2008_3_dioszegi.pdf /letöltés ideje: 2009.11.01./)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Réger Béla
reger.bela@zmne.hu

A LOGISZTIKA ÉS AZ ELLÁTÁSI LÁNC IDŐSZERŰ KÉRDÉSEI NAPJAINKBAN

Absztrakt

A logisztika folyamatos fejlődése során több új elmélet és koncepció került be a köztudatba. Ezek többsége világosan megjeleníthető a katonai logisztika elméletében és gyakorlatában. Ennek ellenére az utóbbi évek során napvilágot látott elméleteket sok esetben helytelenül értelmezték, ami szükségessé teszi ezeknek az elméleteknek a rendszerezését, magyarázatát. Ezen elméletek közül a katonai logisztika számára meghatározó jelentőséggel bír az ellátási lánc modell helyes értelmezése, szerepének pontos meghatározása a logisztikai rendszerben. A cikk az ellátási lánc és a logisztika kapcsolatát mutatja be az utóbbi évtizedek vonatkozó elméleteinek elemzésével.

The continuous development of several new logistics theory and the concept has been introduced to the public. Most of these are clearly displayed on the theory and practice of military logistics. Nevertheless, in recent years have been published theories often misinterpreted, which makes it necessary to organize these theories, an explanation. Among these theories of military logistics for the decisive importance of the supply chain model is the correct interpretation of the role of a precise definition of the logistics system. The article in the supply chain and logistics shows the relationship in recent decades for the analysis of the theories.

Kulcsszavak: *Logisztika, ellátási lánc, támogatási lánc ~ logistics, supply chain, support chain*

BEVEZETÉS

A logisztika meghatározó változásokon megy át napjainkban. A korábban misztifikált ellátási lánc kezdi megtalálni helyét és szerepét a logisztikai rendszerben. A szakmai közvélemény egyetért abban, hogy az alapoktól újra kell értelmezni és egységes rendszerbe foglalni az eltérő elméleti megközelítést. Ennek a munkának az egyik meghatározó képviselője a brit logisztikai szakma.

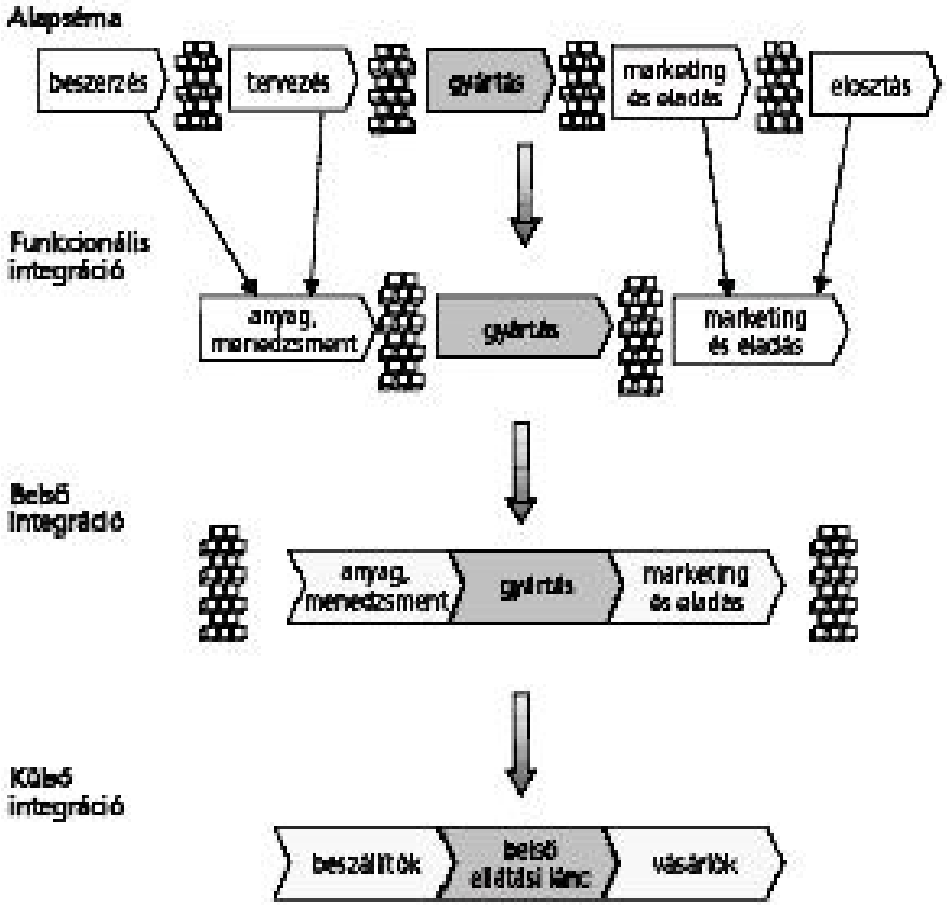
A LOGISZTIKA ÉS AZ ELLÁTÁSI LÁNC IDŐSZERŰ KÉRDÉSEI NAPJAINKBAN

A logisztika katonai gyökereit senki nem vitatja, amellett azonban tudnunk kell, hogy a kialakulás történetében meghatározóak a matematikai, filozófiai és a történelmi gyökerek is.

A folyamatos dinamikus fejlődés megtorpant, a 80-90-es évek céljait és feladatait újra kell értékelni a XXI. század első évtizedének a végén. A felkapott divatos ellátási lánc modell értelmezése véleményem szerint néha vakvágányra, tévútra vezetett.

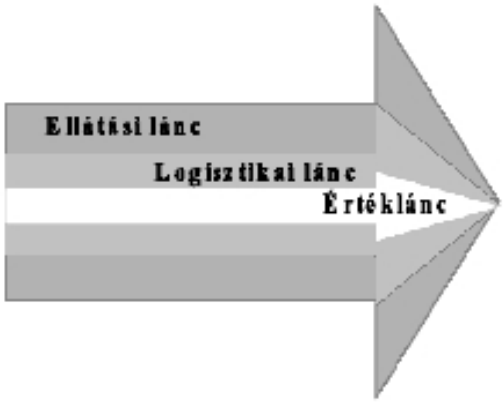
Mindenki egyetért Pfohl 1972 alapelméletével: „A logisztika tartalmaz minden olyan tevékenységet, amellyel egy hálózatban mozgásokat és tárolásokat alakítanak ki, irányítanak és szabályoznak, az együttes működés a hálózatban tárgyak és információk áramlását indítja meg úgy, hogy a teret és az időt minél eredményesebben hidalják át". Véleményem szerint ez a kiinduló pont.

Ugyancsak elfogadhatóak, az ábrán látható integrációs lépések:



1. ábra Az integráció lépései (Forrás: Gyakorlati logisztikai tanácsadói kézikönyv.)

Számomra már vitatható Dolgos Olga tanulmányában megjelent elmélet az ellátási lánc és a logisztika kapcsolatáról:



2. ábra Az értéklánc, a logisztikai lánc és az ellátási lánc egymásra hatása

Nem értek azzal egyet, hogy a logisztikát alárendelik az ellátási láncnak. Véleményem szerint nem foltozgatni kell a néha logikai hibákat is tartalmazó elméleteket, hanem rendszerszemléletű megközelítéssel újra kell építeni.

Az új Magyar Logisztikai Stratégia megfogalmazását figyelembe véve elfogadom ezt a megközelítést:

A logisztika az a szolgáltatás, amely biztosítja, hogy az üzleti folyamatok zavartalan lebonyolításához szükséges termékek a megfelelő helyen és időpontban, a szükségletnek megfelelő mennyiségben, minőségben és választékban rendelkezésre álljanak.

Értelmezzük részleteiben:

A logisztika az a szolgáltatás, (A logisztika, mint szolgáltatási támogató funkció jelenik meg a folyamatokban.) amely biztosítja, hogy az üzleti folyamatok zavartalan lebonyolításához szükséges termékek (A folyamatszervezés alapján támogatja az üzleti folyamatokat. Az üzleti folyamat megnevezés tágabban értelmezve lehet a gazdasági, műszaki és katonai folyamat is).

A következőkben az ún. „M” elveknek a „megfelelő” értelmezésben történik a felsorolása. Örvendetes, hogy nem az ún. „M-k” háborújában próbál minél többet összegyűjteni. Újszerű a logisztika fejlődésének folyamatában a választék megjelenése, ami már az ezredforduló utáni igények növekedésére utal:

a megfelelő helyen és

időpontban,

a szükségletnek megfelelő mennyiségben, minőségben

és választékban rendelkezésre álljanak.

A rendszerszemléletű megközelítéseknél a szakmai közvélemény egységesen elfogadja, hogy az alap vállalati rendszer fő logisztikai részei:

ellátási-;

termelési-;

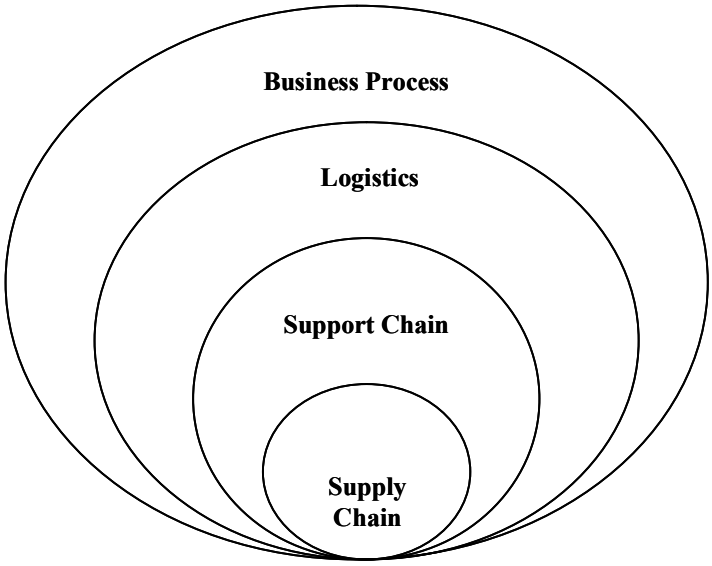
elosztási logisztika.

Így egyértelmű, hogy az ellátás a logisztika része. Sajnos azért napjainkban is akadnak olyan elméletek, hogy a logisztikának az integráló funkciójából egyes részeket próbálnak kiszakítani és önállóan értelmezni. Ilyen napjainkban a beszerzésnek a logisztikából való kiemelésének a kísérlete és külön értelmezése.

A szakma elfogadja, hogy a logisztikát alkotó modulok láncba, hálózatba szerveződhetnek akár az ellátáson keresztül. Frappáns idézett szerint:

„From your supplier's supplier to your customer's customer"

Szabad fordításban:" Az ellátód ellátójától a vevőd vevőjéig"



3. ábra Az ellátási lánc, a támogatási lánc, a logisztika és az üzleti folyamatok kapcsolata (Saját szerkesztés a brit támogatási lánc koncepció adaptációja alapján)

Értelmezzük az ellátási lánc belső és külső kapcsolatát.

Az **ellátási lánc** a logisztikai támogatási hálózat része, magába foglalja azokat az elveket és rendszabályokat és folyamatokat, amelyek az anyagi eszközöknek a kezdeti gazdasági forrás helyétől az igénylő felhasználóig és vissza való áramlást is megvalósítja.

Ebből az újszerű fogalomból látható, hogy alapvetően az anyagi eszközök áramlásáról beszélünk, de nem csak előre, hanem oda és vissza. Itt már jelentkezik az inverz logisztika

is. Tehát fontos, hogy az áramlás nem egyirányú, hanem kétirányú és alapvetően az anyagokra vonatkozik.

A logisztikai támogatási hálózat már egy nagyobb kategória. **A logisztikai támogatási hálózat a támogatási tevékenységek közül az a szolgáltatási tevékenység, amelyik megvalósítja a fizikai áramlási folyamatát az anyagoknak, személyeknek, szolgáltatásoknak és információknak.**

A fogalomból a következő következtetéseket lehet levonni.

- A logisztikai támogatási hálózat az anyagi folyamatokon túlmutató tágabb értelmezés.
- A polgári logisztika a bővített ellátási lánc értelmezéssel próbálta követni ezt a fejlődést.
- A támogatási hálózat egy meghatározott gráf típusú része lehet az ellátási lánc, amikor a hálózat meghatározott pontjai között a kijelölt útvonalakon áramolnak az anyagok.

Az ősszhaderőnemi ellátási lánc értelmezése

Az összhaderőnemi ellátási lánc a támogatási lánc azon eleme, amely tartalmazza azokat az irányelveket, egymáshoz kapcsolódó folyamatokat és tevékenységeket, melyekre szükség van a készletek átvételétől, azok mindhárom haderőnem igénylőihez való eljuttatásáig, valamint az inverz logisztikai folyamatok lebonyolításához. Az Összhaderőnemi Ellátási Lánc a stratégiai, hadműveleti és a harcászati szintű követelményeknek egyaránt meg kell, hogy feleljen.

Alapelvei:

I. Az ellátási folyamatokat szükségszerűen optimalizálni kell a végfelhasználók igényeinek kielégítése érdekében.

II. Az ellátásra vonatkozó tervek kidolgozását és végrehajtását a három haderőnem vonatkozásában integráltan kell kezelni;

III. Az ellátási feladatok végrehajtása során a veszteségeket minimálisra kell csökkenteni és kerülni kell a rugalmatlan és félreérthető megoldásokat.

A fent felsorolt alapelveknek megfelelően az összhaderőnemi ellátási lánc alapvetően a felhasználók igényeinek megfelelően (pull elv) lett kialakítva, az ellátási célok elérése érdekében a lánc minden eleme elszámoltatható és felelősségre vonható. A lánc vezetése és irányítása minden szinten integráltan történik. Az ellátási folyamatok szabványosítottak és egyszerűsítettek, melyek biztosítják a gyors anyagáramlást. Az utánpótlási ellátó és az inverz összhaderőnemi ellátási lánc egy rendszerben funkcionál.

Összefoglalás

A logisztika nem egy statikus tudomány, hanem dinamikus, amely állandóan az élet kihívásainak megfelelően fejlődik. Ebben a fejlődésben előfordulhatnak eltérő irányok is, amit a logisztikai szakmának kell helyes úton tartania, hogy a fő alapelvektől ne térjünk el. A mi feladatunk a rendszer (gazdasági, műszaki, katonai, stb.) folyamatos működőképességének fenntartása és biztosítása.

Irodalomjegyzék

1. Dr. Knoll Imre (2006) Interdiszciplináris logisztika a gazdaság-politikában. 2006 Kovásznai kiadó ISBN 963 85587 8 4

2. Hans Chrisztian Pfohl: Hálózatok együttműködésének alapjai. Logisztikai évkönyv 2007-2008

3. Tokodi Jenő: EU-konform logisztikai informatikai infrastruktúra kialakítása Előadás 2009 Heller Farkas Főiskola Logisztika szakirány

4. JSP 886 - Volume 01 - The Defence Logistics Support Chainhttp://www.mod.uk/DefenceInternet/MicroSite/DES/OurPublications/JSP886/Index.htm

5. Estók Sándor: (2009) Hálózatközpontú integrált interdiszciplináris logisztika

6. Estók Sándor: (2009) A nyerő hármas a Logisztika, Informatika és a Marketing. TRANZIT

7. Estók Sándor: (2007) Intelligens logisztika digitális környezetben. TRANZIT 2007. november

8. Estók Sándor: (2007) Lánc, lánc ellátási lánc TRANZIT 2007. szeptember

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Kozma Tibor
kozmatibor@yahoo.com

AZ EURÓPAI UNIÓ MŰVELETEINEK FINANSZÍROZÁSA

Absztrakt

Az Európai Unió műveletei a második pillért jelentő közös kül- és biztonságpolitika ernyője alá tartoznak, annak érdemi részét alkotják. Az ide sorolható műveletekkel kapcsolatban számos hazai és külföldi irodalom áll rendelkezésre, általánosan elmondható, hogy bőségesen akad forrás a tudományos kutatáshoz. Az irodalmi forrásbőség sajnos kevésbe igaz a műveletek pénzügyi kérdéseire. Megfelelő mértékű, és a kiadások felmerülésekor rendelkezésre álló pénzügyi eszközök, működő finanszírozási mechanizmusok nélkül egy civil vagy katonai műveletet még telepíteni sem lehetne, nemhogy megkezdeni. E téma fontossága ezért nem lehet kérdéses. A szerző nem kíván hiánypótló cikket jegyezni, inkább arra vállalkozik, hogy műveletek főbb pénzügyi kérdéseit áttekintő, egy szűkebb terjedelmi keretek között maradó irodalmat adjon az olvasónak.

The missions of the European Union fall under the umbrella of the second pillar; moreover they are the core element of the second pillar. Concerning these missions there are numerous available Hungarian and international literary works, indeed there are an abundance of sources for academic research. Unfortunately, there are far fewer sources that speak specifically to the financing element of EU missions. However, without adequate financial tools, available financial sources and a functioning financial mechanism, no civilian or military missions can be deployed or even launched. The importance of this subject is indisputable. It is not the author's intent to fill this gap, but to provide readers with a survey of the main issues involved in mission financing, to the greatest possible extent.

Kulcsszavak: *EU műveletek, közös kül- és biztonságpolitika (KKBP), civil műveletek, katonai műveletek, finanszírozás, ATHENA ~ EU missions, Common Foreign and Security Policy, civilian missions, military missions, financing, ATHENA*

BEVEZETÉS

A közös kül- és biztonságpolitika (KKBP) az Európai Unió második, kormányközi jelleggel működő pillérét jelenti. A KKBP-t az 1992-ben aláírt és 1993-ban hatályba lépett Maastrichti Szerződés hozta létre, majd az 1999-ben hatályba lépett Amszterdami Szerződés erősítette meg, innentől indult el a védelmi és a biztonsági oldal intézményesülése. Az intézményesülés alapvetően megindította a közös kül- és biztonságpolitika területén belül az európai biztonság- és védelempolitika (EBVP) létrejöttét, illetve megteremtette az alapokat a dinamikus fejlődéséhez. Az intézményesített közös kül- és biztonságpolitika alapjainak lerakása mellett elindult a közös védelem irányába mutató európai védelmi együttműködés folyamata, későbbikben a képességek fejlesztése is. Számos stratégia jelentőségű politikai eseményhez lehet kötni azt a folyamatot, amely során lefektették az EBVP alapelveit. Egyértelműen elkülönítették a kollektív védelmi és a válságkezelési feladatokat, azokat az úgynevezett petersbergi feladatkörbe sorolták, ezek: a válságkezelési, megelőzési, béketeremtő, humanitárius és evakuációs jellegű feladatok. A 2003-as év során elfogadott Európai Biztonsági Stratégiával megjelentek az új típusú petersbergi feladatok: közös lefegyverzési műveletek; harmadik államok terrorizmus-ellenes erőfeszítéseinek támogatása; a biztonsági szektor reformjára irányuló műveletek. Az EBVP műveleti képességek területén a feladatok jellege alapján megjelent a polgári válságkezelési szakterület és a katonai vagy védelmi vonatkozású műveleti kör. A Lisszaboni Szerződés azon túl, hogy létrehozta az önálló jogi személyiséggel rendelkező Európai Uniót, ami megnövelheti a KKBP jövőbeli kompetenciáját, számos változást hozott intézményi, szervezeti, irányítási szinten is. A közös biztonság- és védelempolitika (KBVP) pontos tartalmát a Lisszaboni Szerződés 42. cikke adja meg: [1]

„(1) A közös biztonság- és védelempolitika a közös kül- és biztonságpolitika szerves része. E politika polgári és katonai eszközök igénybevételével biztosítja az Unió műveleti képességét. Az Unió ezeket az eszközöket az Egyesült Nemzetek Alapokmányának alapelveivel összhangban igénybe veheti az Unión kívüli békefenntartó, konfliktusmegelőző és a nemzetközi biztonságot erősítő missziókban. E feladatok végrehajtása a tagállamok által rendelkezésre bocsátott képességeken alapul.”

A KÖZÖS KÜL- ÉS BIZTONSÁGPOLITIKA, MŰVELETEK

A közös kül- és biztonságpolitika elsődleges célkitűzései:

- az Unió közös értékeinek, alapvető érdekeinek, függetlenségének és integritásának védelme;
- az Unió biztonságának megerősítése; a béke megőrzése és a nemzetközi biztonság megerősítése; a nemzetközi együttműködés előmozdítása;
- a demokrácia és a jogállamiság fejlesztése és megerősítése;
- az emberi jogok és az alapvető szabadságok tiszteletben tartása.

A Lisszaboni Szerződés ugyanakkor pontosan nevesíti azokat a műveleti fajtákat, amelyek végrehajtása során az Unió polgári és katonai eszközöket vehet igénybe. [2] Ezek:

- közös leszerelési műveletek,
- humanitárius és mentési feladatok,
- konfliktus megelőzés,
- békefenntartás,
- harcoló erők válságkezelésben kifejtett feladatai.

Az első EBVP művelet az EU Rendőri Misszió (EUPM) a korábbi Bosznia-Hercegovina ENSZ IPTF műveletének az átvételét, pontosabban fogalmazva más típusú folytatást jelentette 2003.01.01-el. A cikk szerzőjeként egy mondat erejéig szeretnék arra kitérni, hogy én voltam az első magyar hivatásos állományú rendőrtiszt, aki a legelső EBVP műveletbe vezényeltként megkezdte külszolgálatát. Az első polgári műveletet hónapokon belül követte az első katonai vagy védelmi vonatkozású körbe sorolható, rövid ideig tartó katonai művelet: a Concordia (FYROM) Macedónia területén. Jelen dolgozatnak nem célja a korábbi és a jelenleg is tartó műveletek részletes bemutatása, ezért elsősorban a statisztikai adatokra támaszkodva, annyit érdemes megjegyezni, hogy összesen 24 műveletet indított el az EU az elmúlt 8 év során, ebből 10 műveletet befejezett. Jelenleg három kontinensen összesen 14 műveletet tart fenn az EU, amit a következő bontásban szeretnék szemléltetni.

Polgári műveletek: [3]

- EUPM, Bosznia-Hercegovina, kezdete: 2003, létszáma: 280
- EUJUST LEX, Irak, illetve Brüsszel, kezdete: 2005, létszáma: 42
- EUBAM Rafah, Rafah határátkelőhely, kezdete: 2005, létszáma: 22
- EUPOL COPPS, Palesztin területek, kezdete: 2006, létszáma: 83
- EUPOL Afghanistan, kezdete: 2007, létszáma: 445
- EUPOL RD CONGO, kezdete: 2007, létszáma: 57
- EULEX Kosovo, kezdete: 2008, létszám: 2504
- EUMM Georgia, kezdete: 2008, létszáma: 403
- *EUBAM Moldova-Ukraine, kezdete: 2005, létszáma: 200*

Az EUBAM határellenőrző misszió jellegét, mandátumát tekintve egyértelműen polgári művelet. A finanszírozását tekintve eltér az itt szereplő többi művelettől, ugyanis nem a KKBP pénzügyi forrásait veszi igénybe. Az egyedi, atipikus finanszírozási mechanizmusa miatt röviden annyit jegyeznék meg, hogy a pénzügyi forrásbiztosítás, illetve a művelet feletti politikai kontroll révén is közvetlenül a Bizottsághoz tartozik. [4]

Katonai és polgári műveltek: [5]

- EUSEC RD CONGO, kezdete: 2005, létszáma: 43
- EUSSR Guinea-Bissau, kezdete: 2008, létszáma: 33

A fenti két művelet összetett képet mutat, mivel a mandátumból adódóan katonai és a polgári képességek együttes megjelenítését kellett egy műveletben ötvözni, ezért az állomány elsősorban katonai és rendvédelmi szakemberekből áll, ugyanakkor mindkét művelet esetében katonai vezető került kinevezésre. A művelet jellegére vonatkozóan pontos választ kapunk amennyiben a művelet finanszírozását vizsgáljuk, ami az EU költségvetését terheli, illetve a civil jellegre utal az a tény is, hogy a művelet vetője Head of Mission (civil terminológia) és nem Force Commander (katonai terminológia).

Katonai műveltek: [6]

- EUFOR ALTHEA, Bosznia-Hercegovina, kezdete: 2008, létszáma: 1926
- EUTM Somalia, kezdete: 2008, létszáma: 100
- EUNAVFOR, kezdete: 2010, létszáma: 1518

A POLGÁRI MŰVELETEK FINANSZÍROZÁSA

A következőkben, két külön fejezetben kerül tárgyalásra a polgári és a védelmi vagy katonai jellegű műveletek finanszírozásának a bemutatása. Ennek az oka elsődlegesen az, hogy teljesen eltér a két művelettípus finanszírozási mechanizmusa, illetve más forrásokra

támaszkodik. Az Európai Unióról szóló szerződés 28. cikke alapján a KKBP működésével kapcsolatban felmerülő kiadások az Európai Unió költségvetését terhelik, kivéve a katonai vagy védelmi vonatkozású műveletekből eredő kiadások körét. Azokban az esetekben, amikor a kiadások nem az Unió költségvetését terhelik, azok a bruttó nemzeti jövedelem-kulcs (GNI alap) szerint a tagállamokat terhelik, kivéve, ha a Tanács egyhangúlag másként határoz.

A finanszírozás általános jellemzői

A továbbiakban a finanszírozási kérdéskör pontos bemutatása érdekében – a szükséges mértékben – ki kell térni az Európai Unió költségvetésére is, elsősorban a költségvetést jellemző alapelvek bemutatása indokolt: [7]

- Az egységesség elve. 1968-ig öt különböző és egymástól független, önálló költségvetés létezett, jellemezően 1993-tól van egységes költségvetése az Uniónak, ami egy dokumentumban tartalmazza az összes pénzügyi műveletet kiadások és bevételek vonatkozásában.
- A bruttó költségvetés elve. Másképpen a teljesség elve, ami azt jelenti, hogy nem lehet a költségvetési bevételeket előre meghatározott kiadásokhoz kötni, másrészt, a bevételeket és a kiadásokat nem lehet egymással szemben beszámítani.
- Éves költségvetés elve. A költségvetést pontosan 1 éves időszakra kell meghatározni, ugyanakkor az éves költségvetés mellett létezik egy középtávú költségvetési periódus is, ami 7 évet fog át. A jelenlegi ilyen periódus 2007 – 2013 közötti időszak vonatkozásában határozza meg a sarokszámokat.
- Részletesség elve. A költségvetési előirányzatok megfelelő mélységi bontását írja elő.
- Költségvetési egyensúly elve. A költségvetés nem tartalmazhat sem hiányt, sem többletet, ezért nincs hitel felvételére sem lehetőség. Minden kiadást bevétellel kell fedezni.
- A gondos pénzgazdálkodás elve. A költségvetési források optimális felhasználását jelenti.
- A nyilvánosság elve. A költségvetés a Közösségek Hivatalos Lapjában az elfogadástól számított 3 hónapon belül közzé kell tenni.

2. A KKBP költségvetése

Az Unió költségvetésének negyedik fejezetébe: „Az EU mint globális partner” címszó alá sorolták számos más szakterület mellett a közös biztonság- és védelem politikát, valamint a humanitárius segítségnyújtást. A Bizottság javaslatára a Tanács és az Európai Parlament egyetértésével kerül meghatározásra a KKBP éves költségvetési kerete.

A közös kül- és biztonságpolitika 2007 – 2013 keretidőszakára előirányzott finanszírozási főösszege – az EU globális szerepének erősítése érdekében - 2 milliárd eurót tesz ki. [8]
Ez átlagosan éves bontásban mintegy 290 millió eurós összeget jelent. Ugyanakkor a pénzügyi politika tervezői a 2007 – 2013-as időszak vonatkozásában dinamikus kiadás növekedést prognosztizáltak. A következő táblázat a 7 évre vonatkozó éves főösszeg változását mutatja be. [9]

	2007.év	2008.év	2009.év	2010.év	2011.év	2012.év	2013.év
KKBP	159	285	243	281	327	363	406

(A feltüntetett összegek millió euróban szerepelnek)

Az KKBP pénzügyi kiadásainak központi könyvelésére hét alfejezet áll rendelkezésre. Az egyes polgári műveletek éves finanszírozása - művelet jellegétől függően - három különböző alfejezetben történik, a következő bontásban:

1. Könyvelési kód: 19.0301. – A béke és a biztonság nyomon követése és megvalósítása.
   Ide tartozik: EUMM Georgia, EUBAM Rafah.
   A műveletek jellege: monitoring and border control missions.
2. Könyvelési kód: 19.0303. – Konfliktusrendezési és egyéb stabilizációs intézkedések.
   Ide tartozik: EULEX Kosovo, EUSEC RD Congo, EUJUST LEX Iraq.
   A műveletek jellege: rule-of-law missions.
3. Könyvelési kód: 19.0307. – Rendfenntartó missziók.
   Ide tartozik: EUSSR Guinea-Bissau, EUPOL COPPS, EUPOL RD Congo, EUPOL Afghanistan, EUPM BiH.
   A műveletek jellege: police missions.

A KKBP 2008. éves kiadási főösszege és a következő pontban bemutatásra kerülő műveletek összesített kiadási összege közötti különbség abból adódik, hogy a KKBP a műveleteken túl, más, a műveletektől eltérő kiadási köröket is finanszíroz, nevezetesen:

- 19.0302. Non-ploriferáció és leszerelés,
- 19.0304. Szükséghelyzeti intézkedések,
- 19.0305. Előkészítő és nyomon követő intézkedések,
- 19.0306. Az Európai Unió különleges képviselői.

3. A civil műveletek finanszírozási igénye

Az egyes műveletek 2008-as költségvetési kiadásait a következő táblázat mutatja be: [10]

MŰVELET (MISSZIÓ)	Éves kiadások euróban
EUPM BiH	**5 838 560**
EUJUST LEX	**7 200 000**
EUBAM Rafah	**2 500 000**
EUPOL COPPS	**6 000 000**
EUPOL Afghanistan	**45 000 000**
EUPOL RD CONGO	**6 920 000**
EULEX KOSOVO	**120 000 000**
EUMM Georgia	**37 070 000***
EUSEC RD CONGO	**8 450 000**
EUSSR Guinea-Bissau	**5 650 000**
ÖSSZESÍTETT KIADÁS:	**244 658 560**

Az EU éves költségvetésének jóváhagyása után a Bizottság felügyeli a leosztott pénzügyi források felhasználását. Az egyes civil műveletek vezetői szerződéses jogviszonyba kerülnek a Bizottsággal, amelynek egyik lényeges eleme, hogy az adott művelet szakmai vezetésén túl, felelősek a rendelkezésre bocsátott pénzeszközök jogszerű és optimális felhasználásáért. A műveletek pénzügyi gazdálkodása szigorú elszámolási rendszer keretében történik, minden művelet egyik kiemelt szervezeti eleme a pénzügyi szakterület.

4. A civil művelet megkezdését megelőző előkészítési fázis finanszírozása

Az EUMM Grúzia művelet megindítását független tényfeltáró művelet előzte meg, amihez további előkészítő műveleti költség is kapcsolódott, ami együttesen 2.07 millió eurós költséget jelentett. Az EUMM éves működési forrásigénye (35 millió euró) és a fenti (előkészítő, tényfeltáró) költségek összesítve szerepelnek a táblázatban. Az EUMM művelet stratégiai tervezése során a Bizottság 2008.08.02-án meghozott általános elvi érvényű döntése alapján egy adott művelet előkészítése (pontos definiálva, hogy milyen természetű költség számolható itt el) is a KKBP költségvetését terheli. A döntés értelmében már az elfogadott mandátum előtt meg lehet tenni a műveletet előkészítő tényleges érdemi lépéseket, így a művelet a mandátum megnyílásának első napjától kezdve hatékonyan tud funkcionálni (pénzügyi szempontból).
2001 – 2007 során az RRM (Rapid Reaction Mechanism) segítette a dinamikusan fejlődő műveletek kezdeti finanszírozását, mintegy előfinanszírozó mechanizmus működött. Számos kötöttsége miatt a 2006 során jelentős változások érintették az RRM mechanizmust is, elvetették és helyette hozták létre az IfS (Instrument for Stability) rendszert. Az IfS rugalmassága (6 hónapos időkeretről 18 hónaposra nőtt a felhasználási időkeret, megemelték a korábbi 30 milliós keretet, a pénzeszközök lehívása könnyebbé vált) jelentősen megnövelte a Bizottság pénzügyi mozgásterét válságkezelési kérdésekben.

5. Civil művelet során felmerülő (sürgős) finanszírozás problémák megoldása

Amennyiben nem elégséges a tervezett és jóváhagyott pénzügyi forrás egy adott művelet vonatkozásában a KKBP rendszertől független két pénzügyi alap segíthet: az EAR (Emergency Aid Reserve) illetve az FI (Flexibilty Instrument). Az EAR rendszer EU-n kívüli műveletek/rendkívüli események azonnali finanszírozhatósága érdekében a 2007-2013-as keretidőszakra összesen 1.75 milliárd eurót tart fenn. A 2008-as év során a KKBP költségvetését jelentősen megterhelő két „induló" civil műveletet kellett finanszírozni: EUMM, és EULEX Kosovo. Az EULEX 2008-as pénzügyi év alatt felmerülő többletfinanszírozási igényének gyors biztosítása érdekében az FI forrásból lehívásra került 70 millió euró, ami a pénzügyi év elszámolása során végül a KKBP keret terhére lett elkönyvelve. Magyarul a hirtelen felmerült finanszírozási igényre az FI biztosította - átmenetileg - a gyors pénzügyi fedezetet. [11] Mindkét KKBP keretein kívüli pénzügyi alap esetében a felhasználásról a Bizottság dönthet, azonban szükséges a Tanács és az Európai Parlament jóváhagyása is. A Bizottság egy további lehetősége, hogy pénzeszközöket csoportosíthat át a KKBP (négyes főkiadási csoport) finanszírozási keretéből az egyes alfejezeteken belül.

A Lisszaboni Szerződés beemelt egy új elemet a finanszírozási körbe. Nevezetesen felhatalmazza a Tanácsot, hogy konzultálva az Európai Parlamenttel, határozzon külön eljárásokról, amelyek egy adott művelet sürgős megindítása érdekében a sürgős finanszírozást lehetővé teszik, a megfelelő pénzügyi előirányzatokhoz való gyors hozzáférés révén. [12]
Ez azt jelenti, hogy a korábban elvárásként megfogalmazott gyors műveleti képesség mellé most párosították a sürgős finanszírozási képesség megteremtését. Ez jelentős előrelépés, ami érdemben csökkentheti egy művelet során a pénzügy alapokhoz való hozzáférés idejét.

A VÉDELMI VAGY KATONAI MŰVELETEK FINANSZÍROZÁSA

A katonai eszközöket igénylő műveletek során az Unió elsősorban a tagállamok által rendelkezésre bocsátott katonai eszközöket és katonai képességeket veszi igénybe. A katonai vagy védelmi műveletek költségeit két egymástól gyökeresen eltérő elv, illetve működési mechanizmus szerint finanszírozzák. Egyrészt az Unió a meghatározott közös költségek esetkörében az „ATHENA" [13] nevű finanszírozási igazgatási mechanizmust alkalmazza. A katonai vagy védelmi műveletek azon körében, amelyek nem esnek az ATHENA által finanszírozott kategóriába a következő elv érvényesül: akinél a költségek elsődlegesen jelentkeznek, az állja azokat. Másképpen fogalmazva ez azt jelenti, hogy az a pénzügyi kihatású műveleti tevékenység, ami nem került be az ATHENA rendszer finanszírozási körébe, azt az érintett tagállam (esetleg harmadik állam) a saját védelmi költségvetése terhére finanszírozza, és nem kérheti az ATHENA rendszertől a finanszírozás átvállalását. Jellemzően a tagállamokat, illetve résztvevő államokat terheli a devizaellátmány, a kitelepítés, a visszatelepülés, az állomány étkezési és szállás költségei. Érdekes módón ez a kiadási kategória adhatja a műveletek teljes pénzügyi finanszírozási igényének akár a 80-90%-át is. Például a 2008-as év során az EUFOR Tchad/CAR művelet esetében az ATHENA megközelítőleg 120 milliós keretet finanszírozott, míg egyes becslések szerint a művelet összkiadása megközelítőleg 1 milliárd euró volt! [14]

1. Az ATHENA rendszer főbb jellemzői

A Tanács eseti alapon határoz arról, hogy a tervezett művelet katonai vagy védelmi jellegű, ez azt jelenti, hogy a Tanács döntése alapján kerül a művelet a KKPB vagy az ATHENA finanszírozási keretébe.

Az ATHENA szabályozása szerint a katonai vagy védelmi jellegű műveletek előfinanszírozása kiemelten fontos, ezzel a gyorsreagálású műveleteknek is megfelelő, gyors finanszírozási keretet teremt. A műveletek finanszírozásának igazgatása céljából, a szükséges mértékben az ATHENA rendszer jogi személyként jog- és cselekvőképes, tehát bankszámlát nyithat, pénzügyeket kezelhet, szerződéseket köthet, stb..

Érdekes megjegyezni, hogy az ATHENA rendszerben résztvevő államok maguk a tagállamok, kivéve Dániát (Dánia saját döntése értelmében nem vesz részt az EU védelmi vonatkozású határozatainak meghozatalában, végrehajtásában.) Az ATHENA ismeri a hozzájáruló államok kategóriáját is, amelyek lehetnek az érintett katonai művelet finanszírozásában résztvevő tagállamok, illetve további harmadik államok. [15]

Az ATHENA éves időkeretben megadott külön költségvetéssel rendelkezik, amely teljes mértékben megállapítja a bevételek és a kiadások körét. A korábban bemutatott költségvetési alapelvek a megfelelő kontextusban itt is érvényesülnek, pl: valamennyi kiadást egy meghatározott művelethez kell rendelni.

Az előkészítő tevékenységek finanszírozásáról a Lisszaboni Szerződés a következő képen rendelkezik: meghatározza, hogy a katonai vagy védelmi műveleteket előkészítő azon tevékenységek finanszírozására, amelyek nem az Unió költségvetését terhelik, a tagállamok hozzájárulásaiból egy induló alapot kell létrehozni. A Tanács az Unió külügyi és biztonságpolitikai főképviselőjének javaslata alapján, minősített többséggel elfogadott határozatban meghatározza: [16]

a) az induló alap létrehozására és finanszírozására vonatkozó szabályokat, így különösen az alap rendelkezésére bocsátott pénzeszközök összegét.
b) az induló alap kezelésére vonatkozó szabályokat.
c) a pénzügyi ellenőrzésre vonatkozó szabályokat.

Ennek megfelelően az ATEHNA költségvetésének Általános része (General Part) tartalmaz egy művelet előkészítésére elkülönített előirányzatot (Preparatory phase of an operation), ami 2010. évben 820 000 EUR.

2. Az ATHENA szervezeti felépítése, funkciók és feladatok szerint felosztása

Az ATHENA szerkezete, szervezeti felépítése összetett, a következő bontás mutatja be: [17]

- Egy különbizottság az igazgatását felügyelő szerv, amely a tagállamok egy-egy képviselőjéből áll. Ez a különbizottság széles körű jogosítványokat gyakorol, többek között jóváhagyja a műveleti költségvetéseket.
- Az ügyvezető, aki döntések előkészítésében, és általában az ATHENA működéséhez kapcsolódó adminisztratív feladatok ellátásában vesz részt, beleértve a különbizottság által hozott határozatok végrehajtását is.
- A műveleti parancsnok az általa vezetett művelet vonatkozásában engedélyezésre jogosult tisztviselő, az ATHENA nevében szerződéseket köthet, kifizetéseket engedélyezhet, bankszámlát nyithat, stb..
- Számvitelért felelős tisztviselőt a Tanács főtitkára nevezi ki. Felelősségi körébe tartozik a kifizetések megfelelő végrehajtása, a bevételek beszedése, az ATHENA éves elszámolásának az elkészítése, az egyes műveletekre vonatkozó éves beszámolók elkészítése, folyamatos könyvvezetés, stb..

3. Az ATHENA által finanszírozott közös költségek köre, a kiadási oldal

A Tanács 2008/975/KKBP határozata (2008.12.18) amely az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusáról szól, összesen 4 mellékletet tartalmaz. Ezen mellékletek válaszolják meg azt a kérdést, hogy milyen költségeket lehet az ATHENA rendszeren keresztül elszámoltatni. [18]
Az I. Melléklet arról rendelkezik, hogy milyen költségek esnek az ATHENA által viselt közös költségek alá függetlenül a keletkezésük időpontjától. Ezek elsősorban:

1. Kiküldetési költségek.
2. Kártérítések kifizetése.
3. Anyagok tárolási költségei.
4. Banki költségek.
5. Ellenőrzési költségek.
6. A II. Mellékletben szereplő tevékenységek előkészületi költségei.

- A II. Melléklet a műveletek előkészületi szakaszára vonatkozó, az ATHENA által viselt működési közös költségek körét adja meg.
    1. Katonai erők által végzett felderítő küldetések, műveleti előkészületek költségei.
    2. A művelethez kapcsolódó orvosi szolgáltatások.
- A III. Mellékelt a minden esetben az ATHENA által viselt, a műveletek aktív szakaszára vonatkozó működési közös költségek. A Melléklet felsorolása hosszú, a lényegre törekedve a következő fontos elemeket érdemes kiemelni:
    1. Az EU által vezetett műveleti parancsnokságok működési kiadásai, beleértve a Parancsnokságot, a Műveleti Parancsnokságot, az Erők Parancsnokságát, a Komponens Parancsnokságokat.
    2. A jelentkező szállítási költségek, igazgatási költségek, az egyes műveleti parancsnokságokon foglalkoztatott civilek alkalmazási költségei, hírközlő, informatikai és felszerelések beszerzése, üzemeltetési költségeik, műveleti területen belüli utazások, napidíjak, lakatanyák és szállásinfrastruktúra költségei, a nyilvánosság tájékoztatási költségei, reprezentációs költségek.

3. A bevetési erők műveleti telepítése, alkalmazása során jelentkező költségek, pl: telepítéssel, infrastruktúrával kapcsolatos költségek, azonosító jelzés, orvosi szolgáltatások, információszerzés költségei.
4. Közös NATO eszközöknek és kapacitásoknak az EU általi igénybevételéből származó többletköltségek.
5. Harmadik állam, illetve nemzetközi szervezet által – szerződés alapján – biztosított, a művelethez kapcsolódó költségek.

- A IV. Melléklet az ATHENA-t terhelő, valamely művelet befejezésére vonatkozó működési közös költségek.

Egy kiegészítés a fenti mellékletekhez: nevezetesen az EU gyakorlatainak közös költségeit az ATHENA rendszeren keresztül kell finanszírozni, a korábban bemutatott kiadási körök képezhetik a közös kiadások jogalapját.

4. Az ATHENA rendszer bevételi oldala

A folyamatban lévő, vagy tervezett műveletek működési közös költségeinek a megtérítése érdekében előirányzat tünteti fel a szükséges bevétel mértékét. A bevételek két forrásra támaszkodnak. Elsősorban a résztvevő és hozzájáruló tagállamok, valamint – adott esetben a műveletekhez hozzájáruló – harmadik államok által fizetendő hozzájárulások. [19] Kiegészítő mértékben egyéb bevételek, például: kamatbevételek, eladásból befolyt ellenértékek is a bevételi oldalt növelik. Ez azt jelenti, hogy lényegében az ATHENA rendszert a tagállamok védelmi költségvetései tartják fenn. Az egyes tagállami hozzájárulások mértéke évente változik, jellemzően a bruttó nemzeti jövedelem kulccsal, illetve a 2000/597/EK tanácsi határozattal összhangban kell minden évben meghatározni. (A GNI kulcs alapján a 2010-es pénzügyi évben a magyar hozzájárulás kevesebb, mint 0,727006%-át teszi ki az ATHENA teljes keretének.)

ÖSSZEGZETT MEGÁLLAPÍTÁSOK

Az Európai Unió második pillérébe sorolt KKBP műveleti elemit jelentő civil és katonai műveletek története csupán 8 évet fog át. Ennek ellenére az Unió egyik sikertörténetének lehet tekinteni, hiszen számos földrajzi térségben sikerült hozzájárulni a béke és a stabilitás megteremtéséhez, illetve a jelenleg is folyamatban lévő 14 művelet keretében három földrészen van jelen az „Unió csillagos zászlója”. A kérdést finanszírozási oldalról megközelítve látható, hogy hatalmas háttérmunkát igényelt és igényel ma is a civil, és katonai műveletek indítása, fenntartása. Elsőként ki kellett alakítani a műveletek finanszírozásának az alapelveit, majd az első műveletek elindítása, fenntartása során nyert tapasztalatokat be kellett építeni a bemutatott finanszírozási mechanizmusok rendszerébe. A tapasztalt kezdeti nehézségek legyőzése után mára kialakult egy átfogó és műveleti specialitásokra, mint például sürgős telepítési igény, előfinanszírozás, stb.. is érzékeny, azokat kezelni tudó rendszer. Ez persze közel sem jelenti azt, hogy egy végleges és kiforrott finanszírozási mechanizmus alakult ki, sokkal inkább úgy érdemes erre most tekinteni, mint egy működőképességében a gyakorlati tapasztalatok révén feljavított komplex rendszer, ami a közeljövőben is dinamikus képet fog mutatni. Egy, a mai napig megoldatlan problémával szemléltetve ezt a kijelentést, indokoltnak tűnik olyan mechanizmusok beépítése a mostani rendszerbe, amelyek lehetővé tennék egy integrált civil – katonai művelet integrált pénzügyi finanszírozását. Ez a kérdés, és számos más finanszírozási dilemma megoldása továbbra is az EU előtt áll.

HIVATKOZÁSOK

[1] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (Lisszaboni Szerződés) megjelent az Európai Unió Hivatalos Lapjában a C115/13 oldaltól (2008.05.09) 28. cikk.

[2] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (Lisszaboni Szerződés) megjelent az Európai Unió Hivatalos Lapjában a C115/13 oldaltól (2008.05.09) 28. cikk. b) pont.

[3] Forrás: http://www.consilium.europa.eu/showPage.aspx?id=268&lang=HU, letöltés 2010.06.07.

[4] Memorandum of Understanding between the EU Commission, the Gouvernment of the Republic of Moldova and the Gouvernment of Ukraine on the European Commission Border Assistance Mission to the Republic of Moldova and to Ukraine.

[5] Forrás: http://www.consilium.europa.eu/showPage.aspx?id=268&lang=HU, letöltés 2010.06.07.

[6] Forrás: http://www.consilium.europa.eu/showPage.aspx?id=268&lang=HU, letöltés 2010.06.07.

[7] Iván Gábor: Bevezetés az Európai Unió költségvetésébe, Osiris Kiadó, 2008, Bp.

[8] Institute for Security Studies: European Security and Defence Policy, The first 10 years (1999 – 2009) 90. oldal

[9] The European Commission, 'Financial programming 2007-2013' 2009

[10] 2008. A Tanács éves jelentése az Európai Parlamentnek a KKBP fő szempontjairól és alapvető választásairól, Belgium, 2009, ISBN: 978-92-824-2442-1, III. Melléklet.

[11] Institute for Security Studies: European Security and Defence Policy, The first 10 years (1999 – 2009) 94. oldal

[12] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (Lisszaboni Szerződés), megjelent az Európai Unió Hivatalos Lapjában a C115/13 oldaltól (2008.05.09) 28. cikk

[13] Tanács 2004.02.23-án elfogadott 2004/197/KKBP határozata az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusának (ATHENA) létrehozásáról. A többször módosított ATHENA mechanizmust egységes szerkezetbe foglalta a Tanács 2008/975/KKBP határozata (2008.12.18)

[14] Institute for Security Studies: European Security and Defence Policy, The first 10 years (1999 – 2009) 76. oldal

[15] A Tanács 2008/975/KKBP határozata (2008.12.18) az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusának (ATHENA) létrehozásáról. 1 Fejezet.

[16] Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata (Lisszaboni Szerződés), megjelent az Európai Unió Hivatalos Lapjában a C115/13 oldaltól (2008.05.09) 28. cikk

[17] A Tanács 2008/975/KKBP határozata (2008.12.18) az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusának (ATHENA) létrehozásáról. 2 Fejezet.

[18] A Tanács 2008/975/KKBP határozata (2008.12.18) az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusának (ATHENA) létrehozásáról. I.-IV. Mellékletek

[19] A Tanács 2008/975/KKBP határozata (2008.12.18) az Európai Unió katonai vagy védelmi vonatkozású műveletei közös költségei finanszírozása igazgatási mechanizmusának (ATHENA) létrehozásáról. 6 Fejezet.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Illési Zsolt
illesi.zsolt@proteus.hu

Varga Péter
varga.peter@kvk.uni-obuda.hu

WARDRIVING ÉS A TÉRINFORMATIKA

Absztrakt

A technika fejlődésével nő a mobilitás iránti vágyunk. Ennek egyik lehetséges megvalósítása ha olyan munkahelyeket, szórakozó helyeket és lakhelyeket alakítunk ki, ahol mobil eszközeinkkel tudjuk végezni mindennapi tevékenységeinket. A rádiós hálózatok ilyen megoldást nyújtanak. A cikkben bemutatjuk a rádiós hálózatokra irányuló főbb támadási módszereket és a védekezés egyfajta megközelítését, amely maga a felderítés. Ennek a megelőző felderítési módszernek a főbb eszközei a wardriving és a térinformatika.

With technology development increases our desire toward mobility. One possible solution if we develop workplaces, pleasure-grounds, and homes where it is possible to deal with everyday routines with mobile devices. Radio networks provide appropriate solutions to mobility needs but also raise new vulnerabilities and threats. In this paper we summarize the main attack methods which are targeting radio networks, and we also present one possible way of defence, the Wi-Fi enumeration supported with geographic information application. The main tools for this preventive enumeration are wardriving and GIS.

Kulcsszavak: *AP, GPS, GIS, wardriving, Wi-Fi, térinformatika*

BEVEZETÉS

Az információs és kommunikációs technológia (ICT) fejlődése és egyre szélesebb térnyerése új technológiai trendet hozott hétköznapjainkba, mely középpontjában a mobilitás áll. Ezt úgy tudjuk elérni, ha informatikai rendszereinket vezeték nélküli hálózati szegmenssel látjuk el. Ez a trend egyre jobban megfigyelhető a vállalatoknál, infrastruktúra üzemeltetőknél és a magán szférában is. A komplex rendszerek elterjedésével nő az azokkal kapcsolatos támadások száma is. A támadók legtöbbször nem saját hálózatukat használják, hanem egy kiválasztott, általában gyengén védett hozzáférési ponthoz (Access Point, AP) csatlakoznak. Ezt azért tudják megtenni, mert felmérések szerint az AP-ok 60%-a nem rendelkezik megfelelő

biztonsági beállításokkal. A cikkben a vezeték nélküli hálózat (Wi-Fi) elleni támadások közül a wardriving és a térinformatika kapcsolatát mutatjuk be.

Célkitűzéseink között szerepel, hogy rámutassunk arra, hogyan fordíthatjuk a wardrivingot mint felderítési formát saját hálózatunk védelmére.

WLAN HÁLÓZATOK, FENYEGETÉSEK

A vezeték nélküli hálózat (Wi-Fi) egyik fő komponense a hozzáférési pont (Wireless Access Point, WAP) amely egy olyan kommunikációs eszközt jelent, amely mások számára elérhetővé teszi a Wi-Fi hálózat használatát, ezek rendszerint a Wi-Fi és a kábeles hálózatot összekötő útválasztók. A másik fő komponens a Wi-Fi berendezés, amely olyan eszköz, ami képes a Wi-Fi hálózaton keresztül kommunikálni. Wi-Fi hálózat létrejöhet hozzáférési pont(ok) között; hozzáférési pont és Wi-Fi berendezés(ek) között, és Wi-Fi berendezések között közvetlenül. [1]

A vezeték nélküli hálózatokat és állomásokat többféle támadás érhet. Ezen támadások közül a legnépszerűbbek külön nevet is kaptak.

Wardriving

A wardriving során a támadó célja, hogy behatoljon egy vezeték nélküli hálózatba és ott kihasználva a hálózat esetleges internet csatlakozását, ő maga ingyen internethez juthasson. Ehhez először keresni kell egy lehetőség szerint gyenge védelemmel ellátott Wi-Fi-t. Ezt általában egy gépkocsiban elhelyezett laptop segítségével teszi a támadó, és miután célt ért, leparkol és megkezdi a támadást. Innen ered az elnevezés.

Evil twin

Az evil twin a gonosz iker. A támadó célja, hogy megtévessze a felhasználókat és ők így az eredeti hozzáférési pont helyett a támadóhoz csatlakozzanak. A támadó ezért felveszi a megtámadott hozzáférési pont azonosítóját. A támadás során a támadó visszatereli az eredeti hálózatba a forgalmat, annak érdekében, hogy a felhasználó semmit se vegyen észre, azonban a forgalom-továbbítás során ellopja a felhasználó értékes adatait, amelyek segítségével a későbbiekben megszemélyesítheti a felhasználót.

Szolgálatmegtagadás

Ennek a támadástípusnak a célja egy adott hozzáférési pont megbénítása. Ez történhet a fizikai rétegen keresztül zavarással (jamming), de akár magasabb rétegeket is kihasználhat a támadó.

Lehallgatás

A lehallgatás során a támadó belehallgat a hálózatba és próbál mások kommunikációjából értékes adatokat szerezni.

Az itt felsorolt támadási formák közül a wardriving alkalmazható saját hálózatunk biztonságosabbá tételéhez.

A VÉDEKEZÉS

Ahhoz, hogy meg tudjuk védeni saját hálózatunkat tisztában kell lennünk a körülöttünk levő hálózati elemek csoportjaival. A beazonosítás legegyszerűbb módja a felderítés. A Wi-Fi hálózatok technikai felderítése során szerzett adathalmaz azonban önmagában nem vagy csak nehezen értelmezhető. A vizsgálat kulcsfontosságú eleme egy GIS (Geographic Information System) vagy térinformatikai alkalmazás, amely lehetővé teszi az összegyűjtött információknak feldolgozását és térbeli megjelenítését. A megjelenített információk alapján elkülöníthetjük a hálózatunkra veszélyt jelentő külső hálózati elemeket melyek hatósugara a saját hálózatunkig elér.

WARDRIVING MINT A FELDERÍTÉS EGYIK ESZKÖZE

Ez a típusú tevékenység speciális hardver és szoftver környezetet kíván. Hardver oldalról a következő eszközöket kell használni:

- Autó – ez a tipikus wardriving (vagy bicikli – ebben az esetben a warbiking-ról beszélhetünk).
- Hordozható számítógép, ami lehet laptop, kéziszámítógép vagy okostelefon, melyben van, vagy csatlakoztatható, a csomagok lehallgatásához szükséges „monitor” módba kapcsolható WLAN hálózati kártya.
- WLAN antenna. Erre akkor van szükség, ha nem elégszünk meg az eszközbe épített antenna vételi paramétereivel.
- Globális Helymeghatározó készülék (GPS). A pontos helymeghatározáshoz elengedhetetlen.

A következő képen egy átlagos hardveres összeállítást látható (1. ábra).

1.ábra: A wardriving elengedhetetlen eszközei [2]

A wardriving szoftveres oldalát két csoportra lehet bontani

- a felderítésért felelős,
- a kiértékelésért, megjelenítésért felelős programok.

A vezeték nélküli hálózatok felderítéséhez használt programokat platform szerint szokták megkülönböztetni. Linux-os operációs rendszerekhez a következő programokat használják:

- Airsnort: adatfolyamot analizál,
- Airtraf: hálózati protokoll szkenner,
- Kismet: adatfolyamot analizál.

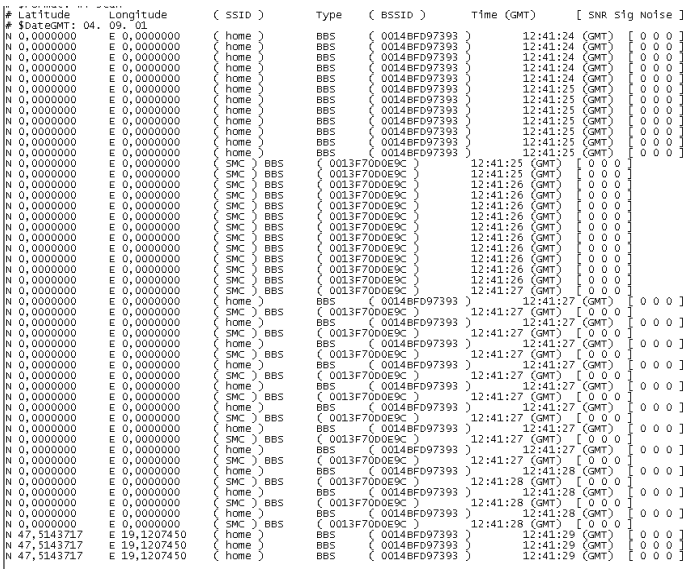
Microsoft windows-os rendszerekben a következő programokat használják:

- Inssider: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket.
- Aerosol: adatfolyamot analizál.

Kéziszámítógépes környezetben a következő programokat használják:

- Ministubler: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket
- Wifiofum: adatfolyamot analizál, megmutatja és tárolja a már megtalált hálózati elemeket.

A kiértékelés és a megjelenítés a felderítő programok lementett napló fájljaiból történik. Ha a hardverhez GPS vevőt csatlakoztattunk később nem csak a hálózati eszközökre vonatkozó információkat elemezhetjük hanem a lementett koordináták segítségével térképre is illeszthetjük a gyűjtött adatokat. A következő ábra egy ilyen adathalmaz részt mutat (2. ábra):



2.ábra: Egy wardriving során lementett adatok egy része (saját szerkesztés)

A mért adatok vizualizálását a térinformatikai szoftverek teszik lehetővé.

A TÉRINFORMATIKA

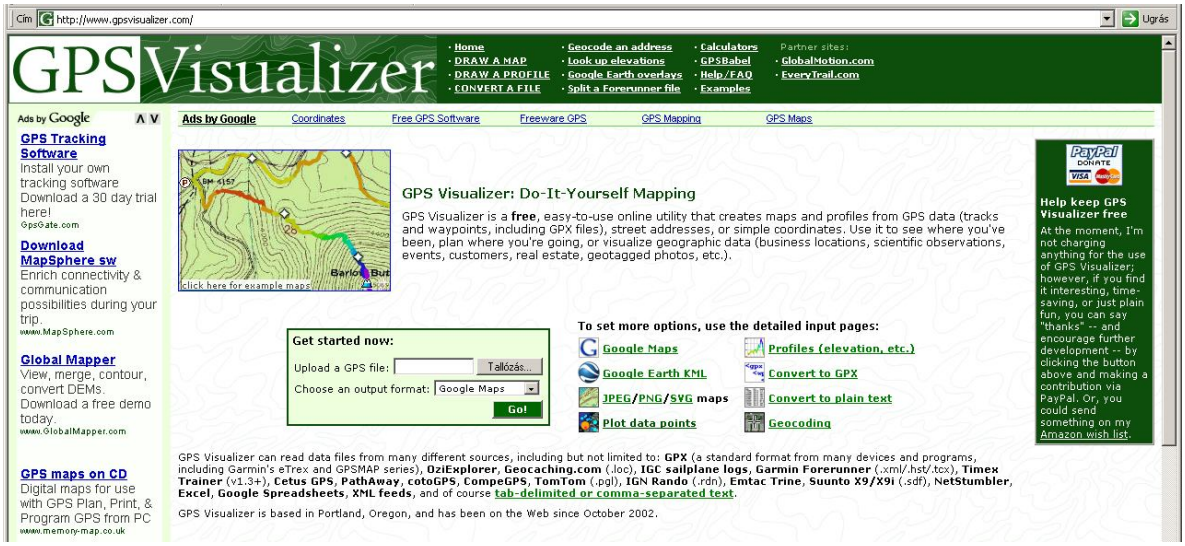
Térinformatika, geoinformatika a digitális térképekre épülő informatika, olyan interdiszciplináris terület, amely elsősorban földrajzi, térképészeti és informatikai szakismeretekre épül.

Térinformatikai rendszerek (térinformációs rendszer) alatt térképi alapú információs rendszert értünk, amely grafikus (térképi) és nem grafikus (leíró) adatokat együtt, integráltan tud kezelni.

A GIS (Geographical Information System) olyan földrajzi információs rendszer, amely tágabb értelemben térképi alapú információs rendszer, szűkebb értelemben csak a kimondottan földrajzi adatokra épülő (pl. környezetvédelmi) rendszereket jelenti, és nem tartalmazza pl. a közműnyilvántartást.[3]

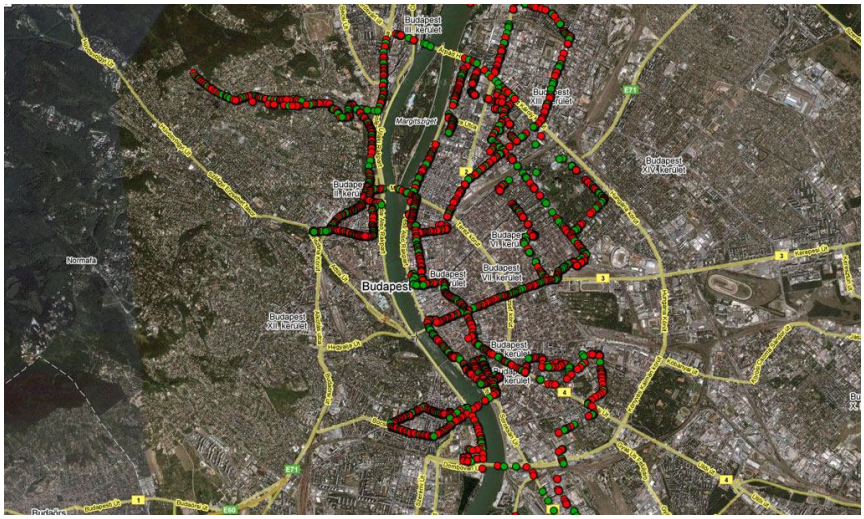
A térinformatikai rendszerek manapság bárki számára elérhetőek. Több alkalmazás is megtalálható az interneten, amely lehetővé teszi megfelelő konverziók után saját mérési pontjaink megjelenítését valamilyen térinformatikai programban.

Digitális térképeken úgy lehet megjeleníteni a vizsgálati eredményeket, hogy a mentett információkat a térinformatikai rendszer számára átkonvertáljuk. A konverziót el lehet végezni segédprogramokkal, de a legegyszerűbb, ha egy erre a feladatra készített weboldalt használunk. A következő képen egy ilyen portál látható (3. ábra):



3.ábra: A GPS naplók konvertálása [4]

A konverzió során elveszhetnek információk (például dátum, jelerősség, csatornaszám). Ezért célszerű több típust is kipróbálni ahhoz, hogy a kiértékelés és a megjelenítés minél teljesebb legyen. A megjelenítést többféleképpen végezhetjük el. Léteznek speciális webes alkalmazások erre a célra, de ezek az információ egy részének megjelenítésére alkalmasak. Ilyen portál például a maps.google.com. A konvertált napló fájl alapján a pontokat a térképre tudja illeszteni, de ezen kívül már csak a színekkel és piktogramokkal tud variálni. Ezt mutatja be a 4. ábra.



4.ábra: Budapest egy részének WLAN térképe [5]

A térképen a zöld pontok a nyitott hálózatokat jelzik. A felderített AP-ok koordinátáit a rendelkezésünkre álló adatok és GIS alkalmazások az út nyomvonalára illesztették, így a térkép közelítő pontossággal jelöli azok helyét.

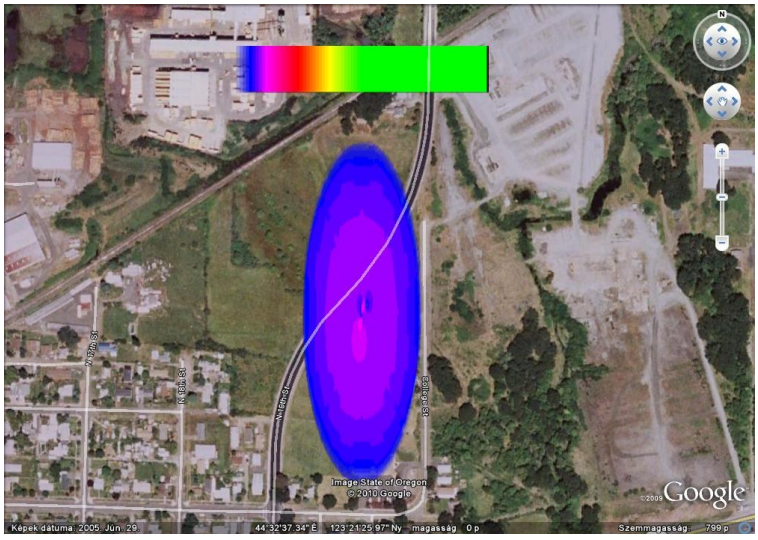
A VIZUALIZÁLÁS ÚJ MÓDSZERE

A vizualizáció abban tér el az előző pontban említettől, hogy egy speciális, erre a célra kifejlesztett PERL alkalmazást kell futtatnunk. A Footprint program a mért értékeinket MAC cím szerint leválogatva tudja értelmezni. Kiválasztva egy AP-ot leválogatja a hozzá tartozó mérési pontokat és generál hozzá két kép fájlt. Az egyik tartalmazza a mérésünk útvonalát, a másik a kiválasztott AP-unk rádiós hőtérképét. [6] A rádiós hőtérképet a táblázatban megjelölt jelszintekhez tartozó színekkel generálja le az alkalmazás.

Jelszint (dB-ben)	Színek
-100dB < Jelszint < -95dB	átlátszó -> kék
-95dB < Jelszint < -90dB	kék -> lila
-90dB < Jelszint < -80dB	lila -> piros
-80dB < Jelszint < -70dB	piros -> sárga
-70dB < Jelszint < -60dB	sárga -> zöld
-70dB < RSSI < -20dB	zöld

A mért jelszintekhez deklarált színek a hőtérképen (saját szerkesztés)

A végső megjelenítéshez a Google Earth programot használunk. A két generált kép és a Footprint által generált koordináták megadásával a Google Earth a helyére illeszti a képeket, és így majdnem pontosan azonosítható az AP helye és a Wi-Fi hálózat térerőssége (5.ábra).



5.ábra: Felderített AP-ok alakulása [7]

ELEMZÉS

A térképen megjelenített adatok alapján vizuálisan beazonosítható a saját és a minket körülvevő AP-ok lefedettsége. A méréseket úgy tudjuk teljes körűen elemezni, ha minden felderített AP-ra elvégezzük az elemzést, és a mért értékeket egy felületen külön rétegekben jelenítjük meg. Abban az esetben, ha a védeni kívánt infrastruktúra körvonalait rávetítjük az így kapott térképre, pontosan meg tudjuk állapítani a számunkra esetlegesen veszélyt jelentő Wi-Fi eszközöket. Ennek birtokában konfigurálhatjuk be rádiós hálózati elemeinket.

ÖSSZEFOGLALÓ

A Footprint alkalmazás segítséget nyújt az infrastruktúra üzemeltetőknek feltérképezni saját és környezetük rádiós térképét. A népszerű mondás szerint a rádióhullámok nem állnak meg a falak mentén, így jó esetben a felfedett AP-okat tiltani tudjuk saját rádiós eszközeinkben. Ezzel el tudjuk érni, hogy közvetlen környezetünkből ne érjen támadás.

A jövőben hogy hatékonyabbá lehessen tenni a Footprint alkalmazást autómatizálni szeretném, hogy ne csak egy AP-t vizsgáljon egyszerre, hanem az összes mért értéket helyezze a térképre. A védekezés az elsődleges, mert a védetlen vagy sebezhető végpontok egy támadás kiindulópontjaként szolgálhatnak, anonimitást biztosítanak a számítógép-hálózatokat jogellenesen használóknak, így a Wi-Fi AP-ok elleni támadások hatása szélsőséges esetben akár az egész nemzetbiztonságra is kihathat.

Felhasznált irodalom

[1] Illési Zsolt: *Wi-Fi hálózatok igazságügyi szakértői elemzése:Wi-Fi hálózatok felderítése,* Hadmérnök IV. Évfolyam 3. szám - 2009. szeptember pp. 285-302

[2] A wardriving elengedhetetlen eszközei
http://www.wardrive.net/wardriving/tools/ (2010.06.12)

[3] Dr. Katona Endre: *Térinformatika*, Jegyzet - Szegedi Tudományegyetem, 2009 p. 5
http://www.inf.u-szeged.hu/oktatas/jegyzetek/KatonaEndre/gis.pdf (2010.06.12)

[4] A GPS naplók konvertálása
http://www.gpsvisualizer.com/(2010.06.12)

[5] Budapest egy részének WLAN térképe
http://www.origo.hu/techbazis/internet/20070601utcannenetezz.html (2010.06.12)

[6] Connelly K., Liu Y., Bulwinkle D., Miller A., and Bobbitt I.: A Toolkit for Automatically Constructing Outdoor Radio Maps
http://www.cs.indiana.edu/surg/Publications/itcc2005_toolkit.pdf (2010.06.12)

[7] Felderített AP-ok alakulása
http://www.cs.indiana.edu/surg/Publications/itcc2005_toolkit.pdf

(2010.06.12)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Inkovics Ferenc
ferenc.inkovics@gmail.com

A KÜLÜGYMINISZTÉRIUM ÉS AZ INFORMATIKAI BIZTONSÁG

Absztrakt

Informatikai rendszerekkel szinte minden nap találkozunk. Az elmúlt évtizedekben életünk része lett számos informatikai rendszer. A biztonság fogalma alatt ma már nem érthetjük csak a fizikai biztonságunkat. Most már az információs tárdalom tagjai vagyunk. Tudnunk kell, mit jelent az informatikai biztonság. Jelen publikáció röviden ismerteti az informatikai biztonsággal kapcsolatos alapfogalmakat és néhány főbb informatikai biztonságot fenyegető tényezőt. Bemutatja a témához kapcsolódó főbb jogszabályokat, szabványokat és ajánlásokat. És legvégül számba veszi a Külügyminisztériumban használt nemzeti informatikai rendszereket és az Európai Unió informatikai rendszerei közül azokat, melyeket a Külügyminisztérium kollégái használnak.

We meet information systems nearly every day. During the past decades numerous information systems have become the part of our lives. Today we can't already mean only our physical security on the concept of security. Now we are a member of the information society. We have to know what the information security means. This publication reports about the basic concepts of information security and some main factors which threaten the information security. It presents the laws, standards and recommendations connecting to this topic. And finally it enumerates national information systems used in the Ministry for Foreign Affairs (MFA) and those information systems of the EU that are used by the colleagues of the MFA.

Kulcsszavak: *Informatikai Biztonság, Információ biztonság, Külügyminisztérium ~ Information Security, Ministry of Foreign Affaires*

Bevezetés

Az információ megszerzése és védelme egészen az ősközösségig visszanyúlik. E tevékenységek, melyek szinte egyidősek az emberi társadalommal folyamatosan fejlődtek és fejlődnek ma is. A számítógép megjelenése és a számítógépes hálózatok kialakítása robbanásszerű fejlődést idézett elő az információtechnikában. Rengeteget változott mind a védendő információ, mind az információ védelem módja is. Régebben az elég volt az, hogy az információt csak kevés megbízható személlyel osztották meg és védett helyre zárták. Ma azonban már nem elegendő a hagyományos módszerekkel való védelem. Az információ gyűjtését, feldolgozását, kezelését és tárolását új alapokra kellett helyezni. A technika új vívmányait már eleve úgy kell kialakítani, hogy azok képesek legyenek megfelelő védelmet nyújtani az információnak. [1]

Tisztázandó fogalmak

Az információ szerves része lett életünknek, ezért nap, mint nap találkozunk, olyan folyamatokkal, melyek az információkat védik meg a nem engedélyezett hozzáféréstől, a használattól, a kiszivárogtatástól, a megsemmisítéstől, a módosítástól és a megzavarástól. Ezen folyamatok összessége az *információ védelem*. Nem szabad összekeverni az informatikai védelemmel, ami ennek csak egy részhalmaza [2].

A félreértések elkerülése érdekében szükséges tisztázni mit is jelent ez a részhalmaz pontosan. Az *informatikai védelem* [3] az humán, technikai (környezeti, fizikai, logikai) és jogi védelmi intézkedések összessége, az informatikai biztonság (mint megkívánt állapot) megteremtésére és fenntartására. Ezen intézkedéseket az olyan tényezők ellen hozzák, amik fenyegetik:

- az informatikai rendszerben tárolt, kezelt, rendszerezett és továbbított adatot (információt),
- az informatikai szolgáltatásokat,
- és a mindezeket biztosító informatikai rendszereket.

Látható, hogy az előző 2 fogalom mindegyike 1-1 állapot elérésére irányuló tevékenységek összessége. Az információ védelem az információbiztonságra, az informatikai védelem pedig az informatikai biztonságra törekszik. Mindezek mellett szükséges tisztázni ezt a két fogalmat is melyek nem tevékenységet, hanem állapotokat tükröznek. Míg az *Információ biztonság* az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából [2], addig az *informatikai biztonság* a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos [4].

Sajnos összekavarodást okozhat az, hogy az információ védelem és informatikai védelem általános angol megfelelője egyforma: information security; és csak a szövegkörnyezet teszi egyértelművé azt, hogy mit is takar [5].

Az informatikai biztonság szükségessége, létjogosultsága

Az információ, az informatika és kommunikáció a mindennapi életünk aktív szereplője. Az informatikai, információs és kommunikációs rendszereket már nem eszközként, hanem erőforrásként hasznosítják az államok és a vállalatok is. Fontosságuk miatt, ezeknek a rendszereknek a védelme századunk központi kérdése lett [6]. Egyre „többet tudó”, bonyolultabb és nagyobb kiterjedésű informatikai rendszereket alkot az emberiség. A legtöbb

irodai munkakör elengedhetetlen része lett a számítástechnika, mert az intézmények, a vállalatok és vállalkozások tevékenységét egyre nagyobb mértékben támogatják informatikai alkalmazásokkal. Az informatikai rendszerek életünkben betöltött funkciójának növekedésével párhuzamosan az informatikai biztonság szerepe és jelentősége egyre nagyobb jelentőséggel bír.

Az alkalmazott információs és informatikai rendszerek állapota, rendelkezésre állása, működése közvetlenül befolyásolja nagytömegű embercsoportok közvetlen életét, munkáját, társadalmi termelőképességét. Mindezek miatt az információs és informatikai rendszerek ellen mért csapások hatása összemérhető a tömegpusztító fegyverekkel mért csapásokkal. Az elmúlt évtizedekben kialakult és megjelent új fenyegetések, mint pl.: hackerek, crackerek, informatikai hadviselés, adatlopás és kiberterrorizmus miatt egyre nagyobb jelentősége van az informatikai és információ biztonságnak is. Mindezek hátterében az áll, hogy az információ az egyben érték, vagyon és hatalom is.

Kihívások az informatikai biztonság területén

A különböző informatikai rendszereknek számos forrásból eredő fenyegetéssel kell szembe nézniük, melyek bekövetkezésükkor jelentős anyagi és erkölcsi károkat is okozhatnak. Ahhoz, hogy megfelelően fel lehessen készülni a fenyegetések kivédésére, elkerülésére, azok károinak minél hatékonyabb enyhítésére, szükséges, hogy már az informatikai rendszerek tervezésénél figyelembe legyenek ezek véve. Informatikai rendszerek biztonságát az alábbi tényezők fenyegethetik:

a. kiberterrorizmus,
b. információs műveletek (információs hadviselés),
c. gazdasági hírszerzés,
d. ipari kémkedés,
e. számítógépes csalás
f. hackerek, crackerek,
g. rosszindulatú, bosszúálló munkatársak,
h. szabotázs,
i. vandalizmus
j. képzetlen, hanyag, felelőtlen munkatársak,
k. természeti csapások (pl.: tűzkár, árvíz, földrengés, stb.),
l. műszaki hibák,
m. elektronikus dokumentumok bizalmasságának vagy hitelességének sérülése
n. támadás rosszindulatú programokkal
o. szolgáltatás igénybevételének letagadása
p. web lapok tartalmának illegális megváltoztatása
q. adatlopás „védett” szerverekről
r. szolgáltatások megbénítása terheléses támadással (Denial of Service, DoS)
s. stb.

A különböző fenyegetések előfordulási gyakorisága eltérő, de egyes rosszindulatú támadások és szándékos károkozások, mint pl.: elektronikus azonosítók és személyes adatok lopása - adathalászat; vírusok, trójai programok terjesztése; stb. szinte mindennapossá váltak. Az informatikában is mindig a védekezés van hátrányban a fenyegetésekkel szemben. A támadók haladva a korral mindig újabb és újabb fenyegetéseket találnak ki és folyamatosan fejlesztik a módszereiket is. Egyre komplikáltabb megoldásokat és egyre bátrabban alkalmaznak, ezzel is folyamatosan nehezítve az informatikai biztonság fenntartását.

A fenyegetések ellen lehet és szükséges is védekezni. Az informatikai biztonság eléréséhez az informatikai védelemnek két fajtája terjedt el: a reaktív és a proaktív védekezés. A lényegi

különbség a kettő között az, hogy míg a reaktív védekezés a már bekövetkezett károkat enyhíti, és a proaktív védekezés során pedig megpróbálunk felkészülni a leendő támadások és fenyegetések káros hatásaira is, ezért a bekövetkezett káresemény által okozott költségek és egyéb károk és hatásaik minimalizálódnak. A proaktív védekezés ugyanakkor jóval költségesebb is lehet és akár sokkal több erőforrás bevonását is szükségessé teszi. Azt mindig mérlegelni kell, hogy adott esetben mekkora védelmi erőforrás ráfordítás éri meg. Ezt az alkalmazott biztonságpolitika határozza meg.

Jogszabályok

Az informatikai biztonság témakörét illetően is több csoportba oszthatóak az alkalmazandó jogszabályok, szabályzók. Az alábbi fontosabb jogszabályokat és szabályzókat különítjük el:

- Minősített adat kezelésére,
- Az üzleti titokra,
- Banktitokra és értékpapírokra,
- Adatvédelemre,
- Elektronikus aláírásra és
- E-közigazgatásra vonatkozóak

Az Országgyűlés 2009. december 14-én fogadta el a minősített adat védelméről szóló 2009. évi CLV. törvényt (Mavtv.), amely az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint a Nemzeti Biztonsági Felügyeletről szóló 1998. évi LXXXV. törvény helyébe lépett. A 2010. április 1-jén hatályba lépett jogszabály alapjaiban kodifikálja újra a minősített adatok védelmének magyarországi struktúráját. Megteremti a minősített adatok védelmének egységes jogszabály- és intézményrendszerét, s egyúttal eleget tesz legfontosabb jogharmonizációs kötelezettségeinknek. Lényegi változás, hogy a törvény mind a nemzeti, mind a külföldi minősített adatok védelmére egységes követelményeket határoz meg.

Egyes információk titokban tartása mögött indokolt állami vagy magánérdek áll, a különböző típusú titkokat ezért szükséges védeni. A magyar jogszabályok meghatározzák a különböző titok fogalmait, és azok kezelési mikéntjét is. A minősített adatok olyan titkok, melyeknél a titoksértést a magyar büntetőjogi törvények szerint büntetni kell. Titkoknak minősülnek az üzleti titkok is, melyet szintén védenek a magyar jogszabályok. A gazdasági társaságok számára létfontosságú, hogy az üzleti információk ne kerüljenek illetéktelen kezekbe. Az a gazdasági társaság, akinek a pénzügyi, gazdasági, termelési információi esetleg jövőbeni tervei idő előtt ismerté válnak a piac többi szereplői előtt, rendkívül kedvezőtlen helyzetbe kerülhet. Ugyanakkor nem szabad megfeledkezni arról, hogy az üzleti titoknak nem minősülő adatokról tájékoztatást kell adni, mert azok viszont közérdekűek. Magyarországon a gazdasági verseny tisztaságát és szabadságát az 1996. évi LVII. törvény szavatolja. Ez a törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szól [7][8].

Az üzleti titok fogalmát a Ptk. 81. § (2) bekezdése tartalmazza. Az üzleti titok azonban nem fed le minden szükséges titok területet. Miként győződhetünk meg arról, hogy a bank kiknek és milyen módon ad tájékoztatást az általa kezelt bizalmas adatainkról, amik üzletileg igen értékesek. De hasonló gondolatok támadhatnak bennünk azon pénzintézetek esetében is, akik az értékpapírjainkat kezelik. Ezt az űrt oldják fel az alábbi törvények:

- 1996. évi CXI. törvény az értékpapírok forgalomba hozataláról, a befektetési szolgáltatásokról és az értékpapír tőzsdéről,
- 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról, és a
- 2001. évi CXX. törvény a tőkepiacról.

E három törvényben meghatározásra kerül a banktitok (1996. évi CXI. törvényben) és az értékpapírtitok (2001. évi CXX. törvényben), valamint azoknak a felhasználhatósági köre is,

tehát hogy kinek és milyen módon adható át, valamint mikor és miként használhatóak fel ezek az adatok [1][9].

Személyes adatainkat[1] nem csak a bankok és pénzintézetek kérhetik el. Bármilyen élethelyzetben szükség lehet arra, hogy használjuk őket (pl.: a boltban való bankkártyás fizetéskor, nemzetközi utazáshoz való jegyváltáshoz, akciós sorsolásokra való jelentkezéskor, regisztrációs űrlapok kitöltésekor stb.). Az Európai Unió Alapjogi Chartája is kimondja, hogy „Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez" [10]. Az államoknak és persze a különböző gazdasági társaságoknak az lenne a célja, hogy az egyes személyek féltett magánéleti adatait is rögzítsék többfajta nyilvántartásban. E tekintetben ütköznek az érdekek az államok, gazdasági társaságok és az egyének között. Mindegyik számára belátható, egyik érdek nem valósítható meg teljes mértékben, ezért kompromisszumos megoldásként születtek meg azok a jogszabályok, melyek meghatározzák, hogy milyen adatok, milyen célból gyűjthetőek és miként lehet őket, tárolni, felhasználni, illetve harmadik félnek átadni. A magyar jogszabályok közül a Magyar KöztársaságAlkotmányának (1949. évi XX. törvény) 59. §-a és az 1992. évi LXIII. törvény foglalkozik e kérdésekkel. Ez utóbbi a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szól és megfelel az Európai Tanács Adatvédelmi Egyezmény valamint a Gazdasági Együttműködési és Fejlesztési Szervezet útmutatásainak is [1].

Életünk során több olyan helyzet is előáll, amikor a személyes adatokon kívül szükség van az aláírásunkra. pl.: egy szolgáltatás megrendelésekor ezzel igazoljuk, hogy az adott megrendelő fél tényleg mi voltunk, magyarán az aláírásunkkal hitelesítjük. Ma az információs társadalomban már arra is van lehetőség, hogy ne csak papíron, hanem elektronikusan is alá tudjunk írni. Mind a papíron, mind az elektronikusan történő aláírásnál is fontos szempont, hogy egyértelműen azonosítható legyen az aláíró fél. A kézzel való aláírásnál a leírt betűk írásmódja az azonosítás alapja, de az elektronikus aláírásnál nem az aláírásunk szkennelt képének az elektronikus dokumentum mellé csatolásáról beszélünk, hanem egy olyan könnyen létrehozható és egyedi azonosítóról, amit csak egyetlen személy, azaz mi tudunk létrehozni. Az elektronikus úton megtett aláírásunk hitelességét törvény is elismeri, a 2001. évi XXXV. törvény az elektronikus aláírásról. Ez a törvény teremtette meg Magyarországon a hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit [11][12].

Az információs társadalom egyre inkább elektronikus útra tereli a különböző szolgáltatásokat. Lehet szó akár adóbevallásról, számlakibocsátásról, szerződések megkötéséről, különböző megrendelésekről, pénzügyi utalásokról és transzferekről; az elektronikus úton történő ügyintézés egyre gyakoribbá válik. Ahogy a társadalom egyre inkább alakul át e-társadalommá, úgy növekszik a közigazgatásban is e-közigazgatási szolgáltatások száma. Magyarországon az alábbi törvények foglalkoznak az e-társadalommal és e-közigazgatással:

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (Ket.)
- 2009. évi LX. törvény az elektronikus közszolgáltatásról
- 2009. évi LXXVI. törvény a szolgáltatási tevékenység megkezdésének és folytatásának általános szabályairól

[1] Személyes adatnak minősül minden olyan információ, amely egy adott személyre vonatkozik, és amely alapján az a személy – közvetlenül vagy közvetetten – azonosítható, pl. a neve, telefonszáma, elektronikus levélcíme, születési helye és ideje stb.

Szabványok és ajánlások [13][14][15][16][17]

A szabványok és ajánlások olyan egységesítő és szabályozó tevékenységnek az eredményei, melyeket a felhasználó és a fogyasztó érdekében hoztak létre azzal a céllal, hogy egységes és következetes megoldási módokat alkalmazzanak a rendszeresen ismétlődő műszaki és gazdasági feladatokra. Ezeket a műszaki dokumentumokat hivatalos, félhivatalos és informális szervezetek készítik. Azonban ugyanazon témakörben készített szabványok és ajánlások is eltérhetnek egymástól. Olyan nemzetközi szervezetek, mint az EU és az OECD is készítenek ajánlásokat és irányelveket, de az USA mégis vezető szerepet játszik a szabványok és ajánlások készítésében. Ez köszönhető annak is, hogy a hagyományoknak köszönhetően civil és kormányzati téren is tekintélyes szabványosítási infrastruktúrával van ellátva, és ezek meglehetősen jó összhangban tudnak együtt dolgozni.

Az informatikai biztonság területén az alábbi szabványokat és ajánlásokat fontos megemlíteni:

1. Common Criteria (CC):
   Az Európai Közösség, az amerikai és kanadai kormányok támogatásával létrehozott dokumentum, ami a korábbi ajánlások (mint pl.: a TCSEC és ITSEC ajánlások) tartalmi és technikai különbségeit kísérelte meg közös nevezőre hozni. Fő jellemzői a következők:
   - Egységes, a megvalósítás módjától független, követelményeket határoz meg.
   - Egységes kiértékelési módszertant ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához.
   - Meghatározza az informatikai rendszerek biztonsági követelményeinek többszintű kategóriákból álló katalógusát.
   - Egyaránt felhasználható szoftver és hardver elemek vizsgálatához is.
   - A termékek rugalmasan megválaszthatók, mert a követelmények nem hardver vagy szoftver specifikusak.
   - Definiálható a biztonsági funkcionalitás, azaz a CC fogalmai szerint a védelmi profil (Protection Profiles), amely függetlenül besorolható a CC-ben meghatározott hét biztonsági szint (Evaluation Assurance Level: EAL) valamelyikébe.
2. BS 7799
   Ezt a nemzetközileg dicsért és használt szabványt a Brit Szabványügyi Hivatal adta ki. Két fő részből áll, melyek 1995-ben illetve 1998-ban lettek publikálva:
   - Az informatikai biztonság irányításának kézikönyve:
     Ez a szabvány a szervezeti szintű, informatikai biztonságmenedzsment központú szemléletet követi és a szervezet üzleti céljaiból és stratégiájából vezeti le a biztonsági követelményeket és intézkedéseket.
   - Az informatikai biztonsági irányítási rendszer specifikációja
     Az előző rész kiegészítéseként jelent meg és elsősorban a szervezetek menedzsmentje részére fogalmaz meg követelményeket az Információbiztonság Menedzsment Rendszer megvalósítására és dokumentációs rendszerére vonatkozóan, valamint szervezeti szintű informatikai biztonsági intézkedéseket ajánl.
3. ISO/IEC 270xx
   Az ISO/IEC 27000 szabványsorozat az informatikai biztonság irányítási rendszerének "legjobb gyakorlatait" (best practices) fogja össze, és elsősorban a felhasználói oldalon helyet foglaló IT menedzserek számára készült. Az informatikai biztonságmenedzsment rendszer megvalósítására és ellenőrzésére vonatkozó követelményrendszer kidolgozását segíti, úgy hogy mindazon előírásokat magában

foglalja, amik a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelmények és védelmi intézkedések és az azok implementálásához, auditálásához, kockázatelemzéséhez szükségesek. A szabványsorozat néhány tagjának rövid ismertetése:

- ISO/IEC 27000: Szószedet és terminológia a sorozat valamennyi szabványához.
- ISO/IEC 27001: Az informatikai biztonság irányítási rendszere (BS 7799-2:2002), a szervezet auditálásához szükséges (megfelelőségi) előírások.
- ISO/IEC 27002: Az informatikai biztonság irányítása gyakorlati előírásait, ellenőrzési célokat és a legjobb gyakorlatot írja le.
- ISO/IEC 27003: Az ISO/IEC 27000 szabvány implementálásához szükséges tanácsokat és útmutatókat fogja tartalmazni.
- ISO/IEC 27004: Egy új szabvány lesz, amely az informatikai biztonság mérésével fog foglalkozni, abból a célból, hogy az informatikai biztonság irányítási rendszerének hatékonyságát mérni tudjuk.
- ISO/IEC 27005: Az informatikai biztonság kockázatkezelésével fog foglalkozni.
- ISO/IEC 27006: az ISO/IEC IEC 27001 szabványnak való megfelelést vizsgáló szervezetek számára tartalmaz követelményeket.
- ISO/IEC 27011: informatikai biztonságirányítási irányelvek lesznek a telekommunikációihoz.

4. MEH ITB 8. sz. ajánlás
   Ez egy tájékoztató az informatikai biztonság megteremtésének legfontosabb elemeiről és célja felkészíteni a szervezetet az informatikai biztonsági koncepciójának kialakítására. Kockázatelemzési módszertanként használják.
5. MEH ITB 12. sz. ajánlás
   A logikai védelem előírásait, részletes követelményeket és védelmi intézkedéseket tartalmaz informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság témakörét illetően is. Informatikai Rendszerek Biztonsági Követelményei névvel is ismert.
6. MEH ITB 16. sz. ajánlás
   A Common Criteria szabvány magyar változata.
7. KIB 25. számú ajánlás
   A Közigazgatási Informatikai Bizottság 25. számú ajánlása a Magyar Informatikai Biztonsági Ajánlások című ajánlássorozat. A sorozatban 12 önálló ajánlás található, melyek 3 jelentős csoportot ölelnek fel:
   - MIBIK (Magyar Informatikai Biztonság Irányítási Keretrendszere)
   - MIBÉTS (Magyar Informatika Biztonság Értékelési és Tanúsítási Séma)
   - IBIX (Informatikai Biztonsági Iránymutató Kis Szervezetek Számára)

   Az informatikai biztonságot a MIBIK szervezeti oldalról, a MIBÉTS pedig technológiai oldalról közelíti meg. És míg a MIBIK és MIBÉTS olyan szervezeteknek nyújt segítséget, amik rendelkeznek jelentősebb informatikai rendszerrel és/vagy az informatikai rendszerhez elkülönült informatikai személyzettel, addig az IBIX mindazon szervezeteknek hasznos, amik nem rendelkeznek ilyen lehetőségekkel.

A Külügyminisztérium informatikai és információs rendszerei

Magyarországon a külügyekkel foglalkozó közigazgatási csúcsszerv a Külügyminisztérium. A Külügyminisztériumban az informatikai biztonság megteremtéséért és fenntartásáért a Biztonsági Informatikai és Távközlési Főosztály felel. Az informatikai támadások alapvető célját az, adatot informatikai rendszer elemein keresztül is el lehet érni és fenyegethetik. A feladata ellátását jócskán megnehezíti az a tény, hogy a közel 2000 fős köztisztviselői

állomány kevesebb, mint a fele dolgozik csak Magyarországon, a többiek a kb. 100 képviselet egyikén vannak külszolgálaton. A Külügyminisztériumnak, feladatainak jellegénél fogva több informatikai rendszere van és mindegyik rendszer biztonságára ügyelni kell. A Külügyminisztériumban az alábbi jelentősebb nemzeti informatikai és információs rendszerek, illetve azok végpontjai üzemelnek:

a. KIR (Konzuli Információs Rendszer – Consular Information System - CIS):
   A két alapvető konzuli tevékenységet, a vízumkiadást és a klasszikus konzuli ügyek intézését informatikailag támogató rendszer. Célja a konzuli feladatok elvégzésének könnyítése és gyorsítása. A KIR kezeli és elektronikusan tárolja a vízumkérelmeket, az egyéb konzuli ügyeket, a vonatkozó pénzügyi forgalmat (bevételeket) is. Különböző paraméterekkel statisztikák készítésére is alkalmas. És 2007 decembere óta, amióta teljes jogú tagjai vagyunk a Schengeni országoknak, azóta közvetetten a Schengeni Információs Rendszerrel is kommunikál a KIR.
b. VKH (Védett Külügyi Hálózat):
   A Magyar Köztársaság nemzeti érdekeinek hatékony érvényesítése az Európai Unióban koncepcióváltást tett szükségessé a diplomáciai információszerzésben, a tájékoztatásban és az információkhoz való hozzáférés terén, valamint szemléletváltást az információk minősítésében és technológiaváltást az információtovábbításban. A diplomáciai információs tevékenység megújításának technikai feltételeit biztosítja a Külügyminisztérium és a külképviseletek védett hálózata a Védett Külügyi Hálózat. A VKH lehetővé teszi a „bizalmas" és „korlátozott terjesztésű" minősített nemzeti, valamint EU- és NATO-információk gyors továbbítását [18]. A „Bizalmas" és „Korlátozott terjesztésű" minősítéssel ellátott iratokat, táviratokat a szervezeti egységek a Védett Külügyi Hálózat számítógépein készítik, kezelik és ugyanebben a rendszerben továbbítják a Központ szervezeti egységei, illetve a Központ és a bekapcsolt külképviseletek, valamint a Központ és egyes magyar kormányzati szervek között (pl.: egyes minisztériumok).
c. EU DOK (EU Dokumentációs rendszer) [19][20]:
   E rendszer fő feladata, hogy segítse az európai uniós ügyek kormányzati koordinációját. Ebbe beleértjük az elektronikus úton Magyarországra érkező nem minősített Európai Uniós dokumentumok szétosztását és különböző magyar intézkedések végrehajtásának folyamatát (pl.: tárgyalási álláspontok kialakítását). A felhasználók számára kialakított felület egy portálrendszer. Ebben az európai ügyekre szakosodott személyre szabott portálban 60 db úgynevezett közösségi felületek alakítható ki a maximális 1000 felhasználónak. Közösségekben csoportosíthatóak azok a felhasználók, akik közösen dolgoznak. A közösségek között szakértői csoportok[2], tanácsok és az EKTB közössége található meg. A rendszer a különböző témákhoz tartozó információkat (megküldött EU-s tervezeteket, tárgyalási álláspontokat, jelentéseket, jegyzőkönyveket, feladatok, események, fórumüzenetek stb.) úgynevezett dossziékban rendszerezi. Az EUDOK lehetőséget ad arra is, hogy mind az EU-s mind a hazai ülések napirendjeit nyomonkövessük. Az egyes napirendi pontokhoz automatikusan hozzárendeződnek a kapcsolódó dossziék is.

[2] A szakértői csoport tagjai azok a személyek, akik az Európai Unió politikáját illetően összefogják a hazai közigazgatási feladatokat, így többek között a beérkező uniós tervezetre kialakítják a magyar álláspont tervezetet, valamint elkészítik a hozzá kapcsolódó egyéb dokumentumokat (pl. környezetvédelem, tőke szabad áramlása, foglalkoztatás- és szociálpolitika)

A Külügyminisztériumban végponttal rendelkező Európai Uniós rendszerek

A fentebb említett nemzeti rendszereken kívül vannak még olyan informatikai rendszereknek végpontjai a külügyminisztériumban, melyeket az EU-val való kapcsolattartás miatt szükséges fenntartani. Ezen rendszerek kialakítása, üzemeltetése során alapvetően az „EU minősített információk védelmét szolgáló biztonsági szabályokról" elnevezésű és 13885/1/09-es számot viselő tanácsi határozat szerint kell eljárni. Természetesen ez nem írja felül a magyar jogszabályokat, de nem is szükséges, mert a jogharmonizációnak köszönhetően igazodnak ehhez. A Külügyminisztériumban az alábbi Európai Uniós informatikai rendszereknek van végpontja:

a. EU Extranet-L és Extranet-LR hálózatok
   Az Európai Únió Tanácsa ezen a rendszeren keresztül terjeszti a dokumentumokat (pl.: tanácsi munkacsoportok üléséhez az anyagokat, dokumentumokat). A rendszer a felhasználóknak alapvetően 2 féle terjesztési módszert nyújt. Az egyik egy automatikus információküldés a felhasználó e-mail postafiókjába, a másik pedig egy WEB-es elérési opció, ahol egy WEB oldalon van lehetőség a szükséges anyagok, dokumentumok keresésére, megnézésére. Az egyes felhasználók esetében be lehet állítani, hogy milyen anyagokhoz és dokumentumokhoz férjen hozzá. Ennek alapja a következők lehetnek:
   - Acronym[3] (betűszó, mozaikszó),
   - Munkacsoport,
   - Dokumentum típus (DOC, PDF stb.) és
   - Minősítési szint (nyílt, nem nyilvános, korlátozott terjesztésű).

   Jelenleg a Tanács 2 fajta Extranet oldalt üzemeltet:
   1. EU Extranet-L oldalt, a nyílt és nem nyilvános (limite) dokumentumokhoz és az
   2. EU Extranet-R oldalt pedig a korlátozott terjesztésű (restraint) dokumentumok eléréséhez.

b. CORTESY (Correspondance Européenne Terminal System) rendszer
   A CORTESY rendszer titkosított kapcsolatot biztosít a tagállamok külügyminisztériumai, Európai Unió melletti állandó képviseletei, a Bizottság és a Tanács Főtitkársága között. Segítségével történik az úgynevezett COREU üzenetek (diplomáciai táviratok) elektronikus továbbítása a Tanács közös kül- és biztonságpolitikai partnerei számára [21]. Nagyon hasznos rendszer pl.: a multilaterális vagy harmadik államot érintő kérdések politikai elemzéseinek szaktanácskozásaihoz.
   A rendszer felépítése majdnem teljesen megegyezik az ESDP-Net hálózatéval, csak apróbb eltérések vannak.

c. ESDP-Net (European Security and Defence Policy – Európai Biztonság és Védelem Politika)

[3] A különböző témákhoz különböző acronymeket rendelnek (pl.: COAFR: Afrikai vonatkozású téma; COASI: Ázsiát és Óceániát érintő témák, COMELEC: elektronikus kommunikációt érintő témák stb.). Az automatikus terjesztés során az egyes tanácsi munkacsoportok és almunkacsoportok tagjai számára azokat az anyagokat, dokumentumokat küldik automatikusan amelyik acronymre fel vannak iratkozva. Illetve a WEB-es felületen az adott acronymekkel ellátott dokumentumokra is rá lehet keresni. A tanácsi munkacsoportok a készítéskor ellátják rá jellemző acronymekkel az anyagokat és dokumentumokat, így minden az érintett témával foglalkozó személy és csoport megkapja azt az információt, amiről tudnia kell, illetve amivel feladata van.

Az ESDP-Net hálózat titkosított kapcsolatot biztosít a Tanács és annak európai biztonsági és védelmi politikai partnerei között. A hálózat felhasználói:

- külügyminisztériumok,
- hadügyminisztériumok,
- vezérkari főnökök és műveleti főhadiszállások,
- az EU Műhold Központja Torrejonban, Spanyolországban
- a Tanács főtitkárság és
- az Európai Bizottság

A hálózat felépítése majdnem teljesen megegyezik a CORTESY rendszerével, csak apróbb eltérések vannak. A hálózat minden egyes üzenete akkor érhető el, ha meg van hozzá a megfelelő felhatalmazás. A rendszer minden egyes végpontja a beérkezett üzeneteket a saját adatbázisában tárolja. A rendszer minden olyan helyben tárolt üzenetben engedi tallózni a felhasználókat, amihez rendelkezik felhatalmazással, vagyis azok között, amikhez a helyi adatbázisában hozzáférést engedélyeztek számára. Arra nincs lehetőség, hogy egy másik végpont adatbázisához férjen hozzá a felhasználó.

d. EU CIRCA (Communication & Information Resource Centre Administrator) [22]
A CIRCA az egy extranet eszköz, melyet az Európai Bizottság IDA programja keretében fejlesztettek ki, és hangoltak a kormányzati igényekhez. Hasonlóan a magyar EUDOK rendszerhez, ez is egy WEB alapú portál. A földrajzilag szétszórt EU-s intézmények és partnereik használják információ és dokumentumok megosztásához, továbbá eszmecserék, viták, tanácskozások lefolytatásához és számos más funkcióhoz is. A CIRCA rendszer a felhasználókat közösségekbe szervezi és minden egyes közösségnek biztosít egy úgynevezett magán tárhelyet, aminek az eléréséhez csak internet elérésre és egy internet böngészőre van szükség. Minden magán tárhely esetében a tanácsi munkacsoportokhoz hasonlóan az közösség egyik tagja a moderátor, az elnök vagy, ahogy a CIRCA nevezi a vezető (leader).

e. SESAME (Secured European System for Automatic Messaging) [23]
A SESAME rendszer ma még nem „élő" rendszer. 2002-ben kezdték a kifejlesztését és a kezdeti céldátum 2004 Júliusa volt, mely különböző okok miatt[4] 2012-re módosult. Az alapötlet szerint a jelenlegi CORTESY és ESDP-Net rendszereket fogja kiváltani. Ugyan azon a fizikai összeköttetésen 2 logikai szintet hoznak létre rejtjelző eszközökkel: egy korlátozott terjesztésű (az EU korlátozott terjesztésű és alacsonyabb minősítésű anyagoknak) és egy titkos szintű (az EU bizalmas és EU titkos minősítésű anyagoknak) kommunikációs csatornát. A két rendszer nem egyszerűen lecserélik, hanem további kommunikációs lehetőségekkel és felhasználói funkciókkal bővítik is. Mivel a rendszer még mindig tervezési fázisban van, ezért még sokat változhat a végső kiépítettsége is.

Következtetések

A ma alkalmazott informatikai rendszerek minden elemére kiterjed a fenyegetettség. Veszélybe kerülhetnek a következő alábbi tényezők:

- hardver környezet

[4] A különböző okok közül néhány: 1) a tagállamok küldöttei nem tudtak megegyezni abban, hogy miként kezeljenek bizonyos fajta érzékeny információkat. 2) alábecsülték az időszükségeltét a szigorú akkreditációs eljárásnak, hogy megszerezzék a tanács biztonsági tanúsítványt 3) ugyancsak alábecsülték a projekt műszaki összetettségét is.

- szoftver környezet
- kommunikációs rendszer
- emberi erőforrás, a jól képzett munkaerő.

Ahhoz, hogy kellően felkészülten reagáljunk az informatikai támadásokra, hogy meg tudjuk tenni a kellő lépéseket azok megelőzéséhez, a károk enyhítéséhez, és a következmények felszámolásához, az alábbiak végig gondolása nélkülözhetetlen.

Szükséges, hogy létezzenek olyan szervezetek, szakemberek, eszközök és módszerek, amelyeket különböző fajta informatikai támadásokra való megelőző lépésként meg tudunk lépni, illetve bekövetkezésük esetén fel lehet használni a védekezéshez, és kárenyhítéshez. Az ilyen helyzetekre való sikeres reagálás és válasz miatt, hozták létre a szabványokat, ajánlásokat és jogszabályokat. A jól átgondolt és használható szabványokat és ajánlásokat a különböző szervezetek még úgy is elkezdik alkalmazni, hogy azok alkalmazása nem kötelező érvényű. Ez pedig az első legjobb automatikus lépés az informatikai biztonság irányába.

Irodalmi hivatkozás

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

[2] Információbiztonság a másik oldalról: Hackerek Magyarországon
http://www.zmne.hu/tanszekek/ehc/konferencia/prez/Krasznay_Csaba.ppt
(letöltve: 2010.05.18)

[3] Krimináltechnika szerepe az informatikai védelem területén
http://www.hadmernok.hu/2009_1_illesi.pdf
(letöltve: 2010.05.16)

[4] Muha Lajos: Az informatikai biztonság evolúciója és revolúciója In: Magyar Tudomány Ünnepe - Gábor Dénes Főiskola (Informatikai rendszerek biztonságtechnikája Konferencia), Budapest, 2006.11.08.,
http://www.mtakpa.hu/kpa/download/1233544.pdf
(letöltve: 2010.05.17)

[5] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme (PhD disszertáció), ZMNE, Budapest, 2007.
http://www.mtakpa.hu/kpa/download/1228916.pdf
(letöltve:2010.05.30)

[6] Az informatikai biztonság alapjai
http://e-oktat.pmmf.hu/webgui/www/uploads/images/1497/Informatikai_biztonsag_1.pdf
(letöltve 2010.05.18)

[7] Az üzleti titkok védelméről - 2. rész
http://www.ugyvezeto.hu/cikk/60415/az-uzleti-titkok-vedelmerol-2-resz?area=595
(letöltve: 2010.05.28)

[8] Mi minősül az üzleti titok megsértésének?
http://www.feketelista.hu/mi-minosul-az-uzleti-titok-megsertesenek/
(letöltve:2010.05.28)

[9] Banktitok
http://www.bankkartya.hu/?cikk=2578&lap=1
(letöltve:2010.05.28.)

[10] Személyes adatok védelme az Európai Unióban
http://ec.europa.eu/justice_home/key_issues/data_protection/data_protection_0108_hu.pdf
(letöltve: 2010.05.28)

[11] Elektronikus aláírás
http://srv.e-szigno.hu/menu/?lap=tudasbazis_elektronikus_alairas
(letöltve:2010.05.29)

[12] Elektronikus aláírás
http://www.csatolna.hu/hu/eloadas/savo/elektronikus_alairas.pdf
(letöltve:2005.05.29)

[13] Szabvány
http://hu.wikipedia.org/wiki/Szabvány
(letöltve:2010.05.29)

[14] 1995. évi XXVIII. törvény a nemzeti szabványosításról

[15] Szabványosítás
http://www.recoware.hu/biometria/szabvanyositas_es_ajanlasok.html
(letöltve:2010.05.29)

[16] Az információbiztonság sarokkövei: szabványok és ajánlások
http://www.isotanusitas.hu/hu/cikkolvas/informaciobiztonsag
(letöltve:2010.05.29)

[17] Muha Lajos: Az informatikai biztonság mérése, In: Tudomány Hete a Dunaújvárosi Főiskolán: interperszonális nemzetközi tudományos konferenciasorozat. Dunaújváros, 2009.11.09-2009.11.13.
(http://www.mtakpa.hu/kpa/download/1278547.pdf letöltve:2010.05.17)

[18] A külügyminiszter 12/2004. KÜM utasítása a Védett Külügyi Hálózat használatáról

[19] EU-s ügyek kezelése a Synergon segítségével.
http://www.terminal.hu/cikk.php?article_id=5565
(letöltve: 2009-11-10)

[20] Synergon MAGASYN - 2005. tél, 16-17. oldal: EUDOK – uniós ügyek e-koordinációja
http://www.synergon.hu/data/cms9687/msyn_tel2005.pdf
(letöltve: 2010.05.26)

[21] The main bodies specific to the CFSP
http://www.diplomatie.gouv.fr/en/european-union_157/eu-in-the-world_1491/common-foreign-and-security-policy_5463/operation-of-the-cfsp_5467/the-main-bodies-specific-to-the-cfsp_5472/cfsp-communication-networks_8757.html
(letöltve: 2009.12.15)

[22] A Quick Reference Guide to CIRCA 3.4
http://circa.europa.eu/docs/circa_quick_guide.pdf
(letöltve: 2010.04.26)

[23] Official Journal of the European Union, 10.11.2009 NOTICES FROM EUROPEAN UNION INSTITUTIONS AND BODIES: COURT OF AUDITORS
http://eca.europa.eu/portal/pls/portal/docs/1/3258349.PDF
(letöltve: 2010.05.20)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Kassai Károly
kassai.karoly@hm.gov.hu

A MOBIL KOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁNAK ÉS VÉDELMI RENDSZABÁLYAINAK SZABÁLYOZÁSA

Absztrakt

A honvédelmi szervezetek tevékenysége nem képzelhető el hatékonyan mobil kommunikációs megoldások alkalmazása nélkül. A vezetési és irányítási folyamatok, az üzemeltetési környezet, kommunikációs eszközök, különböző felhasználói igények, a kezelt adatok fontossága és bizalmassága olyan kulcsfontosságú tényezők, melyek jelzik ennek a kommunikációs formának – és szabályozásának – összetettségét.
Az említett tényezők mellett a rohamosan fejlődő technológia által biztosított szolgáltatások folyamatosan változó fenyegetés és sebezhetőségi hatások alatt állnak.
A honvédelmi tárca információ biztonságpolitika meghatározza az elektronikus adatkezelő rendszerek biztonsági felügyeletét, így célszerű egy rugalmas és strukturált szabályozást kialakítani a honvédelmi szervezetek széles körű tevékenységének biztonságos kommunikációs támogatása érdekében.

The activity of military units and different supporting organisations cannot be effective without the implementation of mobile communication solutions. The communication and controlling processes, the operating environments, the communication equipments, the different user requirements, and the importance and sensitivity of handled information are key factors which sign the complexity of this communication and its regularisation.
Besides the mentioned factors the new services provided by emerging technology have some impacts from the continuously changing known and hidden threats and vulnerabilities.
The Security Policy of Ministry of Defence requires security control of CIS's so it may be useful to create a flexible and structured set of controls for secure mobile communication supporting the wide scale of activities at military organisations.

Kulcsszavak: *biztonságpolitika, információbiztonság, információvédelem, informatika, mobil kommunikáció - security policy, information security, information protection, IT, mobile communication.*

BEVEZETÉS

A mobil kommunikációs eszközök alkalmazása egyre nagyobb szerepet játszik a honvédelmi szervezetek életében. Szolgáltatási lehetőségeinek sokszínűsége miatt a hagyományos szakterületi elkülönülés alapján nehéz eldönteni, hogy mobil IT szolgáltatáshoz vagy híradáshoz kell sorolni a mobil kommunikációs lehetőségek alkalmazását, ami már többet jelent mobiltelefonnál (korábban rádiótelefon), így helyesebb a címben fogalmazott „mobil kommunikációs eszköz" kifejezés használata.

Ezzel a kérdéssel részben foglalkozik a mobil telefonokkal való ellátásra vonatkozó utasítás [1.], minősített adatkezelés esetén a jogszabályban rögzített helyi szabályozási (biztonsági szabályzat) kötelezettség [2.][3.], de ezen kívül a honvédelmi tárcánál kifejezetten erre a területre vonatkozó specifikus szabályozás nincs. Kis irodalomkutatás után kijelenthető, hogy a közigazgatási szervezetekre vonatkozó kötelező hatályú központi követelmény (jogszabály) ebben a témában nem azonosítható.

A területre vonatkozó szabályozást célszerű a nemzetközi szabványokhoz igazítva kialakítani, melynek elemei a biztonság menedzseléséről szóló szabványok [4.][5.], és az ezek alapján készült nemzeti ajánlás [6.] vonatkozó részei. A szabályozás kialakításánál segítséget nyújtanak még a bevált gyakorlat (best practice) körébe tartozó kiadványok [7.][8.].

A fenti támogatás mellett a szabályozási alapot a biztonságpolitika adja, melynek általános irányelveit és követelményeit [9.] a mobil kommunikációs eszközök esetében is érvényesíteni kell.

A továbbiakban azon szempontok bemutatása látható, ami a felső szintű, keret jellegű szabályozás lényégét kifejezi. Az ehhez szükséges technológiától függő paramétereket, központilag meghatározandó műszaki részleteket szűkebb szabályozási hatályú belső rendelkezésben célszerű rögzíteni.

1. A SZABÁLYOZÁSI KÖR AZONOSÍTÁSA

A mobil kommunikációs eszközök használatával kapcsolatos alapelveket meghatározó szabályozásban a honvédelmi szervezeteknél a mobil eszközökkel történő kommunikáció és adatkezelés biztonságához szükséges irányelvek, általános követelmények kereteit kell meghatározni. A szolgálati mobil kommunikációs eszközöket a honvédelmi tárca információ biztonságpolitikában meghatározott biztonsági cél-, és az elérésére vonatkozó követelményeknek megfelelően kell alkalmazásba venni, konfigurálni, működtetni és felügyelni. A magántulajdonú mobil kommunikációs eszközök alkalmazását ugyanezen általános követelmények figyelembe vételével lehet engedélyezni.

A honvédelmi szervezeteknél biztonsági menedzsment eljárásokat, ellenőrzési feladatokat kell kialakítani a mobil kommunikációs eszközök felett. A védelmi rendszabályokat *a szolgálati mobil kommunikációs eszköz teljes életútján keresztül fenn kell tartani*. A mobil kommunikációs eszközök alkalmazásának engedélyezését, korlátozást, vagy tiltását az adott szervezet vezetőjének (vagy az általa megbízott személynek) a hatáskörében kell rendezni.

A honvédelmi szervezetek belső rendelkezéseiben *a helyi szabályozást a központi, keret jellegű követelményekkel összhangban kell kialakítani*. A külföldön szolgálatot teljesítő katonai szervezetek információvédelmi rendszabályait az említett központi-, valamint az illetékes elöljáró követelményei alapján kell kialakítani. A honvédelmi szervezetekkel

szerződéses kapcsolatban álló személyek esetében a központi követelmények érvényesüléséhez szükséges rendszabályok kialakításáról és fenntartásáról a honvédelmi szervezet vezetőjének kell gondoskodnia.

Ezen általános lehatárolás mellett szükség van meghatározására, hogy ehhez a kérdéshez kell sorolni *minden olyan eszközt, ami a mobil távközlési szolgáltatás mellett adatkezelésre (rögzítés, fájl kezelés) képes*. Nem tartozik a szabályozási körbe az EDR (Egységes Digitális Rendszer) eszközök igénybevétele, melynek üzemeltetési és biztonsági szabályozása önálló jogszabályban rögzített követelmények szerint történik.

2. SZABÁLYOZÁSI KÖVETELMÉNYEK

A honvédelmi szervezet vezetőjének a helyi sajátosságoknak és a végzett tevékenységnek megfelelően szabályoznia kell a mobil kommunikációs eszközökkel történő elektronikus adatkezelést. A szabályozás során azonosítani kell:

- a szolgálati mobil kommunikációs eszközhöz kötött, vagy magántulajdonú eszközzel is végezhető elektronikus adatkezelő műveleteket;
- a mobil kommunikációs eszköz használata szempontjából tiltott helyeket;
- a munkavégzés vagy rendezvények alatt alkalmazandó állandó vagy ideiglenes korlátozásokat, tiltásokat;
- azokat a szolgálati mobil kommunikációs eszközöket, melyek magántulajdonú kommunikációra vagy adatkezelésre nem alkalmazhatók;
- a mobil kommunikációs eszközök használatára vonatkozó rendszabályok betartása érdekében alkalmazott eljárásokat;
- a szolgálati kommunikációs eszközökkel kapcsolatos biztonsági incidensek megoldására szolgáló eljárásokat.

A mobil kommunikációs eszközök alkalmazásának engedélyezésekor figyelembe kell venni:

- az eszközök kommunikációs és adatkezelő képességeit;
- az engedélyezett mobil kommunikációs eszköz használat munkavégzésre irányuló hatását;
- az eszközök elvesztéséből, illetéktelen kezekbe jutásából adódó információs fenyegetéseket.

A fenti követelmények bonyolultnak tűnnek, de a valóság ennél egy kicsit egyszerűbb. A szervezet működéséhez szükséges *információs folyamatokat mindenképpen szabályozni kell*, az tehát nem lehet újság, hogy ebbe az is beleértendő, hogy *mit lehet, és mit nem lehet mobil kommunikációs eszközzel végezni*. Ugyanígy nem lehet meglepő az sem, hogy *a szervezet szabályozza azt a lehetőséget, hogy az egyre korszerűbb eszközök esetében fokozottan jelentkező információs fenyegetések ellensúlyozására milyen magántulajdonú eszközökre vonatkozó korlátozást vezet be*.

Fontos kérdés annak tisztázása is, hogy a mobil kommunikációs eszközzel történő ellátásért felelős vezetőnek *szabályoznia kell a szolgálati mobil kommunikációs eszköz fenntartásával kapcsolatos feladatokat is*. Ez azt jelenti, hogy a korábban csak kiosztott és használt eszköz napjainkban már gyakran *szoftveres karbantartást igényel, melyet bonyolultságtól függően szükséges szakértői szinten támogatni*.

A továbbiakban azok az általánosan megfogalmazható kontrollok olvashatók, melyek áttekintésével, helyszínhez és munkavégzéshez történő igazítással a szabályozási elemek pontosan kialakíthatók.

3. ÁLTALÁNOS ALKALMAZÁSI KÖVETELMÉNYEK

A szolgálati mobil kommunikációs eszköz alapesetben csak szolgálati kommunikációra és adatkezelésre alkalmazható. Általános szabályként célszerű kitűzni, hogy *szolgálati eszköz kölcsön nem adható, illetve más személy részére a hozzáférés nem biztosítható*; a kivételeket átgondoltan, pontosan meg kell határozni. A szolgálati mobil kommunikációs eszközzel az előfizetői szolgáltatáson keresztül történő egyéb szolgáltatás fizetését vagy megrendelését tiltani kell (pl. autópálya matrica, adományozás). Meg kell vizsgálni, hogy melyek azok az esetek, amikor a szolgálati mobil kommunikációs eszköz szolgáltatásai magántulajdonú eszközre nem irányítható át (illetve egyes esetekben célszerű megfontolni az általános tiltást). Magántulajdonú eszköz szolgáltatása szolgálati mobil kommunikációs eszközre abban az esetben irányítható át, ha:

- a felhasználó munkavégzése közben a mobil kommunikációs eszköz használat nem tiltott;
- az adott szolgálati mobil kommunikációs eszközön a magán célú kommunikáció vagy adatkezelés nem tiltott.

Általános, mindenki által érthető követelménynek kell megjelennie arra vonatkozóan, hogy *a szolgálati mobil kommunikációs eszköz, az eszközön tárolt adatok az üzemeltetésért felelős honvédelmi szervezet vagy a felhasználó szerint illetékes munkaadó honvédelmi szervezet vezetője által meghatározottak szerint ellenőrizhető*. Ez a követelmény a közhiedelemmel ellentétben nem zavarhatja a személyes adatok védelmét, mert a szolgálati célú adat, vagy eszköz egyértelműen szervezeti célt szolgál, így az ezzel kapcsolatos híváslisták, egyéb üzemeltetési adatok szintén a szolgálati tevékenység részét képezik. Az esetleges engedélyezett magán használat és a szolgálati használatból adódó keveredés (az a tény, hogy az ellenőrzés személyes adatokat is feltárhat) könnyen kivédhető, mert a magáncélú használat nem kötelező, csak engedélyezhető (tehát csak lehetőség), így egyéni aggály esetén a védelem egyszerű: kerülni kell a magáncélú használatot.

A szolgálati mobil kommunikációs eszköz csak az üzemeltető által rendelkezésre bocsátott konfigurációban, kiegészítő elemekkel és alkalmazásokkal üzemeltethető. A felhasználónak tilos:

- az eszköz felügyelet nélkül hagyása;
- az eszköz vagy kiegészítőjének kezelői szintű szétszerelését meghaladó mértékű szétszerelése, vagy kiegészítése;
- az előfizetői kártyát vagy memóriát más eszközben alkalmazni;
- magántulajdonú kártyát vagy memóriát az eszközbe helyezni vagy arról adatot feltölteni;
- olyan üzemmódot vagy beállítást alkalmazni, melynek eredményeképpen honvédelmi vezetékes vagy vezeték nélküli kommunikációs rendszer internethez, más nyilvános hálózathoz, esetleg magáncélú hálózathoz csatlakozik.
- az eszköz alkalmazása során a meghatározott védelmi rendszabályok megkerülése vagy kiiktatása.

Szolgálati mobil kommunikációs eszközzel magáncélú kommunikáció vagy adatkezelés csak az engedélyezett mértékben és formában végezhető *a szolgálati cél elsődlegességének figyelembe vételével*. A felhasználónak tudomásul kell vennie, hogy:

- a felhasználó a felhasználói engedély korlátozása vagy visszavonása esetén a magántulajdonát képező adatot azonnal köteles törölni vagy eltávolítani, mely tevékenység nem akadályozhatja a szolgálati mobil kommunikációs eszköz használatát;
- az engedélyezett magáncélú adatokban keletkezett sérülésért vagy adatvesztésért az üzemeltető nem vállal felelősséget.

Szolgálati tevékenységhez szükséges kommunikáció vagy adatkezelés magántulajdonú, vagy más szervezet tulajdonában lévő eszközzel csak engedéllyel végezhető.

Szolgálati mobil kommunikációs eszköznél automatikus hang vagy adatszolgáltatás beállítása esetén csak olyan adat alkalmazható, *melynek a hívó fél tudomására jutása nem sért szolgálati érdeket*.

Szolgálati kommunikáció vagy adatkezelés más szervezet tulajdonában lévő eszközzel csak az alábbi feltételek együttes fennállása esetén végezhető:

- szolgálati mobil kommunikációs eszköz hiánya;
- a kommunikáció vagy adatkezelés során az adatok biztonsági osztályához rendelt védelmi rendszabályok biztosíthatók;
- a szolgáltatás megszűnése esetén a hívásadatok, felhasználói adatok törlése és szükség szerint mentése biztosított.

A felhasználónak a szolgálati mobil kommunikációs eszköz felügyelet alatt tartásával biztosítania kell a kezelt adatok bizalmasságát-, az eszköz eltulajdonításának megakadályozását-, az eszköz, illetve az eszközbeállítások módosításának elkerülését-, a nem kívánt szolgáltatások aktivizálásának megakadályozását-, és a szolgáltatások alkalmazásával kapcsolatos visszaélések elkerülését.

Az alkalmazással kapcsolatos felhasználói és biztonsági ismereteket a honvédelmi szervezet képzési rendje szerinti *időszakonként oktatni kell*. Az oktatás más foglalkozásokkal összevonható. A távollévők számára pótfoglalkozást kell szervezni.

A fenti szabályozási elemek *nem tartalmaznak végrehajthatatlan követelményeket, esetleg korábbi felhasználói szokásokkal kerülhetnek összeütközésbe*. A szabályozás vezérfonala *a szolgálati tevékenységhez szükséges kommunikáció és adatkezelés elsődlegességének biztosítása, illetve a magán és a szolgálati használat (illetve magán és szolgálati adat) elkülöníthetőségének biztosítása*.

4. ÁLTALÁNOS VÉDELMI RENDSZABÁLYOK

Az előző fejezetben meghatározott, inkább az alkalmazásra vonatkozó szabályozás mellett szükség van az általánosan megfogalmazható rendszabályok azonosítására, melynek specifikálásával már eszköz és szolgáltatás függően részletes védelmi rendszabályok dolgozhatók ki (az itt azonosított, nem teljes körű lehetőségeket szükség esetén eszközcsaládhoz vagy szolgáltatáshoz illesztve tovább lehet pontosítani és tartalom függvényében meghatározott szintű belső rendelkezésben kiadni).

A felhasználónak a szolgálati mobil kommunikációs eszközt és a szolgáltatás igénybevételére jogosító SIM kártyát, valamint az adatok tárolására alkalmas memória kártyát azonosító kód használatával kell védenie az illetéktelen hozzáféréstől. Ennek érdekében az eszköz használatbavételekor a felhasználónak meg kell változtatnia a rendelkezésére bocsátott kódokat. A felhasználó nem használhat a szolgálati mobil kommunikációs eszközhöz és egyéb számítógépéhez megegyező azonosító kódot. Jelszavas védelmi lehetőséggel rendelkező memória kártyákat csak az azonosítási funkció aktivizálásával lehet üzemeltetni.

Az egyes alkalmazások véletlenszerű elindításának megakadályozása érdekében a felhasználók kötelesek billentyűzárat (manuális vagy automatikus) használni.

Azon szolgálati eszközök esetében, ahol adatvesztés nem engedhető meg, *rendszeres időközönként az eszköz hardver és szoftver lehetőségei szerint kialakított mentést kell végezni*. A mentési eljárást szabályozni kell. Az adatmentés megvalósítható:

- számítógéppel történő mentéssel vagy szinkronizálással;
- adathordozóra történő mentéssel;
- nyomtatással.

Mobil kommunikációs eszköz hálózati számítógéppel történő összekapcsolása, illetve szinkronizálása csak:

- engedélyezett program alkalmazásával, arra kijelölt számítógéppel történhet;
- célszerűen csak naptár, jegyzet adatokra és SMS-re korlátozódjon (az adatok másolását, illetve tárolását egyedi esetekre külön-külön vizsgálni kell, és csak célhoz kötötten lehet engedélyezni).

A teljes címtárral, adatbázissal történő szinkronizálást tiltani kell. *A mobil kommunikációs eszköz szinkronizálásához szükséges telepítéseket, biztonsági beállításokat csak az arra kijelölt, kiképzett rendszeradminisztrátor végezheti*. Az adatmentésre feljogosított felhasználókat az adatmentéssel kapcsolatos műveletekre ki kell képezni.

Memóriakártyára, vagy más adathordozóra történő mentés esetén a mentett adatokat a szolgálati mobil kommunikációs eszköztől elkülönítve, a biztonsági osztálynak megfelelően kell tárolni, illetve védeni.

A szolgálati mobil kommunikációs eszközökön *alkalmazni kell a biztosított logikai védelmi alkalmazásokat, magasabb biztonsági osztályú adat esetén az eszköz sajátosságainak megfelelő kiegészítő szoftveres védelmet kell alkalmazni*.

A memóriakártyákat a használatból történő kivonáskor a visszaállítás és elemzés megakadályozása érdekében az adatok bizalmasságával arányos törlési eljárásokat kell alkalmazni. *Törlésre csak engedélyezett eljárások alkalmazhatók*, ennek hiányában fizikai megsemmisítést kell alkalmazni.

A csatolt fájlokban, üzenetekben lévő rosszindulatú programok elleni védelem érdekében *az ismeretlen forrásból eredő üzenetek esetén a vírusvédelmi rendszabályok szerint kell eljárni*. Vett üzenetek esetében a végrehajtandó utasítások aktivizálása a felhasználó által tilos.

A mobil kommunikációs eszközök által kezdeményezett ismeretlen program telepítésének engedélyezése tilos.

Az ismeretlen forrás felől érkező vezeték nélküli interfész csatlakozási kérelmet tilos engedélyezni. Nem azonosított, nem megbízható forrásból származó adat letöltése és telepítése tilos.

Az automatikus adatátviteli szolgáltatásokat a szolgálati mobil kommunikációs eszközökön ki kell kapcsolni.

A vezeték nélküli interfészeket alaphelyzetben kikapcsolt állapotban kell tartani és csak a szükséges időtartamra lehet bekapcsolni. A vezeték nélküli interfészen keresztüli láthatóságot alaphelyzetben le kell tiltani. Amennyiben az eszköz típusa lehetővé teszi, olyan beállítást kell alkalmazni, ami jelzi a vezeték nélküli interfészen keresztül érkező csatlakozási kérelmet. A vezeték nélküli interfészen keresztüli kommunikáció engedélyezése során az eszköz rendelkezésre álló jelszavas azonosítási szolgáltatását alkalmazni kell.

A vezeték nélküli interfészen keresztüli kommunikáció során kerülni kell azokat a nyilvános helyeket, ahol feltételezhető az adatcsere más eszköz által történő vétele. Amennyiben az eszköz vezeték nélküli interfészének energia szintje szabályozható, a lehető legkevesebb energiaszintet kell alkalmazni.

Az ellopott, vagy elvesztett szolgálati mobil kommunikációs eszköz jelentésére és a szükséges azonnali teendők meghatározására a honvédelmi szervezeteknél eljárást kell kialakítani.

Amennyiben a szolgálai mobil kommunikációs eszköz lehetővé teszi, *alkalmazni kell az eszköz szolgáltatásból történő kizárására, zárolására vagy tartalomtörlésre biztosított távoli elérési szolgáltatásokat*. Az ilyen programok telepítése előtt teszteléssel meg kell, győződni a szolgáltatás működőképességéről, illetve arról, hogy a szolgáltatás nem megkerülhető.

A szükségtelen beállításokat a konfigurációs beállításokon keresztül le kell tiltani, vagy amennyiben az eszköz tulajdonságai lehetővé teszik, el kell azokat távolítani. A szolgáltatók által rendelkezésre bocsátott kiegészítő szolgáltatások engedélyezése előtt *meg kell vizsgálni, hogy a változás milyen új fenyegetést és sebezhetőséget hordoz, és azok ellensúlyozására milyen védelmi rendszabályt kell alkalmazni*.

Amennyiben a szolgálati feladatok ellátása nem kíván internet hozzáférést, a szolgálati mobil kommunikációs eszközre csak hang és SMS szolgáltatást célszerű engedélyezni.

5. SPECIÁLIS ALKALMAZÁSI KÖVETELMÉNYEK

I. vagy II. osztályú biztonsági területre általános esetben mobil kommunikációs eszköz nem vihető be. A korlátozást a biztonsági területre történő belépés előtt közölni kell a látogató személyekkel.

Amennyiben szolgálati feladatok ellátása célhoz kötötten biztonsági területen mobil szolgálati kommunikációs eszköz bevitelét vagy alkalmazását követeli, az eszköz alkalmazásával kapcsolatos részletes szabályokat ki kell dolgozni:

- a biztonsági területre vonatkozó biztonsági szabályzatban;
- a biztonsági területen belül alkalmazott elektronikus adatkezelő rendszerek rendszer-specifikus biztonsági dokumentumaiban.

A minősített adatokat is feldolgozó rendezvényen a mobil kommunikációs eszközök alkalmazásával kapcsolatban szabályozni kell:

- a mobil kommunikációs eszköz használatára engedélyezett területeket;
- a mobil kommunikációs eszköz beviteli tilalma esetén a tárolásra, őrzésre, visszaszolgáltatásra vonatkozó eljárást.

Azon biztonsági területek, adminisztratív zónák, vagy egyéb helyek esetében, ahová mobil kommunikációs eszköz nem vihető be, a rendszabályt meghatározónak gondoskodnia kell:

- a rendszabály látogatók által történő megismeréséről;
- az eszközök biztonságos tárolásáról.

Amennyiben a rendezvényre vonatkozó biztonsági követelmény technikai védelmet is meghatároz, a zavarásra, detektálásra vonatkozó eljárásokat:

- célhoz kötötten, a szükséges mértékre korlátozva-,
- a rendezvényen kívüli kommunikációs szükségletek figyelembe vételével kell kialakítani.

Szolgálati mobil kommunikációs eszköz honvédelmi szervezet vagy más szervezet tagja számára történő kiutalása, biztosítása *csak célhoz, feladathoz kötötten szolgálati célból történhet*. Kiutalásra csak olyan eszköz kerülhet, melyből a korábbi felhasználás során keletkezett napló, forgalmazási, cím, vagy tárolt felhasználói adatok törlése megtörtént.

Minősített adat mobil kommunikációs eszközzel történő kezelése *csak az illetékes hatóság által engedélyezett eszközzel és védelmi megoldások alkalmazásával történhet.*

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A mobil kommunikációs eszközök használatának alkalmazása és felügyelete a fentiekben bemutatott keretrendszer szerint nem túl bonyolultan szabályozható.

Az ajánlott szabályozási elemek pontosítása alapján a honvédelmi szervezeteknél első lépésként annak meghatározására van szükség, hogy *mely helyszíneken van szükség és milyen mértékű korlátozás bevezetésére*, illetve *annak meghatározására, hogy a szolgálati adatok védelme érdekében milyen rendszabályok alkalmazása szükséges (pl. elkülönítés vagy korlátozás).*

Az üzemeltetési helyszínek mellett egyedileg azonosítani kell azokat az eszközöket, melyek esetében szigorúbb rendszabályokra van szükség. Belátható, hogy egy ügyeleti szolgálatot támogató eszköz esetében más eljárásokat kell életbe léptetni, mint a beosztáshoz köthető normál alkalmazás esetében.

Kulcsfontosságú a tájékoztatás és a pontos, félreérthetetlen megfogalmazás, és annak megértetése, hogy *a személyes adatok védelmére hivatkozva nem lehet a szolgálati adatok védelmét háttérbe szorítani, vagy mellékesként kezelni.*

A téma általános szabályozása során az egyik legfontosabb kérdés, hogy a túl szűkre szabott szabályozás, vagy egy technológiához, megoldáshoz köthető követelmény nagyon könnyen alkalmazási, vagy üzemeltetés-támogatási problémákat okozhat. Formailag a bemutatott keret jellegű szabályozás a szükséges pontosítások és egyeztetések után történhet miniszteri utasítással hatályba léptetett szabályzat részeként, vagy önállóan kiadott miniszteri utasítással. E mellett szükség van az üzemeltetés szabályozásának áttekintésére is, valamint

célszerűnek látszik egy lépéssel tovább haladva a különböző képességekkel rendelkező hordozható számítógépekkel kapcsolatos eljárásrendet is pontosítani, a helyi szabályozások központi támogatása érdekében.

Egy ilyen szabályozási keretrendszer nem tekinthető tökéletesnek és véglegesnek, így *az időszakos felülvizsgálat, illetve új szolgáltatások, technikai megoldások megjelenése esetén szükség van a felülvizsgálatra és a pontosításra*. Az esetleges hiányosságok lefedésére irányuló adatgyűjtés támaszkodhat a szakmai továbbképzésekre, a helyi képzésekre, vagy a tanfolyam rendszerű képzésekre.

FELHASZNÁLT IRODALOM

[1.] 64/2007 (HK 12.) HM utasítás 64/2007. (HK 12.) HM utasítás a szolgálati rádiótelefon-ellátás és használat szabályairól, 3. §.

[2.] 90/2010. (III. 26.) Korm. rendelet a Nemzet Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 58-59. §.

[3.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 59. §.

[4.] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, A melléklet, A 10. 8. 1. p. és 11.7.1. p

[5.] MSZ ISO/IEC 17799: 2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2005), 10.8.1. p és 11. 7. 1. p.

[6.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, 10.8.1. p és 11. 7. 1. p.

[7.] The Standard of Good Practice for Information Security; Information Security Forum (ISF), 2007, UE4. 4.2. p, SM 5.2. 5.2.2. p. SM 5.3. 5. 3. 6. p.

[8.] Guidelines on Cell Phone and PDA Security (SP 800-124), National Institute of Standards and Technology (NIST), 2008

[9.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Koleszár Béla
koleszar@tele2.at

ROBOTER-PLATTFORMEN FÜR RISIKOMINIMIERUNG BEI MILITÄRISCHEN FRIEDENSEINSÄTZEN

Absztrakt/Abstract/Abstrakt

A szerző a szárazföldi járművek robbanásvédelmével foglalkozik, a műszakilag kivitelezhető rizikó/veszteségcsökkentés lehetőségeit kutatja. Röviden megemlíti az IED-k elleni aktív védelmek és elektronikai zavaróadók alkalmazását. Ezt követően taglalja a járművek passzív védelmének problematikáját. A szerző szerint – az aszimmetrikus fenyegetettségek miatt – elhamarkodottan nem szükséges minden járművet lecserélni a magas MRAP járművekre. Számolni kell új (ill. régi) veszélyekkel is. Javaslatot tesz a valós méretű robotjárművek fokozottabb bevetésére, felsorolja a szárazföldi robotjárművek előnyeit és hátrányait. Megfogalmazza a robotplatformok fejlesztéséhez szükséges követelményeket. Szorgalmazza a légi-, ill. földi robotok szorosabb együttműködését. Bemutat egy, a légi robotok számára szolgáló startoló- dokkoló állomást – egy robotrepülőgép-hordozót.

The author developed technical means to protect human life, exploring feasible solutions for the explosion resistance of vehicles. He refers to the borders of active protection and electronic jammer against roadside explosive devices. He describes passive protection on vehicles. According to the author it is not necessary – because of asymmetric threat – to hastily exchange all vehicles for high MRAP vehicles. We must also reckon with new (and old) threats. He suggests an increased use of full size robotic vehicles, and lists the advantages and disadvantages of ground robots. He formulates the requirements for the development of robotic platforms. He recommends greater collaboration between air and ground robots. He presents a launcher-docking station for the flying robots – a "robotic aircraft carrier".

Autor beschäftigt sich mit der Entwicklung vom Sprengschutz an militärischen Fahrzeugen, er forscht technisch durchführbare Möglichkeiten für die Risikosenkung/Verlustreduzierung. Erwähnt kurz die Anwendung von aktiven Schutz und elektronischen Störsendern gegen IED. Nachfolgend wird die Problematik von passivem Schutz an Fahrzeugen beschrieben. Laut Autor ist es nicht nötig – wegen asymmetrischer Gefahr – mit überstürzter Eile alle Fahrzeuge für hohe MRAP Fahrzeugen auszutauschen. Wir müssen auch mit neuen (und alten) Gefahren rechnen. Er schlägt einen vermehrten Einsatz von Roboterfahrzeugen mit realen Größen vor und listet die Vorteile und Nachteile

von Bodenrobotern auf. Formuliert die Anforderungen für die Entwicklung von Roboterplattformen. Empfiehlt eine verstärkte Zusammenarbeit von Flug- und Bodenrobotern. Er präsentiert eine Start-Dockstation für die Flugroboter – einen „Roboterflugzeug-Träger".

Kulcsszavak/Keywords/Schlüsselworte: *asymmetrische Bedrohung, aktiv-passiver Schutz, unbemannte Fahrzeug-Plattformen, Roboterflugzeug-Träger ~ asymmetric warfare, active-passive protection of vehicles, unmanned vehicle platforms, robotic aircraft carrier ~ aszimmetrikus fenyegetetés, aktív-passzív védelem, személyzet nélküli jármű platformok, robotrepülőgép-hordozó*

1 EINLEITUNG

Seit 14 Jahren arbeite ich als Konstrukteur von Spezialfahrzeug- Baugruppen (GDELS[1]-Steyr, in Wien). Parallel bin ich Doktorand am ZMNE[2] in Budapest seit 3 Jahren. Das von mir ausgewählte Thema: „*Konstruktions- und Einsatzfragen von unbemanntem Bodenfahrzeugen, mit besonderem Hinblick auf Sicherheitserhöhung von Friedensmissionen"* forsche ich von verschiedenen Gesichtspunkten, und nehme an Veranstaltungen in diese Richtungen aktiv Teil. Meine bisherigen wissenschaftlichen Publikationen und Vorträge wurden in ungarischer (resp. eine in slowakischer) Sprache veröffentlicht und gehalten. [1-12] In diesem Artikel versuche ich über meine Forschungstätigkeiten in deutscher Sprache eine Übersicht zu bieten.

2 JETZIGE SITUATION

Für die internationalen Friedensmissionen ausreichend sichere Länder sind wegen derzeitigen asymmetrischen Bedrohungen immer seltener. Wo „Kalaschnikows" erreichbar sind, dort können wir das Auftauchen von Panzerabwehrwaffen, die von der Schulter bedienbar sind erwarten, wie zum Beispiel die in drei Teile zerlegbare RPG-7[3]. Bei Straßen- und Gebirgskämpfen nach Stein-, Molotow Cocktails-, respektive Faustfeuerwaffen- Bedrohungen wird die nächste logische ballistische Bedrohungsstufe wahrscheinlich die „RPG-7" Stufe sein.
Auch der Schutz gegen einzeln verlegten Blastminen[4] (mit 6, 8, 10… kg Sprengstoff) ist nicht immer ausreichend. Bei Patrouillen müssen wir mit mehreren, übereinander verlegten einfachen Minen, oder mit der Verlegung von Richtminen, meist seitlich wirkenden EFP[5]-s rechnen. Zeitverzögerte und ferngesteuerte, selbstgebastelte Sprengsätze -IED[6]-s, und „Autobomben" bedeuten auch große Gefahr. Wir müssen auch mit vermehrten Angriffen von oben, von Gebäuden, Brücken über Straßen, Bergen, aus der Luft rechnen. Vermehrt sind Flugkampfrobotern im Einsatz, immer mehr zielsuchende Munitionen sind eingeführt.
Bei der Entwicklung von Kampffahrzeugen sind die Anforderungen für die Sicherheit immer schärfer und es ist immer schwieriger entsprechende Lösungen zu finden. Einerseits benötigen wir ausrechenden ballistischen Schutz, bzw. so gut wie möglichen Schutz gegen

[1] GDELS- General Dyanamics European Land Systems
[2] ZMNE- Zrínyi Miklós Nemzetvédelmi Egyetem - Zrínyi Miklós Militärakademie /-Universität Budapest
[3] RPG-7 Die Abkürzung steht für *rutschnoi protiwotankowy granatomjot*, kyrillisch *ручной противотанковый гранатомёт*, zu Deutsch etwa Granatwerfer zur Panzerabwehr, der von Hand abgefeuert werden kann. Das englischsprachige "*R*ocket-*P*ropelled *G*renade" ist ein Backronym. [14]
[4] Schutzstufen nach NATO AEP-55 STANAG 4569 Annex B
[5] EFP- Projektilbildende Ladung, Abkürzung für den englischen Begriff **E**xplosively **F**ormed **P**rojectile, auch **E**xplosively **F**ormed oder **F**orged **P**enetrator. [15]
[6] IED- **I**mprovised **E**xplosive **D**evices ~ Improvisierte Spreng- und Brandvorrichtungen [16]

Minen und improvisierten Sprengvorrichtungen. Andererseits können wir die hochgradige Mobilität und die Geländegängigkeit unserer Fahrzeuge nicht verschlechtern. Für die Erfüllung der Friedensmissions-Aufgaben und das Bekämpfen von schnell aufflammenden lokalen Konflikten, brauchen wir statt schwerer Bewaffnung eher luftverlastbare Kampffahrzeuge. Für die **strategische Mobilität** ist es sehr wichtig eine Fahrzeugkategorie, die mit in NATO Armeen verbreiteten C-130 Hercules [13] Flugzeugen noch transportierbar sind. Das bedeutet ungefähr 20 t Gesamtgewicht mit begrenzter Fahrzeugbreite und -höhe. Bei amphibischen (schwimmenden) Fahrzeugen müssen wir noch zusätzlich die sichere Verdrängung (ausreichende Auftriebskraft) berücksichtigen. **Überlebensfähigkeit, Gesamtgewicht, Manövrierfähigkeit** sind Gesichtspunkte, welche nur mit Kompromissen verbesserbar sind, zum Nachteil von anderen Parametern.
Neuentwicklungen mit viel höherem Schutz (z.B. Mannschaftstransporter Nakpadon – geschützt gegen 150 kg Sprengladung [17] sind sehr schwer, Luftverlastbarkeit mit üblichen Transportflugzeugen ist nicht mehr möglich. Neuer Schützenpanzer PUMA ist nur ohne Zusatzpanzerung im geplanten A 400M transportierbar (max. 31,5 t). [18]
MRAP[7] Fahrzeuge können wir als „Zweckmaschinen“ gegen irakische und afghanische Bedrohungen nennen. Die Größe deren Silhouetten haben eine ähnliche Größe zu den Silhouetten von Autobussen. Geländegängigkeit (vor allem bei 4x4 Fahrzeugen) ist nicht sehr gut – außerhalb von befestigten Straßen (Sand, Schnee, nasse Wiese, weiches und tiefes Boden – z.B. Acker) – die Gefahr von Wegrutschen, „Einsinken“ ist groß. Tragfähigkeit der bestehenden, oft veralteten und durch Kampfmitteleinwirkung beschädigten Brücken in Einsatzgebieten ist zusätzlich ein einschränkender Faktor. Ein unüberlegte Austausch von ganzen Fahrzeugflotten auf diese Fahrzeugkategorie wäre nicht sinnvoll. Wir müssen auch mit neuen (eventuell alten) Gefahren rechnen.

3 INDIREKTER, DIREKTER, AKTIVER, PASSIVER SCHUTZ

Indirekter Schutz: *„Schutz ist heute vielmehr als räumlich und zeitlich weit gefasstes System zu begreifen. Auf einen Zeitstrahl projiziert, darf Schutz nicht erst im Moment des Treffers wirksam werden, sondern muss vielmehr auf die Rahmenbedingungen einwirken, um eine Bedrohung bereits im Vorfeld zu unterdrücken und ihr die Grundlage ihrer Entstehung zu entziehen.“* [19]
Direkter Schutz richtet sich gegen die Gefahr selbst, kann aktiv und passiv sein.
Fahrzeuge zu verbessern, werden immer mehr **aktive Schutzsysteme** eingeführt. **Soft-Kill-Systeme** (Nebelwerfer, IR-Jammer, usw.) sind gut, aber haben ihre Grenzen. Mobile Störsysteme gegen elektronisch ausgelösten Sprengfallen sind umgekehrt abhängig von der räumlichen Anordnung (Entfernungen) von Sender-Auslöser-Störsender Einheiten. [20]
Bei kombinierten Zündungen versuchen die Attentäter die ferngesteuerten Einheiten außerhalb der Reichweite von Störsendern zu verlegen. Gegen die primitivste Auslösung (mechanische Schalter, Zündschnur, direkter Draht, usw.) bieten Störsender überhaupt keinen Schutz!
Ziel von **Hard-Kill-System**-en (AwiSS, ARENA, Iron Fist, LEDS, u.a.) ist in einer Richtung fokussierten kinetischen, oder kumulativen Energie - z.B. in einem Geschoß inkludiert - vorzeitig zu initiieren, zu zerstreuen (auslenken, abscheren). Leider sind diese Systeme extrem zeitkritisch, können auf Gefahren in unmittelbarer Nähe nicht rechtzeitig reagieren. Gegen schon ausweitende „dumme“ Detonationswellen sind sie praktisch wirkungslos. Grundsätzliches Problem ist im urbanen Gelände, dass sie wegen der kurzen Kampfentfernung keinen ausreichenden Schutz gegen RPG-7 und EFP bieten. Eventuelle Kollateralschäden bedeuten auch ein Problem.

[7] MRAP - **M**ine **R**esistant **A**mbush **P**rotected ~ Minensichere und vor Hinterhalten geschützte (Fahrzeuge)

Passiver Schutz: *„Es ist unmöglich, das gesamte Fahrzeug zu panzern, weil Motoren und Fahrgestelle nicht für derartige Zusatzbelastungen ausgelegt sind, außer man verzichtet auf Nutzlast.“* [17] Wenn wir versuchen unser Fahrzeug gegen alle erwarteten Gefahren zu schützen, wenn wir die strengen ballistischen, Sicherheits-, ABC-, Feuerunterdrückungs-, ergonomischen, psychischen, usw. Anforderungen berücksichtigen, wird das Fahrzeug immer schwerer… Mit der Verwendung von neuen Materialen können wir zwar Gewichtreduktionen erreichen, aber nur zwischen gewissen finanziellen Grenzen.
Bei einem kleinen Fahrzeug ist der Schutz der ganzen Fahrzeugwanne und des Aufbaus gegen RPG-7 und deren Folgenvarianten unmöglich. Passive Gefechtkopfabwehr („Käfig“, Drahtgeflecht) gegen klassischen RPG bietet nur knapp über 50 % Schutz. Gegen neueren Panzerabwehrwaffen noch weniger… IED-, Sprengladung- und EFP- Sicherheit ist auch kritisch.
„Ewiger Wettlauf zwischen Bedrohung und Schutz auch bei Panzerfahrzeugen schreitet weiter fort. „Aber auch Gefechtsfahrzeuge, die mit den derzeit modernsten Schutzsystemen ausgestattet sind, haben gegen die "Super-IEDs" kaum Chancen.“ [17]
Als Militärfahrzeug-Konstrukteur habe ich manchmal das Gefühl, dass ich in eine Sackgasse geraten bin… Einen realen Ausweg sehe ich mit vermehrter Anwendung von Bodenrobotern. Die Verletzungsgefahr von Menschen ist nur mit der Anwendung von Robotern hundertprozentig ausschließbar.

4 MILITÄRISCHE EINSATZ VON ROBOTERN

Aufklärung und Räumung von Minen und anderen Kampfmitteln, Entschärfungsroboter, UAV[8], UAS[9], Kampfdrohnen sind moderne und immer öfter zitierte Wörter und Abkürzungen. UGV[10] -s sind noch nicht so gut bekannt, aber in der nahen Zukunft können wir mit erhöhtem Einsatz auch von größeren Boden-Robotern rechnen.
Derzeit gehen die meisten Roboterentwicklungen [21] in die Richtung Miniaturisierung, was ihre Verwendungsmöglichkeiten beschränkt. Vor allem die Nutzlastbegrenzung bedeutet ein Problem. Mit der Verkleinerung verschlechtern sich die Geländegängigkeit und die Geschwindigkeit, Reichweite wird kürzer, es gibt zu wenig Platz für den Einbau von Qualitätssensoren, wegen schwachem Schutz genügt ein „größerer Stein“, eine Antipersonenmine, und die Mission kann gefährdet sein. Von positiven Wirkungen bei der Anwendung von kleinen Kampfrobotern in Irak und in Afghanistan haben wir viele Beispiele gesehen. Eindringen mit Robotern in Gebäuden, Höhlen, Aufspürung und ferngesteuerte Vernichtung von Sprengmitteln haben sehr viele Menschenleben geschont, das diskutiert niemand weg. Konvoibegleit- und Schutzaufgaben benötigen andere Roboter-Kategorie, welche echtgroßen Kampffahrzeugen ähnlich sein könnten.

Wenn wir die Missions-Aufgaben untersuchen, sehen wir, dass die Besatzung großteils für die Fahrzeug-Führung und für den Schutz und die Verteidigung von mitgeführten Lasten nötig ist. Die meisten inneren Einrichtungen von Kampffahrzeugen sind für den Lebenserhalt der Fahrzeugbesatzung, wie z.B. Ergonomie, ABC- und Feuerschutz zu schaffen. Würde man ohne Fahrzeugbesatzung auskommen, wäre eine ganze Reihe von teuren Systemen unnötig. Die Nutzlast könnte höher sein und bei einem (über-) schweren Angriff könnten wir personelle Verluste reduzieren/verhindern. Diese Überlegungen eröffnen uns einen neuen Horizont. Anstatt bisheriger Fahrzeugbesatzung könnten wir **autonom**e, **teilautonom**e, **ferngesteuert**e Maschinen – **Robotern** einsetzen. Diese Überlegungen Untersuche ich anschließend detaillierter.

[8] UAV- **U**nmanned **A**erial **V**ehicle = unbemanntes Luftfahrzeug
[9] UAS- **U**nmanned **A**ircraft **S**ystem = Gesamtsystem für UAV-s
[10] UGV- **U**nmanned **G**round **V**ehicle = unbemannte Bodenfahrzeug

In den Kolonnen wäre es genügend z.B. nur in jedem vierten Fahrzeug eine sehr gut geschützte, hochgepanzerte, innere „Kapsel“ für vier-sechs Personen einzubauen. Aus diesen könnten das eigene, weitere drei Fahrzeuge und ihre Waffensysteme gesteuert werden. Von außen betrachtet schauen alle Fahrzeuge gleich aus, der äußere Beobachter weiß es nicht, welche bemannt und unbemannt sind.

Die ganze Nutzlast vom Führungsfahrzeug ist für die Kapsel-Panzerung verbraucht. In den weiteren drei ferngesteuerten Roboterfahrzeugen kann wegen Weglassen von Bedienungspersonal die Nutzlast von „spartanischen“ – äußerst vereinfachten – Fahrzeugen sogar verdoppelt werden. So können die logistischen Transportfahrzeuge viel mehr Material zum Ziel bringen, Kampfahrzeuge können wir mit viel effizienteren Waffensystemen ausstatten, resp. Munitionsvorrat erweitern, usw. Das Ganze bei wirksamem Schutz von Bedienungspersonal.

Mit Fernsteuerung – ähnlich wie bei unbemannten Drohnen – sind die Einsatzdauer von (Fern-) Operatoren und die Einhaltung gesetzlicher Auflagen wie Lenk- und Ruhezeiten besser steuerbar.

5 BODENROBOTER STATT BEMANNTER MILITÄRFAHRZEUGE?

Implementiert (teilweise ergänzt) nach der SWP[11] Studie von Sascha Lange: „Flugroboter statt bemannter Militärflugzeuge? [22] In Telegrammstil:

Problemstellung und Empfehlungen
- ohne das Leben von Besatzung aufs Spiel zu setzen
- eine weitgehende Ablösung bemannter Systeme
- stufenweise Einführung unbemannter Systeme
- multinational beschafft und betrieben

Die neuen Bodenroboter
- völlig neue Einsatzmöglichkeiten
- für Menschen zu ermüdend und zu gefährlich, über viele Tage
- hohe Stehzeit – Gegner dauerhaft unter Bedrohung halten zu können
- stationäre Überwachungs- „Posten/Warten“
- künftig wesentlich schlagkräftigere Waffenanordnungen umfassen
- geringeres Risiko personeller Verluste
- Kosten bei den Streitkräften zu senken
- durch zunehmende Automatisierung und Anonymisierung das Kriegsbild immer mehr in Richtung ferngelenkter ziel- und zeitgerechter Zerstörung (Destruction on Demand) verändern
- technologische Überlegenheit als Element der Abschreckung

Das Spektrum heutiger UGV (und UAV)
- alle Komponenten der Systemrichtung noch immer im Entwicklungsstadium
- Suche nach optimalen Designauslegungen, Anwendungsgebieten und Einsatzstrategien
- gleiches Design in mehreren Größen
- Konzeptlosigkeit in der Welt
- UAV aufgrund der noch relativ geringen Stückzahlen nur vereinzelt und meist allein eingesetzt worden, größere UGV-s gibt es kaum
- Umbau der Streitkräfte

[11] SWP- **S**tiftung **W**issenschaft und **P**olitik - Deutsches Institut für Internationale Politik und Sicherheit

- intensive Experimentalaktivitäten
- Reichweite der sichtliniengebundenen Datenübertragungsstrecke
- Datenübertragung mittels Relaisfahrzeug/-station oder Satellit
- bis zu einem gewissen Grad Satelliten ersetzen, ergänzen
- militärisch relevante Nutzlasten
- Hauptaufgabe der UGV-s zur Zeit meistens Minen / Sprengmitteln suchen und entschärfen
- Unmanned Combat Ground Vehicles (UCGV)
- Zusammenarbeit /Symbiose mit TUAV (Tactical Unmanned Aerial Vehicles) Luftnahaufklärung für Bodentruppen (organisatorisch generell der Armee unterstellt)
- kleine Bodendrobotern – wenige Nutzungsnischen, wie etwa für den Einsatz in Spezialeinheiten
- unbemannte Bodenroboter haben immer noch die gleichen Probleme wie die bemannten Fahrzeuge zu Beginn des 20. Jahrhunderts
- sie sind unzuverlässig und schwer zu bedienen
- im Gegenteil dazu wurden in den letzten zwei Jahrzehnten, speziell durch massive Förderung in Israel und den USA, die unbemannten Flugzeuge zusehends ausgereifter

Vorteile unbemannter Systeme

- im Idealfall führen Roboter ihre Mission unbeaufsichtigt aus, die bei Bedarf jedoch von Menschen überwacht und korrigiert werden können
- entsprechend wurde ihr Potential von immer mehr Entscheidungsträgern erkannt
- komplett von unbemannten Systemen übernommen
- angesichts des steigenden Entwicklungstempos sind langfristig der weitgehenden Ablösung der bemannten Systeme kaum Grenzen gesetzt
- Heranziehung von Menschen zur Führung bemannter Fahrzeuge bringt einige physiologisch bedingte Begrenzungen mit sich
- wenn für die Überwachungspatrouillen in erster Linie UGV genutzt würden, könnte das Operationstempo der bemannten Fahrzeugen gesenkt werden
- Operatoren müssen nicht am Ort sein
- für den UGV- Einsatz bieten sich insbesondere riskante Operationen in den frühen Phasen eines militärischen Konflikts
- Patrouillen und Transportaufgaben in gefährlichen Kampfgebieten
- UGV vermitteln den Eindruck ständiger Präsenz

Offene Fragen

- Fahrer oder Operator für die Steuerung
- Systembediener steuert Sensorik und Bewaffnung
- bei Steuerung ohne direkte Sichtlinie (*line of sight*) auf dem Wege der Satellitenübertragung bis zu eine Sekunde Verzögerung
- wenig Sinneseindrücke (Fehlbedienung)
- zukünftige UGV weitgehend autonom, fahren selbstständig (Lagekontrolle, Navigation und Subsystemkontrollen werden vom Bordcomputer durchgeführt)
- mittels kombinierter GPS/INS- Navigation Fahrzeugposition weniger als einen Meter genau
- die Datenübermittlung für die Steuerung ist die Achillesferse der UGV- Systeme
- sichere hochvolumige Datenübertragung
- Datenkomprimierung
- Datenverschlüsseln (Kryptologie)

- doch auch bemannte Fahrzeuge sind bei der zunehmenden Datenvernetzung im Zuge einer netzwerkorientierten Kriegführung von der robusten Datenübermittlung abhängig
- Zukunft: Kontrolle und Koordination auch des bemannten Verkehrs wird automatisiert
- dies bedeutet, dass die Vermeidung von Zusammenstößen automatisiert zwischen den einzelnen Fahrzeugen selbst erfolgt
- Widerstände in der Öffentlichkeit zu erwarten

Entwicklungstendenzen
- ständig ändernde Wünsche der Streitkräfte treiben die Kosten in die Höhe
- vom belächelten Spielzeug zum militärisch und wirtschaftlich bedeutenden Hochtechnologieträger (bei der UAV schon derzeit, bei der UGV erst in der Zukunft)
- generell scheint das Interesse in Richtung größerer Fahrzeuge zu gehen (bei der UAV schon derzeit, bei der UGV erst in der Zukunft)
- die Forderung, UGV als Waffenplattformen zu benützen, wird ebenfalls tendenziell zu größeren Fahrzeugen führen
- günstigeres Verhältnis von Volumen und Oberflächengewicht beim gleichen Schutz
- leistungsfähige Sensorsysteme benötigen viel Energie
- entsprechend motorisierte Plattformen
- Sensoren und Effektoren modulartig austauschbar
- Plattform sollte grundsätzlich modular ausgelegt sein
- Lastenheft eines zu beschaffenden UGV- Systems

6 VORTEILE UND NACHTEILE VON BODENROBOTERN

Für den gemischten Einsatz von Menschen und Robotern nehmen wir als Beispiel die Kolonnenfahrt. In der Vergangenheit haben die Fahrer des Pferdewagens viel weniger Stress gehabt, als Fahrer von derzeitigen Fahrzeugen. Natürlich hängt das mit der höheren Geschwindigkeit und dem immer größer werdenden Verkehr zusammen, aber nicht ausschließlich. Die Pferde beobachten auch, weichen die auftauchenden Hindernisse aus, geben Rückmeldung für den Fahrer. Sie können sogar von selbst nach Hause finden. Die Kraftfahrzeuge im Gegensatz zu den Pferden helfen dem Fahrer nicht, deshalb sollten wir irgendwie anders seine monotone Arbeit erleichtern. Wenn die Fahrzeuge in der Kolonne stundenlang, über mehrere hundert Kilometer fahren, könnten die Spuren von erstem Fahrzeug (halb-) automatisch „kopiert“ werden. So wäre es möglich auch den Abstand zwischen Fahrzeugen zu verringern. Die Belastung von mitfahrenden Fahrern wäre viel kleiner, weil sie nicht immer 100% konzentriert sein müssten, an einfacheren Strecken könnten sie sogar ruhen. Wer die ganze Kolonne führt entscheidet der Kommandant, es wäre möglich während der Fahrt in einen anderen „Fahrerplatz“ umzuschalten.

VORTEILE:
- in Roboterfahrzeugen gibt es keine gefährdete Besatzung
- keine ergonomischen Beschränkungen
- hermetische Abdichtung des Motorraumes ist nicht nötig/ Motorraum muss nicht getrennt sein
- Innenraum voll nutzbar, kann sehr klein sein: das ganze Fahrzeug kann damit kleiner sein
- ABC Schutz, Heizung, Klimatisierung, Lüftung, Beleuchtung ist nicht nötig
- Feuerunterdrückungsanlage muss nicht den strengen (wegen der Anwesenheit von Menschen) Gesundheits-Vorschriften entsprechen, Innenraum kann sogar sauerstofffrei sein

- wegen eventuellen Feuer entstandene giftige Rauchgase sind unproblematisch, bei der Konstruktion (Material-Wahl) müssen wir dies nicht berücksichtigen
- unbeschränkter Aufenthalt in „Stellung“, auch in verseuchten Gebieten
- wir müssen die strenge ergonomische Anforderungen nicht berücksichtigen
- Vibrationen, starke Stöße, Schockbelastungen, Lärm sind unproblematisch
- bei Roboterfahrzeugen mit billigerem Aufbau können wir wegen der Erhöhung von Nutzlast auch leichteren Panzerschutz verwenden
- eventueller Fahrzeugverlust ist taktisch und finanziell einkalkulierbar => „Einwegrobotern“
- mit gängigen Transportflugzeugen luftverlastbar
- „vollgepackte“ Roboterfahrzeuge mit relativ kleinen Auftriebsvolumen könnten eventuell tauchen (Motorluft über Schnorchel, oder kurzzeitig von Druckflaschen)
- niedriges Profil – niedrige Silhouette
- „Selbstzerstörung“ jederzeit durchführbar

NACHTEILE:

- Besatzung ist nicht voll ersetzbar
- für den Mannschaft- Transport nicht verwendbar (eventuell für den Robotern-Transport)
- immer einsetzbare Roboterfahrzeuge mit ausreichender Sicherheit sind relativ teuer
- braucht gut ausgebildete Bedienungs- und Instandhaltungspersonal
- fernsteuerndes Bedienungspersonal, ohne Eigengefährdung, kann eventuell zu sehr riskanten Aktionen hingerissen werden
- autonome Wahrnehmung von „negativen“ Hindernissen (Löcher, tiefer Graben, weicher Boden…) ist sehr schwierig
- Datenverarbeitung (nahe) Echtzeit braucht große Rechner-Kapazitäten mit Temperaturbeständigkeit auch bei sehr tiefen Temperaturen (bis zu -40°C)
- feldsichere und zerstörungsresistente Subsysteme sind nötig
- nicht störbare / nicht erkennbare Funkverbindungen zu garantieren ist sehr schwierig
- Entwicklung und Systemkomponenten können sehr teuer sein

Allerdings stellt uns die Abwesenheit der Besatzung vor neuen **Problemen mit der Verwendung, Bedienung von Fahrzeugen, Ethik der Waffenbenützung**. Mit diesen Themen habe ich mich in zwei Artikeln detailliert beschäftigt [6,7] Nicht nur bei den Friedenskräften, aber auch bei anderen Kampfverbänden ist der Einsatz von selbststeuernden (autonomen) Robotern fraglich. Die Verwendung von Waffen ohne Aufsicht des Bedienungspersonals sollte vom militärischen Ethik und Recht verboten werden. Bis jetzt gibt es keine, und wahrscheinlich wird es noch eine sehr lange Zeit **keine künstliche Intelligenz** geben, **was die Verantwortung von Menschen übernehmen könnte!** Auch deshalb wäre es sehr sinnvoll alle Roboter mir einer „Black-Box” auszustatten.

7 UGV – PLATTFORMEN – ENTWICKLUNG

Bei der Konvoifahrt könnten Roboterfahrzeuge auch als **Träger von** manchen nicht tödlichen, **„non lethal / nicht-letalen“ Waffen** [23] für die direkte Verteidigung eingesetzt werden. Neu entwickelte Waffen sind oft groß und schwer, sie können auch für das eigene Bedienungspersonal gefährlich sein. Anders gesehen: wenn wir auf das Bedienungspersonal keine Rücksicht nehmen müssen, dann kann die Waffen-Ausführung viel einfacher/billiger sein. Zusätzlich ist auch der lokale Rundum- Schutz vom Fahrzeug gelöst.

Für oben beschriebenen und ähnlichen Anwendungen ist es nötig, dass die einzelnen Fahrzeugkomponenten elektronisch steuerbar, oder noch besser fernsteuerbar sind. Vieles gibt

es schon, die fehlende Komponente müssen wir bei den erfahrenen Herstellern entwickeln lassen.
Schon jetzt sind eingebaut:

- vollelektronisch geregelte Motoren
- automatische Getriebe
- automatisch wirkende Längs- und Quersperren, wie zum Beispiel das von der Firma Steyr entwickelte ADM System: (Automatic Drive-train Management-System (ADM-System) [24, 25]
- statt Periskopen Kameras
- „swim by wire" fernsteuerbare Schwimmkomponenten
- statt Ein- Zweimann Türmen ferngesteuerte: RCWS- Remote Controlled Weapon Stations, z.B. [26]

Bei einzelnen Fahrzeug-, resp. Waffensystem-Komponenten ist **schon bei der Entwicklung, oder bei der Ausschreibungen zu berücksichtigen, dass sie möglichst fernsteuerbar sind**. Die geschätzte Lebensdauer von den in der letzten Zeit eingeführten, resp. im Bau befindlichen Fahrzeugen sind mehrere Jahrzehnte. Veralterungszeiten der Steuerungssysteme sind nach wenigen Jahren veraltet. Schon jetzt ist es nötig mit der Ausbildung von Robotern- Bedienungspersonal, Operatoren zu beginnen, theoretisch auf eine bisherig weit entfernte Wahrnehmung- und Handlungs- Dimension vorzubereiten.

Wegen verantwortungsvollen Handelns braucht das weit entfernte Bedienungspersonal ein umfangreicheres und echtzeitiges Bild. Deshalb ist die echtzeitige, breitbandige, angemessen verschlüsselte, störungsfreie Datenübertragung viel mehr hervorzuheben.

Roboterfahrzeuge (Basisplattformen) müssen mindestens so gute Geländegängigkeit und Höchstgeschwindigkeit haben, als bemannte Fahrzeuge (wegen wirksamer Mitwirkung, gemischten Kolonnenfahrten, usw.)

Argumente für einen 6x6 Grundfahrzeug:
- bewehrt, leistungsfähig, zuverlässig, erprobt
- klein, wendig, relativ niedriges Profil
- handelsübliche Komponenten
- relativ billig, wirtschaftliches Betrieb
- sehr viele kleine Bodenroboter haben 6x6 Antrieb (wegen Geländegängigkeit)
- auch unbemannte Fahrzeuge, mit teuren Systemen ausgestattet, brauchen eine solide Grundpanzerung und Minen- resp. IED- Schutz
- tiefe Rampe (wie z.B. bei PANDUR-Valuk), oder sogar sinkbare Rampe (wie bei LKW-s) für eventuell mitgeführten kleineren Roboterfahrzeugen (z.B. Entschärfungsrobotern) ermöglicht den selbständigen „Aus- und Einbooten"
- verstärkte Komponenten - Reserven für =>
- **militärisch relevante Nutzlasten**

ZU ENTWICKELN?

- eine reine **Nichtschwimmer** Basisvariante - Entwicklungs- und Kostenreduktion
- **Notschwimmen** mit aufblasbaren Säcken (ohne Besatzung eventueller Verlust einkalkulierbar)
- **Voll- Schwimmvariante** (Hochseetauglich) separates Leichtbau mit anderer Materialwahl, strengeren Korrosionsschutz (auch gegen Salzwasser), speziellen Dichtungen, zielorientierten Aufhängungen und Wannenform usw.

Subsysteme:

- Lastenheft eines zu beschaffenden UGV- Systems definieren
- Welche Subsystemen können wir weglassen im Vergleich zu bemannten Fahrzeugen?
- Was brauchen wir zusätzlich?
- Forderungskatalog (Final Operational Requirements)
- Durchführbarkeitsstudien (Feasibility Studies)
- Militärische Anforderungen (Military Requirements)
- Technischer Testzyklus (Technical Test Cycle)
- Automatischer Abstandhalter – Abstandsregeltempomat
- Spurhalteassistent, Einparkassistent
- Interaktiver Austausch von Daten, integrierte und externe Diagnose Tools (diagnostische und prognostische Informationen in Echtzeit), „Black-Box"-en
- Beim Ausfall von der Steuerung (z.B. wegen schlechter Funk- Verbindung) während der Fahrt ist es nötig einen „Notverhalten" zu definieren, was das Fahrzeug genau machen soll, abhängig von Fahrsituationen, momentanen Geschwindigkeiten, usw.
- Einrichtung zum „irgendwie Heimkommen" (Limp Home Facility)
- Lokales Rundum- Schutz gegen Feindeinwirkung
- akustische Warnung und nicht letaler (Selbst-) Schutz gegen Vandalen, zivile Bevölkerung, neugierigen Kindern, usw.

Bemannte Roboterfahrzeuge – mit Tauschcontainern im Nutzlastbereich – können als eine „Kapsel" („Crew Citadel") für die Besatzung ausgeführt werden. Diese Mannschaftszellen können mit verschiedenen Schutzkits (verschiedene Schutzstufen) ausgestattet werden. Die Möglichkeit von autonomem/ferngesteuertem Abtransport von Verletzten aus gefährlichen Gebieten hat ein sehr hohes Potenzial in sich.

Eventuelle „Vernetzung" von Roboterfahrzeugen mit Roboterflugzeugen und/oder Roboterhubschraubern mit Kameras und Zeitgleich-Datenübertragung untersuche ich in einem eigenen Kapitel.

8 ZUSAMMENARBEIT/SYMBIOSE VON BODEN- UND FLUGROBOTERN UGV & UAV => UGAS

Landfahrzeuge können nicht „über den Hügel" sehen, deshalb sind Informationen von der Luftaufklärung sehr wertvoll. Starten und Landen von unbemannten Flugzeugen sind immer mit Gefahren verbunden. Eingebaute Beobachtungsgeräte und Waffen (auch wegen angeforderten niedrigen Gewichts) sind sehr empfindlich und teuer. Diese Teile, beziehungsweise das ganze Flugzeug sind beim Landen sehr gefährdet. Flugapparate mit Drehflügeln lösen die Probleme auch nicht. Im Vergleich zu unbemannten Flugzeugen sind ihre Überlebensraten leider viel niedriger, sie sind lauter (leicht aufklärbar), teurer, haben kürzere Lebensdauer, ihr Betrieb ist weniger wirtschaftlich, sie sind langsamer und haben einen kürzeren Aktionsradius. Von ihrem Konstruktionsaufbau gegebene Vibration verursacht auch Schwierigkeiten. Das Einsatzgebiet von Hubschraubern konzentriert sich weiterhin auf spezielle Anwendungen, wo andere Fluggeräte ausgeschlossen sind.

In Konfliktsituationen können wir uns nicht nur auf Daten von Satelliten-Navigations-Systemen verlassen. Diese sind leicht störbar, oder können für uns nicht entschlüsselbar kodiert sein. Mit verschiedenen Sensoren (Kamera, Radar, Laserradar) ausgestattete kleine

unbemannte Flugzeuge mit Starrflügeln sind besser für die echtzeitige Kampffeld-Beobachtung geeignet.

„Symbiose“ von Boden- und Flugrobotern kann weiter für die lokale Luft-Aufklärung dienen. Die Flugroboter helfen den weiteren Weg zu bestimmen, eventuelle Hindernisse, Gefahren, Fallen zu orten, und ausreichende Informationen für die Festlegung von möglichen Umfahrungen zu sammeln.

Volle Automatisierung ist sehr wichtig auch wegen der **Sicherheit**. Aktive Mitwirkung des ungeschützten Bedienungspersonals auf offenem Gebiet ist wegen eventueller Feindeinwirkung sehr gefährlich, bzw. durch Flugbahn von eigenen Fluggeräten. Beispiel stellen die häufigen Modellflugzeug-Unfälle dar. Diese geschehen oft mit der Aufsicht von geübten Piloten unter friedlichen Umständen! Beim Starten und Landen von/auf eine(r) Fläche von mindestens 10 m breit und 100 m lang sind die stehenden und bewegenden Soldaten, die zivile Bevölkerung, neugierige Kinder, Tiere, Fahrzeuge und wegen einem eventuellen Zusammenstoß selbst die Roboterflugzeuge gefährdet.

In der Presse, im Internet, im Fernseher sind oft spektakuläre „Aktionsbilder“ über Soldaten zu sehen, die in den offenen Gebieten aus der Hand (kleinere) Roboterflugzeuge starten. Im Einsatz kann das sehr gefährlich sein, weil es einen aus der Ferne sehbares, völlig „offenes“ Zielpunkt bietet!

1. Bild. Starten von Kleinflugzeugen aus der Hand [27]

Ich bin überzeugt, dass das vollautomatisch funktionierende Roboterflugzeugträger-System technisch, steuerungstechnisch schon in der nächsten Zukunft verwirklichbar ist.

FLUGROBOTER „WERFER UND FÄNGER”

Ein mehrachsiges Industrieroboter-Arm „wirft“ den Flugroboter auf die Flugbahn, und nach dem Einsatz fängt er es wieder ein! Nötig ist eine „Dockstelle“ in der Nähe des Massenschwerpunktes und ein Sender. Nach dessen Signalen findet mit der Hilfe von einem

Empfänger am Roboterarm die sichere Verbindung rechtzeitig statt und das Fluggerät ohne Überlast kann auf dem Restweg gebremst werden.

2. Bild. Starten und Landen von Kleinflugzeugen mit Roboter-Arm (Bild vom Autor)

Das Wesentliche meines Vorschlages ist, dass nicht der Flugroboter die Dockstelle sucht, weil eine „cm“ Genauigkeit heute noch nicht erreichbar ist. Es fliegt nur einfach mit niedriger Geschwindigkeit über den, in Bereitschaftsposition wartendem Roboterarm. Der Roboterarm „jagt“ von hinten und von unten die Maschine runter. Die Geschwindigkeit, Beschleunigungswerte, Genauigkeit und Nutzlast von Industrierobotern machen das möglich. Wenn die rechnerische Auswertung nach Flugzeugtyp, momentanen Gewicht, Kurs, Höhe, Empfindlichkeit von den an Bord befindlichen Geräten, Waffen, gefährlichen Stoffen, nach meteorologischen Situation usw. die Landung nicht sicher beurteilt, dann bleibt der Roboterarm in der Grundposition. Momentanes Gewicht wird nach der Betriebszeit, den Betriebszuständen (Kraftstoffverbrauch), resp. auf Grund des eventuellen Munitionsverbrauchs interpoliert. Wenn nach einer positiven Entscheidung vom Rechner die „Andockung“ doch nicht gelingt (z.B. wegen einer starken Windböe) startet das Flugzeug durch. Nach einer „Ehrenrunde“ bietet das Flugzeug gegen die Windrichtung manövrierend wieder und wieder (bis es gelingt) eine Möglichkeit für den Einfang. Nach einer gelungenen Andockung werden die Antriebsmotoren sofort automatisch ausgeschaltet, Elektromotoren sind theoretisch sogar in Bremsmodus umschaltbar. Alle Flugbewegungen befinden sich über den Köpfen, in sicherer Höhe.

Schnelles und vor allem sicheres Starten/Einfang von Flugapparaten mit Drehflügeln sind auch möglich. Bei starkem Wind, wenn die am Boden stehenden Fluggeräte nicht mehr in Sicherheit sind, könnte es eine große Hilfe bieten: es könnte die Einsatzmöglichkeiten ausweiten. Beim Landen wartet der Hubschrauber hoch schwebend über der Roboterarm, bis es von der Dockstation sicher fixiert ist. So könnte die Gefahr von Entstehung von Bodenwirbeln und Wirbelringen [28] minimiert werden.

Derzeitige Industrierobotern mit vielen Freiheitstufen, mit sehr genauen Positions- und Bahnwiederholgenauigkeiten, hohen Gelenkdrehmomenten und Achsgeschwindigkeiten übertreffen die Möglichkeiten vom menschlichen Arm.
Die höheren Landungsgeschwindigkeiten von größeren Flugzeugen sind wahrscheinlich nur mit Weiterentwicklung erreichbar, zum Beispiel auf Nachteil der absoluten Genauigkeit, was bei dieser Anwendung nicht so maßgebend ist. Der Bewegungsraum, Kräfterichtungen sind auch begrenzbar, angepasst an diese spezielle Anwendung.

VORTEILE VOM SYSTEM:

- voll automatisierbar
- starten praktisch ohne Vorbereitungszeit
- Fluggeräte können viel einfacher und leichter/belastbarer sein
- alle bisherigen Komponente, welche den sicheren Start und das Landen ermöglichen (Räder, Kufen, Schutzhüllen, verstärkte Teile, Dämpfern, Energieabsorbers, Luftsäcke, Fallschirme, Schwimm- Körpern/Pontonen usw.), können wir weglassen
- Geräte müssen nicht so robust gebaut werden, viel seltenere „harte“ Landung (bei herkömmlichen Landung als Grenzfall eingestuften/übertroffenen Verhältnissen)
- im automatischen Betrieb ist das Bedienungspersonal geschützt, so bei Schlechtwetter (Kälte, Wind), bei schlechten Sichtverhältnissen (in der Nacht, bei Nebel, Regen, Schnee) ist nicht zu Wettereinflüssen ausgesetzt
- in ABC verseuchten Gebieten ist es auch einsetzbar
- verwendbar außerhalb von „grünen Zonen”, wo wir die Anwesenheit von feindlichen Richtschützen nicht ausschließen können
- bessere allgemeine Sicherheit
- „Docken“ auf bewegende (!) Fahrzeuge, stark „schaukelnde“ Schiffe (wegen dem Wellengang), aufgetauchten U-Boote sind möglich, das kann auch bei unbemannten Fluggeräten mit Drehflügeln wichtig sein
- bewegende Fahrzeuge können sogar (größere) Roboterfahrzeuge sein
- nach der Einführung wirtschaftliches Betrieb

NACHTEILE VOM SYSTEM:

- bei Landfahrzeugen ist wegen Gewichtsbeschränkungen das bedienbare Gewicht der Drohnen begrenzt
- für schwerere Drohnen bräuchten wir schwere Roboterarme mit sehr großen Abmessungen für das Erreichen der nötigen Beschleunigungs- und Bremskräften (für die stationäre Anwendung kann ich mir eine Entwicklung von diesen überschweren Systemen vorstellen)
- bis zu der System-Einführung sind viele Probleme zu lösen, die Details müssen ausgearbeitet werden und langzeitig testen
- die materiellen Aspekte von solchen Projekten sind nicht zu vernachlässigen
- die Entwicklung einer mit ausreichender Traglast und Geschwindigkeit, den strengen militärischen Anforderungen entsprechende, bei rauen Bedingungen (z.B. extreme Temperaturen) verwendbare, für diese Anwendung optimalisierte Industrieroboter kosten viel Geld

Größere Militärfahrzeuge sind als „Roboterflugzeugträger“ geeignet. Kleine Roboterflugzeuge haben meistens kleineren Aktionsradius, deshalb ist es zielführend es zum Einsatzgebiet näher zu transportieren. Für die Erfüllung einer eigener Mission bleibt ausreichend Kraftstoff/Energie. Das Transportfahrzeug kann als Arbeitsplatz für die

Operatoren, resp. bei den Robotfahrzeugen als Übertragungsstation zwischen Bedienungspersonal und Roboterflugzeugen dienen.

3. Bild. „Roboterflugzeug-Träger“ (Bild vom Autor)

Ein Roboterarm kann mehrere Flugapparate bedienen, nach dem Einsatz werden sie automatisch auf ihren Transportplatz gelegt. Von diesem Platz kann das Bedienungspersonal das Flugzeug für Instandhaltung, Reparatur, Kraftstoff/Energie Auffüllung, Programmieren, Tausch von Subsystemen, usw. ins Fahrzeuginnere einnehmen.

9 AUSBLICK

Für immer größere Selbstständigkeit sind weitere Schritte wichtig: für ungestörtes Patrouillieren können die Beobachtungs-, und/oder Antriebseinheiten, Batterien, Kraftstofftanks, Waffen und Munition selbständig (ohne direktes Einwirken vom Bedienungspersonal) getauscht und ergänzt werden. Aufgenommenes Informationsmaterial muss nicht immer „online“ gesendet werden. So sind die Systeme weniger störbar, weniger aufklärbar/zerstörbar, nicht so energieaufwendig. Bei einer kurzen Zwischenlandung, nach dem automatisierten Tausch von Datenträgern, können die Patrouillieren fortsetzen. Die Zusammenarbeit von Roboterfahrzeugen und Drohnen als Sensorträger bei der Erstellung von Bildfolgen dient zur Ausarbeitung von realen 3D-Modellen. In Deutschland: *„Für die Verfahren ist ein Experimentalsystem ABUL (Automatisierte Bildauswertung am Beispiel UAV LUNA) entwickelt worden…“* [29]

„Heute spricht sehr viel dafür, dass der Mensch seine Intelligenz als steuerndes Element einsetzen und sich zunehmend von der unmittelbaren Frontlinie zurückziehen und sie den ferngesteuerten Maschinen überlassen wird. Die fliegenden Roboter-Systeme bilden dabei lediglich den Anfang.“ [22]

Bodenroboter werden wahrscheinlich die klassischen Transport- und Kampffahrzeuge nie völlig verdrängen. Die sinnvolle Kombination von Robotern und klassischen Fahrzeugen (die

Hybrid-Verbände) werden in der Zukunft aber Raum gewinnen, vor allem bei den Spezialeinheiten. Die wissenschaftliche Forschung in der nahen Zukunft muss Antwort finden auf technischen, strategischen (militärtaktischen) und ethischen Fragen (welche die Kriegsverwendung von der Robottechnik stellt). Wirtschaftlich muss die Weiterentwicklung von militärtechnischen Mitteln so erfolgen, dass diese wirkungsvoll eigene lebende Kräfte schützen und erfolgreich den Kampf mit der gegnerische Seite aufnehmen können. Heute können die technische Möglichkeiten den Menschen ersetzen. Die Wissenschaftler sollten die optimale Proportion finden wo Mensch und Maschine sich vervollständigen.
Es wäre schon derzeit sinnvoll alle Fahrzeugkategorien vor der Ausschreibung/Entwicklung/Beschaffung zu überprüfen auch als fernsteuerbare UGV-Ausführung.
Ältere Militärfahrzeuge könnten – statt teueren, und fast immer zu Kompromissen führenden Modernisierungen – als UGV Plattformen umgebaut werden. Auch ältere Fahrzeuge haben oft einen soliden Schutz, aber sind z.B. gegen IED-s nicht ausreichend geschützt. Einen Zusatzschutz zu entwickeln ist oft nicht möglich, oder nicht rentabel.

10 FAZIT

Bei der Durchführung von Logistischen-, Konvoibegleitungs- und den gefährlichsten Aufklärungsaufgaben verursachen die Terrorangriffe (meistens durch Minen und selbstgebastelten Sprengmitteln) den Truppen enorme personelle und materielle Verluste. Die immer verbreitetere Verwendung von Bodenrobotern ist eine Möglichkeit für Verlustreduzierung. In der Logistikkette bereitet der Ausfall von einzelnen Fahrzeugen (inklusive Ladung) keine großen Schwierigkeiten. Der Nachschub ist in wenigen Tagen möglich – der Verlust von Menschenleben ist hingegen nicht ersetzbar! Deshalb sind die Soldaten bzw. deren Leben erstrangiges Ziel von Terroristen und nicht die Fahrzeuge! Laut Oberst Walter Ohm, General der Heereslogistiktruppen: *„Es gibt's kein „hinten" und kein „vorne", überall ist vorne"* [30]
Vermehrte Einführung von Roboterfahrzeugen könnte den Rückgang von Anschlägen gegen Konvois bewirken – ohne vorhandene Zielpersonen werden die Anschläge zwecklos. Natürlich braucht man für nötige Bergungen (eventuelle Fallen!) sehr gut geschützte Bergefahrzeuge, oder (ebenfalls) ferngesteuerte Roboterfahrzeuge.

Literatur:

1. Koleszár Béla: Harcjárművek továbbfejlesztése és a szárazföldi robotok = Weiterentwicklung von Kampffahrzeugen und die Bodenroboter; Hadmérnök http://www.hadmernok.hu/archivum/2008/1/2008_1_koleszar.html
2. Koleszár Béla: Elképzelések a szárazföldi és légi robottechnikai eszközök jövőbeni kölcsönös együttműködéséről/szimbiózisáról = Überlegungen zu der zukünftigen gegenseitigen Zusammenarbeit/Symbiose von Boden- und Flugrobotern http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Koleszar_Bela.pdf
3. Koleszár Béla: Szárazföldi robotok, az UAV-k szegény rokonai? = Bodenroboter, die armen Verwandten von UAV-s? http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/Koleszar_Bela.pdf
4. Koleszár Béla: Szárazföldi robottechnikai eszközök tervezésének és alkalmazásának biztonsági szempontjai = Die Sicherheitsaspekte der Konstruktion und Anwendung von Boden-robotertechnischen Geräten (http://hadmernok.hu/2009_2_koleszar.pdf

PowerPoint:
http://www.zmne.hu/tanszekek/ehc/konferencia/prezrw8/Koleszar_Bela.pdf

5. Koleszár Béla: A földi robottechnikai eszközök informatikai részegységeivel szemben támasztott speciális (terepi kivitelt igénylő) követelmények rendszerezése, elemzése = Gliederung und Analyse von speziellen (geländetaugliche Ausführung benötigende) Anforderungen für Informatik-Untergruppen von Boden-robotertechnischen Geräten http://hadmernok.hu/2009_4_koleszar1.pdf
6. Koleszár Béla: A robothadviselés etikai kérdései I. Harci robotok = Ethische Fragen zu Roboterkriegen I. Kampfrobotern http://hadmernok.hu/2009_4_koleszar2.pdf
7. Koleszár Béla: A robothadviselés etikai kérdései II. Katonai erkölcs = Ethische Fragen zu Roboterkriegen II. Militärmoral http://hadmernok.hu/2010_1_koleszar.pdf
8. Koleszár Béla: A vegyes, humán és robotjárművekből álló konvojok modellezése = Modellierung von Konvois bestehend aus gemischten, Human- und Roboterfahrzeugen http://www.szrfk.hu/rtk/kulonszamok/2010_cikkek/Koleszar_Bela.pdf
9. Koleszár Béla: Szárazföldi harcjárművek és robotjárművek védelme a rögtönzött robbanóeszközök ellen = Schutz von Land-Kampffahrzeugen und Roboterfahrzeugen gegen improvisierte Sprengsätze, Műszaki Katonai Közlöny 2010
10. Koleszár Béla: Járművek robbanásvédelme = Sprengschutz von Fahrzeugen; (in Publikation)
11. Koleszár Béla, Ványa László: Ő, a Robot (Isaac Asimov után szabadon) = Er, der Roboter (frei nach Isaac Asimov) (in Publikation)
12. Koleszár Béla: Predstavy o budúcom spoluúčinkovaní obrnených vozidiel, pozemných a vzdušných robotov = Überlegungen zu der zukünftigen gegenseitigen Zusammenarbeit von Boden- und Flugrobotern, Konferencie „Špeciálna technika 2008“ Bratislava
13. http://de.wikipedia.org/wiki/Lockheed_C-130
14. http://de.wikipedia.org/wiki/RPG-7
15. http://de.academic.ru/dic.nsf/dewiki/1134014
16. http://www.streitkraeftebasis.de/portal/a/streitkraeftebasis/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLNwyON_Z1DQVJQjiOhgb6kQjxoJRUfV-P_NxUfW_9AP2C3IhyR0dFRQBrhHPs/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfMVNfM01FVQ!!?yw_contentURL=%2F01DB040000000001%2FW284XGFE578INFODE%2Fcontent.jsp
17. David Eshel: Schutz vor improvisierten Sprengsätzen, Truppendienst 1/2007 http://www.bmlv.gv.at/truppendienst/ausgaben/artikel.php?id=558)
18. Dan Löffler: Schützenpanzer PUMA, http://www.danmil.de/15433.html
19. Ario Pfeifer: Überlebensfähigkeit und Schutz; Strategie & Technik Februar 2010, p.46
20. Ványa László: Pilóta nélküli repülőgépek és földi eszközök a rádió-távirányítású alkalmi robbanótestek (RCIED) elleni harcban; Repüléstudományi Közlemények 2008. április 11 Kiadó: ZMNE ISSN: HU ISSN 1789-770X http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Vanya_Laszlo.pdf
21. Joint Robotics Program Master Plan FY2005 http://www.jointrobotics.com/activities_new/2005%20JRP%20Master%20Plan.pdf

22. Sascha Lange: Flugroboter statt bemannter Militärflugzeuge? Stiftung Wissenschaft und Politik - Deutsches Institut für Internationale Politik und Sicherheit)- Studie Juli 2003, Berlin http://www.swp-berlin.org/common/get_document.php?asset_id=187

23. Nicht-tödliche Waffe http://de.wikipedia.org/wiki/Nicht-t%C3%B6dliche_Waffe

24. Franz Kosar: Die "Pandur" II-Radpanzerfamilie 6 x 6 und 8 x 8 http://www.bmlv.gv.at/truppendienst/ausgaben/artikel.php?id=60

25. Automatic Drivetrain Management http://de.wikipedia.org/wiki/Automatic_Drivetrain_Management

26. Samson Remote Controlled Weapon Station http://en.wikipedia.org/wiki/Samson_Remote_Controlled_Weapon_Station

27. http://images.dailytech.com/nimage/13211_large_Army%20UAVs.JPG

28. Gausz Tamás-Szilágyi Dénes: *Az örvényesség és a helikopterek;* Repüléstudományi közlemények: „Fél évszázad forgószárnyakon a magyar katonai repülésben" 2005. 04. 15 ZMNE Szolnok;, p.p. 5-7 HU ISSN 1789-770X

29. Norbert Heinze: Automatisierte Bildfolgenauswertung für die luftgestützte Überwachung und Aufklärung. Wehrwissenschaft Forschung & Technologie Jahresbericht 2007 http://www.int.fraunhofer.de/FuT_Jahresbericht_07_de.pdf

30. Michael Horst und Gerhard Heiming: Heereslogistik der Zukunft; Strategie & Technik Februar 2010, p. 31

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Krasznay Csaba
csaba@krasznay.hu

E-KÖZIGAZGATÁSI RENDSZEREK ÉS ALKALMAZÁSOK SEBEZHETŐSÉGI VIZSGÁLATA

Absztrakt

A programozási hibák kiszűrésére körültekintő tesztelésre van szükség. Amíg azonban a funkcionális és terheléses teszteknek kifinomult módszertana van, a biztonsági hibák felderítésére csak az elmúlt években kezdtek eljárásokat kidolgozni. Jelen tanulmány célja, hogy bemutassa azokat a releváns szabványokat és ajánlásokat, melyek segítségével az e-közigazgatási rendszerek fejlesztői szisztematikus módon tudják a legfontosabb biztonsági hibákat webes alkalmazások esetén kiszűrni. A sebezhetőség-vizsgálati módszertanok széles skálájának ismertetése és a Common Criteria behatolás-tesztelési követelményei segítenek meghatározni az elvárt ellenőrzési mélységet. A tipikus hibák ismertetése után célunk ezekből kiindulva egy olyan tesztelési követelményrendszer összeállítása, mely tetszőleges internetes alkalmazás esetén személyre szabható, és segít a támadási felületek csökkentésében az elektronikus közigazgatási környezetben.

Careful testing is required to detect programming errors. However, while functional and stress tests have sophisticated methodology, procedures for detecting security errors were established in the last few years. The study aims to present the relevant standards and recommendations that help the developers of e-government systems to filter the most important security errors of web applications in a systematic manner. Introducing the wide range of vulnerability assessment methodologies and the Common Criteria intrusion testing requirements will help establishing the required depth of control. Our aim is to compile a security test standard based on common errors which is customizable for any internet application and helps reducing the attack surface of the e-government environment.

Kulcsszavak: *sebezhetőség-vizsgálat, Common Criteria, OWASP, elektronikus közigazgatás ~ vulnerability assessment, Common Criteria, OWASP, e-government*

BEVEZETÉS

Az elektronikus közigazgatás kialakulásával párhuzamosan fókuszba kerül az ezt megvalósító alkalmazások biztonsága is. Miután döntően olyan rendszerekről beszélünk, melyek közvetve vagy közvetlenül interneten keresztül is elérhetők, ráadásul az adatcserék miatt akár több, egymástól független szervezet megoldásai is szoros kapcsolatban állnak egymással, a külső informatikai támadások elleni védelem alapvető tervezési kérdés kell, hogy legyen.

Az e-kormányzati rendszerek stabil működésének egyik legfontosabb kihívását a köznyelvben hackerként elterjedt támadók jelentik. Módszereik jellemzően tisztán informatikaiak, melyek a hálózati réteget, az operációs rendszereket, az alapszoftvereket és magát az alkalmazást célozzák meg, melynek eredménye az adatszivárgástól kezdve a szolgáltatás ellehetetlenítéséig terjed. A magyar központi közigazgatás informatikai rendszerei kielégítőnek mondható hálózati védelemmel rendelkeznek, melyet a Nemzeti Hálózatbiztonsági Központ működése is elősegít, de az alkalmazási réteg felé haladva egyre több kockázattal szembesülhetünk. Különösen igaz ez a böngészőn keresztül elérhető portálokra, melyek sebezhetőségeit szinte észrevétlenül fel lehet deríteni, és ezeket kihasználva akár a védettnek gondolt adatbázisokig vagy belső hálózatokig is el lehet jutni. Egy nem kellő körültekintéssel megírt alkalmazás tehát akár olyan erőforrásokat is veszélybe sodorhat, melyekről az üzemeltető ezt nem is gondolná.

A tesztelési forgatókönyv végrehajtása nem garantálja minden távoli támadás sikeres kivédését, de nagymértékben csökkenti az automatizálható és kevesebb hozzáértést igénylő hibák kihasználásának kockázatát. Mivel magyar nyelven ilyen jellegű módszertan nem érhető el, jelen dokumentum célja hiánypótló módon segíteni a közigazgatási fejlesztők és megrendelők munkáját a behatolás-tesztelés területén.

1. BIZTONSÁG A FEJLESZTÉSI ÉLETCIKLUSBAN

Az információbiztonságra már az alkalmazás első tervezéséi lépéseinél gondolni kell. Ezért bármilyen fejlesztési életciklus modellt is használ a fejlesztő, a biztonsággal kapcsolatos lépéseket be kell építenie a modelljébe. Az egyes fejlesztési életciklus modellek eltérő elnevezéssel ugyan, de általában az alábbi lépéseket tartalmazzák: Projektindítás és tervezés, Funkcionális követelmények meghatározása, Rendszertervezés, Fejlesztés és dokumentálás, Elfogadás, Telepítés, Üzemeltetés és fenntartás, Áttekintés és kivonás.[1]

Projektindítás és tervezés

- A biztonsági igények felderítése:
  - Az alkalmazásban tárolt információk kritikusságának meghatározása
  - Alapvető biztonsági célok meghatározása
- Kezdeti kockázatelemzés
  - Fenyegetések/Sérülékenységek/Kockázatok
  - A védelmi intézkedések megvalósíthatóságának elemzése
  - A biztonsággal kapcsolatos költség/haszon elemzés elvégzése
- Biztonsági keretrendszer meghatározása
  - Lényeges biztonsági kérdések és kockázatok
  - A szolgáltatás szint megállapodás (SLA) meghatározása

Funkcionális követelmények meghatározása

- Biztonsági feladatok a projekttervben
  - Konfigurációkezelés és hozzáférés-védelem a projekt végrehajtása során

[1] Ehhez nagyon hasonló felépítésű a National Institute of Standards and Technology (NIST) SP 800-64 Rev. 2 alapvető szabványa is, de a felsorolás ennek egy pontosított változatát tartalmazza.

    - Nyomon követés
- Biztonsági követelmények meghatározása
    - A kockázatelemzés alapján védelmi intézkedések meghatározása
- Előzetes biztonsági tesztelési terv
    - Tesztelési eljárások és erőforrások
    - Értékelési követelményrendszer meghatározása
- Biztonsági követelmények beépítése a pályázatokba és szerződésekbe
    - Az SLA szerződések tartalmazzák a biztonságot
    - Hardver és szoftver mentések, letétek
- A funkcionális alapkövetelmények tartalmazzák a biztonságot

Rendszertervezés

- Biztonsági specifikációk meghatározása
    - Rendszer/alrendszer/interfész
    - Alkalmazás/adatbázis/hardver és firmware/hálózat
- A biztonsági tesztelési terv frissítése
    - Biztonsági tesztelési eljárások kidolgozása
    - Biztonsági tesztelés abnormális és illegális körülmények között
- A biztonsági terület beillesztése a formális dokumentációba és a minőségbiztosításba

Fejlesztés és dokumentálás

- A biztonsággal kapcsolatos kód megírása és beillesztése
    - Hozzáférés-védelem a kódhoz
    - A kód dokumentálása
- A biztonsággal kapcsolatos kódok tesztelése és értékelése
- Annak ellenőrzése, hogy a jóváhagyott biztonsági komponensek megvalósultak-e

Elfogadás

- Biztonsági komponensek tesztelése
- Biztonsági tesztelés az integrált környezetben
    - A funkcionális működés és teljesítmény felmérése
    - A tesztelési hibák azonosítása
    - A teszteredmények összevetése a biztonsági követelményekkel
- A biztonsági kód telepítése a szükséges módosításokkal
- A biztonsági intézkedések dokumentálása
    - A felhasználói útmutatóknak tartalmaznia kell a biztonságos működés feltételeit
- Elfogadási tesztelés
    - Az utolsó lehetőség a sérülékenységek azonosítására
- A projekt biztonságosságának elfogadása/megerősítése

Telepítés

- Biztonsági minősítés megszerzése
- Felhasználók oktatása
- A rendszer élesüzemű telepítése

Üzemeltetés és fenntartás

- Mentési és visszaállítási tesztelések
- Biztonsági eljárások megfelelőségének ellenőrzése
- Periodikus kockázatelemzés
- Újratanúsítás
- A környezetet érintő változások hatásainak elemzése
- SLA megállapodások ellenőrzése

Áttekintés és kivonás

- A változások hatásait folyamatosan monitorozni kell
- Ha a változások olyan hatásokat váltanak ki a rendszerből, hogy azt már nem lehet gazdaságosan/biztonságosan üzemeltetni, akkor ki kell vonni a működésből
- A kivonásra megfelelő stratégiát kell kidolgozni.

A fentiek szerint a biztonsági tesztelési követelményeket már a funkcionális követelmények meghatározásánál figyelembe kell venni, majd háromféle részletességgel kell végrehajtani: kód, modul és integrált környezet szinten. Ez a három megközelítés egymástól lényegesen eltérő módszertan használatát kívánja meg.

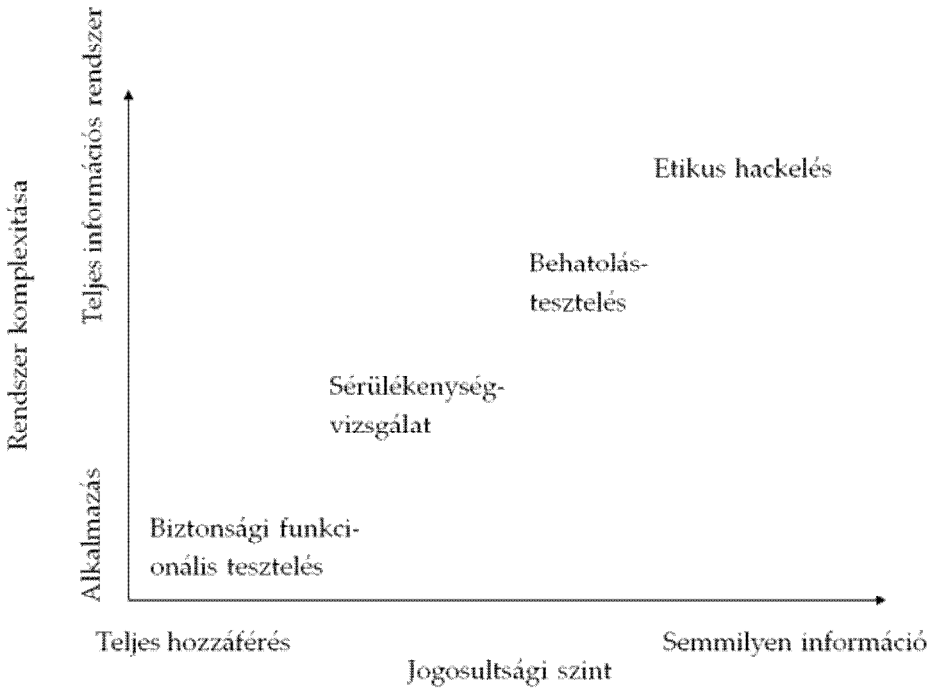
2. A BIZTONSÁGI TESZTELÉSI MÓDSZERTANOK BEMUTATÁSA

A biztonsági tesztelések módszertanával több, mérvadó ajánlás is foglalkozik. Ezek közül a legjelentősebbek az Open Source Security Testing Methodology Manual [1], mely az Institute for Security and Open Methodologies kiadványa, a NIST SP 800-115 Technical Guide to Information Security Testing and Assessment ajánlás [2], mely az amerikai kormányzat szabványa és az OWASP Testing Guide [3], amit az Open Web Application Security Project keretében fejlesztenek. A webes alkalmazások tesztelésének módszertanát ezek együttes használatával érdemes összeállítani.

A biztonsági tesztelési módszertanok csoportosítására jelenleg nincs egyezményes megállapodás, a tesztelt rendszerek ismeretétől kezdve, a hozzáférés mértékén át, a bevetett tesztelési eszközökig számos taxonómia létezik. Néhány fogalom azonban gyakran előfordul a szakirodalomban, melyek jól bemutatják a lehetséges módszereket [4].

- *Biztonsági funkcionális tesztelés*: az újonnan fejlesztett rendszer (alkalmazás) beépített védelmi kontrolljainak megfelelőségi ellenőrzése. Más néven white-box tesztelésnek is hívják, kód közeli megközelítésnek minősül. Pl. nézzük meg, hogy tényleg legalább 8 karaktert kell-e megadni jelszónak.
- *Sérülékenység-vizsgálat*: a rendszer (alkalmazás) védelmi kontrolljainál előforduló sebezhetőségek felderítése, tipikusan automatikus eszközökkel. Más néven black-box tesztelésként ismert, a modulszintű vizsgálatnak tekinthető. Pl. egyes bemeneteken olyan adatok megadása, melyekre a rendszer egyébként védett információkat ad át.
- *Behatolás-tesztelés:* az újonnan fejlesztett vagy már működő rendszer védelmi kontrolljainak kijátszása műszaki megoldásokkal, bármilyen kapcsolódó környezeti infrastruktúra felhasználásával. Két alfaja létezik, a Blue teaming, melynek során a tesztelő pontosan ismeri a tesztelt infrastruktúrát, és a Red teaming, melynél semmilyen ismerettel nem rendelkezik.
- *Etikus hackelés*: a működő rendszer védelmi kontrolljainak kijátszása bármilyen technikával, a rendszer előzetes ismerete nélkül. Ebbe beletartozik az emberi ráhatással (social engineering) történő támadás is.

A fenti technikákat a jogosultsági szint és a rendszer komplexitása szerint az 1. ábra mutatja be.



1. ábra: Biztonsági tesztelési módszertanok

A fenti módszerek közül a sérülékenység-vizsgálat és a behatolás-tesztelés a legelterjedtebb, használatát több forrásban is kötelező előírásként találhatjuk meg. A tipikusan amerikai szabványok, jogszabályok az informatikai biztonság egyik alapkövének tekintik az ilyen típusú teszteléseket. Az alábbi felsorolás összefoglalja a legelterjedtebb követelményeket.

- Payment Card Industry Data Security Standard (PCI DSS): a nagy bankkártya cégek kártyaadatok biztonságos elektronikus kezelésére vonatkozó előírása az ellenőrzés egyik legfontosabb alapkövének tekinti a sérülékenység-vizsgálatokat. A tanúsításhoz szükséges kétszintű vizsgálat mellett már az érintett rendszerek fejlesztését követően, a megrendelő számára is előírt a biztonsági tesztelés elvégzése. Az előírás 6.3.7 követelménye szerint a webes alkalmazásokat az OWASP útmutatói alapján kell fejleszteni és ezeket mintavételes módszerrel kell ellenőrizni (biztonsági funkcionális tesztelés), majd a 6.6 követelmény szerint manuális vagy automatikus módszerrel (sérülékenység-vizsgálat) legalább évente vagy minden változás után, egy erre specializálódott szervezettel (belső vagy külső) teszteltetni kell, és az esetleges hibák kijavítása után ezt a tesztet meg kell ismételni. [5]
- Federal Information Security Management Act (FISMA): Az USA 2002-ben elfogadott e-kormányzati törvénye alapján a központi ügynökségek valamennyi informatikai rendszerét biztonságos körülmények között kell üzemeltetni. [6] Az alapvető követelményeket a NIST SP 800-53 szabvány [7] tartalmazza, mely a magyar Közigazgatás Informatikai Bizottság 28. [8] ajánláshoz hasonlóan három besorolási szintet határoz meg a rendszerekre. Az előírások között RA-5 jelzéssel szerepel a sérülékenység-vizsgálat. Ez az automatikus eszközökkel végrehajtott tesztelést preferálja, melynek eredményeit egységes formájú jelentésben kell bemutatni. A vizsgálatot a szervezet által meghatározott időközönként vagy a rendszert érintő új sebezhetőség megjelenésekor kell végrehajtani. Közepes biztonsági szinten az automatikus eszköz használatát integrálni kell a változáskezelési eljárások közé, kiemelt szinten pedig a sebezhetőség-vizsgálati folyamatot kell továbbfejleszteni. A

külső értékelő által végzett, akár komplex vizsgálatok (behatolás-tesztelés) nem kötelező elem, de ajánlott teszteljárásként fel van tűntetve.

- Control Objectives for Information and related Technology (CObIT): Az elsősorban pénzintézeti szektorban használt IT irányítási ajánlás a DS5.5 Security Testing, Surveillance and Monitoring részben javasolja az informatikai rendszerek rendszeres biztonsági tesztelését, ám ennek módját nem jelzi. Az erre vonatkozó RACI táblázat viszont már nevén nevezi a sérülékenység-vizsgálatot, melynek végrehajtása a Megfelelőség, Audit, Kockázat és Biztonság szerepkör feladata. A biztonsággal kapcsolatos folyamat érettsége akkor tekinthető meghatározottnak, 3-as szintűnek, ha legalább ad hoc módon történnek ilyen vizsgálatok. [9]
- ISO/IEC 27002: A legismertebb információbiztonsági szabvány a 12.6. fejezetben foglalkozik a sérülékenység-vizsgálattal. Eszerint a szervezetnek bizonyos időközönként fel kell mérnie rendszerének technikai sebezhetőségeit, és megfelelő védelmi intézkedésekkel csökkenteni kell az ezekből eredő kockázatokat. A szabvány nem ad útmutatást a vizsgálat pontos végrehajtására, akár a gyártóktól érkező vagy hiteles forrásokban megjelent információk rendszeres olvasása is kielégíti a követelményeket. A lényeg, hogy a szervezet rendelkezzen ilyen típusú folyamattal. [10] A KIB 28. ajánlás ezt a szellemiséget követi az RS-2 Hibajavítás követelményben, de a folyamat szerepét meglehetősen eljelentéktelenítve.

A biztonsággal foglalkozó szabványok és ajánlások túlnyomó többsége tehát foglalkozik a biztonsági tesztelésekkel, de ezt eltérő szigorúsággal teszi. Jelen tanulmány célja, hogy ezek alapján egységes közigazgatási módszertant dolgozzon ki.

3. COMMON CRITERIA KÖVETELMÉNYEK

Egy webes alkalmazás biztonsági teszteléséhez a legjobb kiindulópontot a Common Criteria (CC) szabvány adja, melynek Common Evaluation Methodology (CEM) című kiadványának B melléklete részletesen leírja egy értékelő feladatait. [11] A CC terminológiájában a sebezhetőségi felmérés az a folyamat, melynek során a termék hibáinak vagy gyengeségeinek a létét és kihasználhatóságát elemzik. A tesztelést az értékelő végzi értékelői tesztelés módszerével. Alapszinten csak a nyilvános forrásból hozzáférhető sebezhetőségeket kell felderíteni (az ISO 27002 és a KIB 28. ajánlásoknak megfelelően), ám a rendszer biztonsági besorolása szerint ennél sokkal részletesebb vizsgálatokra is sor kerülhet. A sérülékenység-vizsgálat három lépésből áll: a lehetséges sebezhetőségek felderítése, a sebezhetőség kockázati besorolása és a sebezhetőség kihasználása annak megerősítésére, hogy az az adott környezetben valóban kihasználható.

A CC öt típusba sorolja a sebezhetőségeket:

- Kikerülés (bypassing): Ebbe a kategóriába tartozik minden olyan hiba, melynek során a rendszer beépített biztonsági eljárásait megkerülik, pl. jogosulatlan hozzáférés, kriptográfiai védelem feltörése.
- Meghamisítás (tampering): Olyan sebezhetőségek, melynek kihasználásával a termék működése módosítható, pl. a biztonsági funkciók leállítása vagy a fizikai módosítás.
- Direkt támadások (direct attacks): A permutációt vagy véletlenszerűséget felhasználó védelmi eljárások tesztelése tartozik ebbe a körbe, pl. jelszóhosszúságokon alapuló támadások.
- Megfigyelés (monitoring): Az információk átvitelének vagy kiszivárgásának figyelése és felhasználása, pl. információs csatornák lehallgatása, rejtett csatornák alkalmazása, elektromágneses sugárzás figyelése.

- Nem megfelelő használat (Misuse): Ez alatt a termék nem megfelelő dokumentációját, helytelen konfigurációját és szokásostól eltérő használatát értjük.

A fenti hibák felderítésére két útja lehet az értékelőnek. Egyrészt a vizsgálat során szembesülhet olyan sebezhetőségekkel, melyek kihasználása nem triviális, de minden valószínűség szerint lehetséges. Ezek többnyire olyan véletlen felfedezések, melyek a tesztelés „melléktermékei", nem direkt ezekre volt kíváncsi a tesztelő. Példa lehet erre egy olyan teszteredmény, mely a termékben puffer túlcsordulást okoz, ami akár a védelmi funkciók megkerülését is lehetővé teheti alaposabb elemzés után. A másik lehetséges elemzési mód a valamilyen elvek alapján felépített analízis. Ez lehet nem strukturált, amelynek során az értékelő saját tapasztalata alapján általános sebezhetőségeket keres, fókuszált, ami egyes sebezhetőnek tűnő területek alapos elemzését jelenti, vagy módszertan alapján történő, a korábban felsorolt ajánlásokra épülő.

Az értékelési eljárás azonban elsősorban a támadási potenciál szintjétől függ. A tesztelés előtt el kell dönteni, hogy a termék milyen környezetben fog működni, és ennek alapján négy kategóriába lehet sorolni a lehetséges támadói képességeket: alap, alap-erősített, mérsékelt, magas. A Közigazgatási Informatikai Bizottság 25. számú ajánlása szerint besorolásban a magyar közigazgatási rendszereket alacsony és fokozott kihatású esetben alap-erősített, kiemelt kihatású esetben mérsékelt szintű sebezhetőség-vizsgálatnak kell alávetni. [12] Ez azt jelenti, hogy az értékelő a tesztelést olyan támadási kapacitással végzi el, ami az előírt szinten meg van adva. Természetesen az eljárás során felderíthetnek olyan sebezhetőségeket is, melyek az adott támadási szinten nem kihasználhatók, ilyenkor a fejlesztőnek/megrendelőnek kell meghoznia azt a döntést, hogy ezt a kockázatot elfogadja vagy nem.

A támadási potenciál kiszámolásához a CC kiváló segédletet nyújt. 5 paraméter segítségével meghatározható, hogy a tesztelő milyen körülmények között végezze el a vizsgálatát. Ezek a következők:

- a sebezhetőség sikeres kihasználáshoz szükséges idő (eltelt idő), lehetséges értékei: egy napnál kevesebb, egy nap és egy hét között, egy hét és két hét között, két hét és egy hónap között, egy hónap és hat hónap között, hat hónapnál több.
- a kihasználáshoz szükséges szakértelem (szakértelem szintje), lehetséges értékei: laikus (általános ismeretei vannak), profi (jól ismeri az adott terméktípust), szakértő (széleskörű ismeretei vannak a támadási technikákról), több szakértő (részterületek szakértői).
- a vizsgált termék felépítésének és működésének ismerete (termékismeret), lehetséges értékei: nyilvános információk (internetről elérhető), korlátozott információk (a fejlesztői közösségen belül ismert), érzékeny információk (csak egy speciális fejlesztői csapat által ismert), kritikus információk (csak néhány személy által ismert).
- a sikeres támadáshoz szükséges hozzáférés ideje és a próbálkozások száma (próbálkozási ablak), értékei: korlátlan (a támadás észrevétlen marad), egyszerű (egy napnál rövidebb ideig tartó hozzáférés, 10-nél kevesebb próbálkozás), mérsékelt (egy hónapnál rövidebb ideig tartó hozzáférés, 100-nál kevesebb próbálkozás), nehéz (legalább egy hónapig tartó hozzáférés vagy legalább 100 próbálkozás), nincs (a rendelkezésre álló idő vagy próbálkozásszám nem elégséges egy sikeres támadás véghezviteléhez).
- a támadás kivitelezéséhez szükséges hardverek és szoftverek (eszköztár), lehetséges értékei: szabványos eszközök (internetről szabadon letölthető), speciális eszközök (piacon beszerezhető), egyedi eszközök (adott célra fejlesztett), több egyedi eszköz (résztámadások egyedi eszközei).

A CC minden lehetséges értékhez egy számot rendel, melyek összege adja a támadási potenciált. A forgatókönyvek összeállításánál külső támadókkal számolunk, hiszen az e-

közigazgatási rendszerek üzemeltetői azzal számolnak, hogy legitim felhasználóik megbízhatóak. Természetesen a gyakorlat azt mutatja, hogy az ilyen támadásokat is szimulálni kell, ez azonban csak ajánlott, célunk az, hogy alapvető technikák felhasználásával jelentősen emeljük az ilyen rendszerek biztonsági szintjét.

Az alap-erősített támadási potenciál eléréshez a tesztelési forgatókönyv összeállításánál egy olyan támadóval kell számolni, aki bár ismeri a támadási technikákat, azokat csak nyilvánosan elérhető eszközök felhasználásával tudja végrehajtani. Célja a könnyen azonosítható hibák felderítése, melyet segítenek a rendszerről kiszivárgó információk. A szakzsargonban script-kiddie[2] névvel ellátott képességeket értjük ide. Ehhez a paraméterek: eltelt idő egy hónap, a szakértelem szintje profi, a termékismeret korlátozott információ, a próbálkozási ablak egyszerű, az eszköztár pedig szabványos.

A mérsékelt vizsgálat szimulált támadója olyan magas tudással rendelkező szakértő, aki képes hamar észrevenni az elemi hibákat, és ezekhez akár saját eszközöket is tud fejleszteni. A rendszer azonban megfelelően védett, arról semmilyen információ nem szivárgott ki. A szakszóval cracker-nek[3] vagy black hat hackernek nevezett személyek képességeit mutatja be. Ennek a támadásnak a paraméterei: eltelt idő egy hét, a szakértelem szintje szakértő, termékismeret nyilvános, próbálkozási ablak egyszerű, eszköztár egyedi eszközök.

Az OWASP Application Security Verification Standard Project (ASVS) a Common Criteriához hasonló elvek alapján különböző szintű ellenőrzésekre tesz javaslatot az elkészült alkalmazásban, így a hasznos kiegészítője lehet a szabványnak.

4. TIPIKUS TÁMADÁSI FELÜLETEK

Az Open Web Applications Security Project (OWASP) keretében 2003 óta rendszeresen közzéteszik a webes alkalmazásokra vonatkozó nagy kockázatú sebezhetőségeket. Az OWASP Top 10 2010-es kiadása [13] alapján a behatolás-tesztelés olyan módszertana állítható össze, mely segít a legtipikusabb hibák felderítésében, így jelentősen növekedhet az alkalmazás biztonsági szintje. A legnagyobb kockázatú hibák felsorolása az alábbiakban található.

A1 – Beszúrásos támadások (Injection): A beszúrásos hibák, melyek közé elsősorban az SQL, operációs rendszer és LDAP injection értendő, olyankor történnek, amikor a támadó nem megbízható adatokat küld a parancsfeldolgozó felé parancsként vagy lekérdezésként. A támadó kód eléri a parancsfeldolgozónál, hogy az nem kívánt parancsot hajtson végre, vagy érzékeny adatokat szivárogtasson ki.

A2 – Cross-Site Scripting (XSS): Az XSS hibák jellemzője, hogy egy alkalmazás nem megbízható adatokat vesz át és küld tovább a böngészőn keresztül megfelelő ellenőrzés és szűrés nélkül. Az XSS lehetővé teszi a támadónak, hogy szkripteket hajtson végre az áldozat böngészőjében, mellyel el tudja téríteni a felhasználó session-jét, weboldalakat tud megváltoztatni vagy át tudja irányítani a felhasználót egy kártékony oldalra.

A3 – Hibás hitelesítés és sessionkezelés (Broken Authentication and Session Management): Az alkalmazások hitelesítéshez és sessionkezeléshez kapcsolódó funkciói sok esetben nem megfelelően lettek implementálva, ezért lehetővé válik a jelszavak, kulcsok, session tokenek megszerzése, vagy más hibák előidézése, melynek segítségével a támadó más, jogosult felhasználó nevében tud eljárni.

A4 – Nem biztonságos direkt objektumhivatkozás (Insecure Direct Object References): Direkt objektumhivatkozásról akkor beszélünk, amikor a fejlesztő felfed egy hivatkozást valamilyen belső, implementációhoz szükséges objektum felé, mint pl. egy fájl, könyvtár

[2] http://en.wikipedia.org/wiki/Script_kiddie
[3] http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Black_hat

vagy adatbázis tábla. Megfelelő hozzáférés-védelem vagy más biztonsági megoldás nélkül a támadó vissza tud élni ezekkel a hivatkozásokkal, és nem jogosult hozzáférést szerezhet az ezekben tárolt adatokhoz.

A5 –Cross-Site Request Forgery (CSRF): A CSRF támadás során a támadó kényszeríti az authentikált felhasználó böngészőjét arra, hogy egy hamisított HTTP kérést küldjön egy sebezhető webalkalmazás felé, mely tartalmazza az áldozat session cookie-ját és más hitelesítési információkat. Ez lehetővé teszi, hogy az áldozat böngészője olyan kéréseket küldjön a sebezhető alkalmazás felé a támadó nevében, melyről azt hiszi, hogy az legitim forrásból érkezik.

A6 – Helytelen biztonsági beállítások (Security Misconfiguration): A megfelelő biztonság eléréséhez meg kell határozni az alapvető beállításokat, és ezeket meg is kell valósítani az alkalmazásokban, keretrendszerekben, alkalmazásszervereken, webszervereken, adatbázis-szervereken és minden más érintett platformon. Mivel a legtöbb rendszer nem olyan alapbeállítással kerül telepítésre, mely az elvárható biztonsági szintet valósítja meg, ezeket a konfigurációkat meg kell határozni, implementálni kell, és folyamatosan fenn kell tartani. A folyamat során a szoftverek frissítéseire is figyelemmel kell lenni.

A7 – Nem megfelelő kriptográfiai tárolás (Insecure Cryptographic Storage): Számos webalkalmazás nem megfelelően kezeli az érzékeny adatokat, mint pl. a hitelesítési adatok, mert ezeket nem titkosított vagy lenyomatolt formában őrzi. A támadók ezért megszerezhetik vagy módosíthatják a gyengén őrzött adatokat, ami számos visszaéléshez vezethet.

A8 – URL hozzáférés korlátozásának hibája (Failure to Restrict URL Access): A webes alkalmazásokban fontos az URL-ek hozzáférési jogainak ellenőrzése, mielőtt a felhasználó elérne egy védett hivatkozást vagy akciógombot. Ezt a hozzáférési jog ellenőrzést viszont minden esetben meg kell tenni, amikor ezeket a védett oldalakat elérik, mert különben a támadó elérheti a rejtett oldalakat.

A9 – Nem megfelelő szállítási réteg védelem (Insufficient Transport Layer Protection): Az alkalmazások gyakran nem megfelelő hitelesítést, titkosítást és bizalmasság-sértetlenség védelmet használnak az érzékeny hálózati forgalomban. Amikor viszont használnak, akkor is gyenge algoritmusokkal, lejárt vagy érvénytelen tanúsítványokkal teszik ezt, vagy egyszerűen nem megfelelően használják a kriptográfia adta lehetőségeket.

A10 – Nem ellenőrzött átirányítások és továbbítások (Unvalidated Redirects and Forwards): A webes alkalmazások gyakran irányítják át vagy továbbítják a felhasználókat más oldalakra, és használnak nem hiteles adatokat a forrásoldal megállapítására. Megfelelő ellenőrzés nélkül a támadók átirányíthatják a felhasználókat adathalász vagy kártékony oldalakra, vagy a továbbításokkal nem jogosult hozzáférést szerezhetnek.

A Common Criteria szerint besorolás a következő:

- Kikerülés: A2, A4, A5, A8
- Meghamisítás: A1, A10
- Direkt támadások: A3, A7
- Megfigyelés: A9
- Nem megfelelő használat: A6

5. VIZSGÁLATI MÓDSZERTAN

A webes alkalmazások teszteléséhez az Open Web Application Security Project keretében megalkotott módszertanok tekinthetők a leghasznosabbaknak, legalábbis ezekre hivatkozik a legtöbbet a szakirodalom napjainkban. Az OWASP kétfelé bontotta az ellenőrzési folyamatokat. Az OWASP Code Review Guide (CRG) [14] célja a létrehozott kódok manuális ellenőrzése, white-box módon. Gyakorlatilag a biztonsági funkcionális tesztelésnek

felel meg. Az OWASP Testing Guide (TG) a már elkészült alkalmazás black-box teszteléséhez, azaz sérülékenység-vizsgálatához ad segítséget.

A CRG tehát a kódok áttekintésére készült, mely folyamat célja meggyőződni arról, hogy a forráskódban a megfelelő biztonsági kontrollok implementálásra kerültek és úgy működnek, ahogy a tervezés szerint működniük kell. Ellenőrzi továbbá azt is, hogy a biztonsági kódokért felelős fejlesztők követték a számukra megállapított eljárásrendeket. Mivel a behatolás-tesztelés, de még a sérülékenység-vizsgálat sem képes teljes körűen felderíteni az esetleges hibákat, egyedül a white-box tesztelésnél van lehetőség a rosszul megírt kódrészleteket átfogóan megtalálni. A biztonsági funkcionális tesztelés a humán erőforrás és a célszoftverek alkalmazását is szükségessé teszi. Az automatizált eszközök itt a leghatékonyabbak, de nem képesek teljes mértékben pótolni a tesztelési szakembert, hiszen az egyes kontextusok döntően befolyásolhatják a kódolás megfelelőségét vagy nem megfelelőségét.

A CRG a legfontosabb technikai kontrolloknak az authentikációt, az authorizációt. a sessionkezelést, az input validációt, a hibakezelést, az alkalmazás telepítését és a kriptográfiát tartja, többé-kevésbé összhangban a Common Criteria 2. kötetében leírt biztonsági funkcionális követelményekkel. A legkomolyabb programozáskor elkövetett hibaforrásoknak pedig a puffer túlcsordulást, az operációs rendszer és SQL injektálást, az adatvalidációt, a cross-site scriptinget, a cross-site request forgery-t, a naplózási hiányosságokat, a session sértetlenségét és a versenyhelyzeteket tartja, szinkronban az OWASP Top 10 megállapításaival. A CRG részletesen bemutatja azokat a tipikus hibákat, amiket a biztonsági funkciók implementálásánál el szoktak követni, illetve azt is, hogyan lehet a programozási hibákat felderíteni.

A biztonsági funkcionális tesztelés azonban idő- és erőforrás-igényes, tehát drága. Emellett a szükséges szakértői háttér is nehezen elérhető Magyarországon. Célravezetőbb a TG-ben leírt sérülékenység-vizsgálatokat végrehajtani, ami nem jelent ugyan akkora bizonyságot, mint a CRG folyamatai, de így is jelentősen tudja csökkenteni a támadási felületeket. A TG az OWASP Top 10 fenyegetéseit veszi sorra, és írja le, hogy milyen tesztelési eljárásokkal lehet meggyőződni arról, hogy a kész alkalmazás ellenáll ezeknek. Black-box tesztelés esetén az automatikus teszteszközök már körülményesebben használhatók, de még bevethetők. Ezért az egyes tesztesetekhez konfigurálható céleszközöket szoktak használni, mely feltételezi, hogy a tesztelő jól ismeri ezt a területet.

A TG 9 kategóriában 66 tesztesetet határoz meg. Az alkalmazás típusától és megvalósításától függően kell ezeket végrehajtani.

Információszerzés:

- Webes keresők robotjai
- Felderítés webes keresők adatbázisában
- Alkalmazás belépési pontjainak azonosítása
- A webes alkalmazás ujjlenyomatának tesztelése
- Alkalmazás felderítés
- Hibaüzenetek elemzése

Konfigurációmenedzsment tesztelés

- SSL/TLS tesztelés
- DB Listener tesztelés
- Infrastruktúra konfigurációmenedzsmentjének tesztelése
- Alkalmazás konfigurációmenedzsmentjének tesztelése
- Fájlkiterjesztés kezelésének tesztelése
- Régi, mentett és nem hivatkozott fájlok
- Infrastruktúra és alkalmazás adminisztrátori interfészek
- HTTP metódusok és XST tesztelés

Authentikációs eljárások tesztelése

- Authentikációs adatok átvitele biztonságos csatornán keresztül
- Felhasználói adatbázis tesztelése
- Kitalálható (szótár alapú) felhasználói fiókok felderítése
- Nyers erejű tesztelés
- Az authentikációs séma kikerülésének tesztelése
- Sebezhető emléketető jelszó és jelszó visszaállítási lehetőségek
- Kilépés és böngésző cache menedzsment
- CAPTCHA kódok
- Többfaktorú authentikáció tesztelése
- Versenyhelyzetek kezelése

Sessionkezelés

- A sessionkezelési séma tesztelése
- Cookie attribútumok
- Session fixálás
- Kiterjesztett sessionváltozók tesztelése
- CSRF

Authorizáció tesztelése

- Elérési útvonalak tesztelése
- Az authorizációs séma kikerülése
- Jogosultság kiterjesztése

Üzleti logika

- Az üzleti logika tesztelése

Adatvalidáció:

- Nem perzisztens XSS
- Perzisztens XSS
- DOM alapú XSS
- Cross Site Flashing
- SQL Injection
- LDAP Injection
- ORM Injection
- XML Injection
- SSI Injection
- XPath Injection
- IMAP/SMTP Injection
- Kódbeszúrás
- Operációs rendszer parancsok kiadása
- Puffer túlcsordulás
- Összetett adatvalidációs tesztelés
- HTTP splitting/smuggling tesztelés

Túlterheléses támadások (DoS) tesztelése

- SQL wildcard támadás
- Ügyfélfiókok zárolása
- DoS puffer túlcsordulások tesztelése
- Felhasználó által meghatározott objektumallokáció
- Felhasználói adatbevitel, mint körbeforgó számláló
- Felhasználó által bevitt adatok lemezre írása
- Erőforrás sikertelen elengedése

- Túl sok adat tárolása egy session-ben

Web service tesztelés

- Web service információszerzés
- WSDL tesztelés
- XML struktúra tesztelés
- XML tartalom szintű tesztelése
- HTTP GET paraméterek/REST tesztelés
- SOAP csatolások
- Visszajátszásos támadás

AJAX tesztelés

- AJAX sebezhetőségek
- AJAX tesztelés

ÖSSZEFOGLALÁS

Az 1. fejezetben ismertetésre került a biztonságos alkalmazásfejlesztés folyamata, melynek alapvető része a biztonsági tesztelés. A 2. fejezetben bemutattuk a szóba jöhető módszertanok és azok a megfelelőségi követelmények, melyek kötelező módon előírják a sebezhetőség-vizsgálatok lefolytatását. Ezekből egyértelműen következik, hogy a modern e-közigazgatási rendszerek fejlesztésénél elkerülhetetlen az ilyen vizsgálatok lefolytatása. A 3. fejezetben meghatározásra került, hogy a magyar elektronikus közigazgatási rendszerekben milyen támadói profilt kell szimulálni a követelmények alapján. A 4. fejezetben a legfontosabb webes biztonsági fenyegetések leírásával egyértelművé tettük, milyen hibák kiküszöbölése elvárható minimálisan a fejlesztőktől, és mely területekre kell a tesztelőknek fókuszálnia. Végül az 5. fejezetben megneveztük azt a két módszertant, melynek segítségével a biztonsági funkcionális tesztelés és a sérülékenység-vizsgálat a leghatékonyabban megtervezhető.

Az érintett rendszerek megrendelőinek ezek alapján egyértelmű segédlet áll rendelkezésre a biztonsági vizsgálatok követelményeinek meghatározásához. A pontos keretek természetesen csak a rendszer ismeretében határozhatók meg, de ha a biztonság fontos kritérium, – márpedig a tapasztalatok szerint az – már a tender kiírása során figyelmet kell fordítani az ilyen részletekre is.

IRODALOMJEGYZÉK

1. Herzog, Pete. *Open-Source Security Testing Methodology Manual 2.2.* s.l. : Institute for Security and Open Methodologies, 2006.
2. Scarfone, Karen, et al. *Technical Guide to Information Security Testing and Assessment.* Gaithersburg : National Institute of Standards and Technology, 2008. NIST Special Publication 800-115.
3. Meucci, Matteo (szerk.). *OWASP Testing Guide V3.0.* s.l. : Open Web Application Security Project, 2008.
4. Krasznay, Csaba. A rendszer próbája: az etikus hackelés és penetrációs tesztelés. *krasznay.hu.* [Online] június 18, 2008. [Cited: április 22, 2010.] http://www.krasznay.hu/presentation/ethical_hacking_krasznay.ppt.
5. PCI Security Standards Council LLC. *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 1.2.1.* s.l. : PCI Security Standards Council LLC, 2009.

6. National Institute of Standards and Technology. Federal Information Security Management Act (FISMA) Implementation Project. *NIST.gov - Computer Security Division - Computer Security Resource Center.* [Online] National Institute of Standards and Technology, április 13, 2010. [Cited: április 22, 2010.] http://csrc.nist.gov/groups/SMA/fisma/index.html.

7. —. *Recommended Security Controls for Federal Information Systems and Organizations.* Gaithersburg : National Institute of Standards and Technology, 2009. NIST Special Publication 800-53.

8. e-Közigazgatási Keretrendszer Kialakítása projekt. *IT biztonsági műszaki követelmények.* Budapest : Miniszterelnöki Hivatal Elektronikuskormányzat-Központ, 2008. Közigazgatási Informatikai Bizottság 28. számú ajánlása.

9. IT Governance Institute. *Control Objectives for Information and related Technology (COBIT®) v4.1.* Rolling Meadows : IT Governance Institute, 2007. ISBN 1-933284-72-2.

10. International Organization for Standardization. *Code of practice for information security management.* Geneva : International Organization for Standardization, 2005. ISO/IEC 27002:2005.

11. Common Criteria Recognition Arrangement. *Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3.* s.l. : Common Criteria Recognition Arrangement, 2009. ISO/IEC 18045.

12. Krasznay, Csaba. Szoftverfejlesztői követelmények minősített környezetben. *Hadmérnök.* 2009, Vol. IV, 4.

13. Williams, Jeff and Wichers, Dave. *OWASP Top 10 - The Ten Most Critical Web Application Security Risks.* s.l. : Open Web Application Security Project, 2010.

14. Keary, Eoin (szerk.). *OWASP Code Review Guide.* s.l. : Open Web Applications Security Project, 2008.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Lipics László
laszlo_lipics@yahoo.de

A SCHENGENI INFORMÁCIÓS RENDSZER SZEREPE AZ INTEGRÁLT HATÁRBIZTONSÁGI RENDSZERBEN

Absztrakt

A szerző jelen cikkben bemutatja a Schengeni Információs Rendszer (SIS) kialakulásának rövid történetét, valamint az integrált határbiztonsági rendszert. Az integrált határbiztonsági rendszerből kiemelt három olyan területet, amelyben a SIS alkalmazása szükséges, illetve bemutat két olyan további intézkedést, melyek során a SIS-ben történő ellenőrzés elengedhetetlen. Magyar példán keresztül bemutatja a SIS hasznosságát, és a felfedések számában várhatóan bekövetkező változásokról, valamint a rendszer fejlesztéséről is ír.

The author demonstrated in this article the short formation's history of Schengen Information System (SIS) and the integrated border system. Out of the integrated border system he picked three fields, in which SIS using is needed. Moreover he demonstrated two measures, where the SIS control is indispensible.
Why SIS is useful – we can read about it through a Hungarian precedent, and he wrote about changes of hit's number, which are to be expected. The author presented the development of system.

***Kulcsszavak**: fejlesztés, alkalmazás, idegenrendészet, rendőri ellenőrzés, SIS ~ development, application, foreign-order, police control, SIS*

A cikkemben be kívánom mutatni a Schengeni Információs Rendszer kialakulásának rövid történetét, felépítését, jelenlegi fejlesztését.
A Schengeni Egyezmény aláírói szerint a SIS a határellenőrzések, az országon belül végzett rendőrségi és vámellenőrzések, továbbá a vízumok és tartózkodási engedélyek kiállítása, valamint az idegenrendészeti jogszabályok alkalmazása céljából lett létrehozva.
Hipotézisem szerint a SIS önmagában nemcsak a fenti ellenőrzések során, hanem az integrált határbiztonsági rendszer több elemében is segíti a külföldiekkel kapcsolatos ellenőrzések véghezvitelét. A SIS alkalmazására pedig azért van szükség, mert a belső határok nélküli térségben - a Római Szerződésben foglalt szabadságjogokkal élve - mindenki és minden szabadon mozoghat, egy-egy rendőri ellenőrzés során pedig kiszűrhetőek a jogellenesen használt járművek, a beutazási és tartózkodási tilalom alatt álló személyek. Be kívánom bizonyítani azon feltevésemet, hogy a SIS Magyarország, valamint a schengeni térség biztonságához is hozzájárul.

Ezért röviden be kívánom mutatni az integrált határbiztonsági rendszert, annak elemeit. Le kívánom írni, hogy a határbiztonsági rendszer mely elemeiben használható fel a SIS, illetve Magyarországon mely szervek, milyen adatkörbe tekinthetnek be a SIS-be.
Cikkemben ismertetem továbbá a rendőri ellenőrzések során felfedett SIS találatokat, illetve azon okokat, melyek elgondolásom szerint csökkenést fognak okozni a feledések számában.

1. AZ ELSŐ KÖZÖS RENDSZER KIALAKULÁSA

Az Európai Unió a három szervezetből álló Európai Közösségekre alapulva jött létre 1957-ben. Az Európai Közösségeket hat ország - Németország, Franciaország, Olaszország, Belgium, Hollandia és Luxemburg – alapította.[1]

Az Európai Közösségek három szerződéshez köthetőek: az Európai Szén- és Acélközösséghez, az Európai Gazdasági Közösséghez, valamint az Európai Atomenergia Közösséghez, melyek 1967-ben olvadtak össze.

1992-ben a Maastrichti Szerződés (MSZ) aláírásával alakult meg az Európai Unió. Az egyezmény a tagállamok közötti együttműködés új formáit vezette be. Az Európai Unió alapja az ún. három pillér lett. Az első pillért az Európai Közösségek alkotják, a második pillér a közös kül- és biztonságpolitika, a harmadik pillér – eredeti elnevezés szerint - a bel- és igazságügyi együttműködés.[1] A szerződés 1993. november elsején lépett hatályba.

A közös piac egy igazi egységes piacot jelent, amely biztosítja az áruk, szolgáltatások, személyek és a tőke szabad mozgását. A szabad mozgás eredménye az, hogy először a közös határokon megszüntették a vámellenőrzést, majd a Schengeni Egyezmény hatályba lépésével folyamatosan (az abban részt vevő tagállamok közt) a személyellenőrzést. Ennek egyik eredménye az uniós polgárok nagyobb mobilitása, valamint a kívülről érkezők szabadabb mozgása.

A MSZ szerinti felosztásban, az Európai Unió közösségi politikájának tizenhárom területe közül a II. a Bel- és Igazságügyi Együttműködés, mely eredetileg az Európai Unió harmadik pillére volt. Területei: menekültügy, tagállamok külső határainak ellenőrzése, bevándorlási politika, kábítószer elleni küzdelem, nemzetközi korrupció elleni küzdelem, igazságszolgáltatási együttműködés a polgári és a büntetőjog területén, vámügyi együttműködés, rendőrségi együttműködés a terrorizmus, a kábítószer-kereskedelem, illetve a nemzetközi bűnözés egyéb formái ellen, rendőrségi és büntetőjogi igazságügyi együttműködés.

Az Amszterdami Szerződés (ASZ)[2] tulajdonképpen ebbe a közösségi politikába emelte be a Schengeni vívmányokat (ún. Schengen acquis). Az új egyezmény generális változásokat is hozott, nem véletlenül említik az Európai Unió első reformjaként. Az I. pillérbe átkerült, azaz közösségi szintre emelkedtek ez egyes területek: menekültügyi politika, a vízumpolitika és a külső határ ellenőrzése, bevándorlási politika, a személyek szabad mozgásához kapcsolódó egyéb politikák. Az ASZ elfogadott módosításai után az Európai Unió Működéséről szóló szerződés új VI. címe „Rendőrségi és igazságügyi együttműködés büntetőügyekben".

A Lisszaboni Szerződés [2], mely 2009. decemberében lépett hatályba megváltoztatta mind az Európai Unióról, mind az Európai Unió Működéséről szóló szerződést. Ez utóbbi harmadik része, mely az Unió belső politikái és tevékenységeiről szól, immár 24 közös területet

[1] Az Európai Unió tagjai: 1957. (alapítás) óta: Belgium, Franciaország, Hollandia, Luxemburg, Németország, Olaszország; 1973. óta: Dánia, Írország, Nagy Britannia; 1981. óta: Görögország; 1986. óta: Portugália, Spanyolország; 1995. óta: Ausztria, Finnország, Svédország; 2004. óta: Ciprus, Csehország, Észtország, Lengyelország, Lettország, Litvánia, Magyarország, Málta, Szlovákia, Szlovénia; 2007-től: Románia, Bulgária.
[2] Egyes források Amszterdami Egyezményként is említik (pl.: Dr. Virányi Gergely: A schengeni integráció és az Európai Unió RTF, Bp.2003.)

tartalmaz. A módosítás érintette a bel- és igazságügyi együttműködést is, mely az V. címbe került, új néven: A szabadságon, a biztonságon és a jog érvényesülésén alapuló térség.

Már a Római Szerződés aláírásakor tervbe vették a tagállamok lakóinak szabad lakó- és munkahelyválasztását. Akkor még szűkebb értelemben, a másik tagállamban munkát vállalókra gondoltak.

1985. június 14-én Luxemburgban, Schengenben öt EU-tagország[3] megkötötte az immár történelmi jelentőségűnek nevezhető egyezményt: „A határellenőrzésnek a közös határokon történő fokozatos megszüntetéséről".[3] A szerződésnek két fő része van, melyek címként jelentek meg. Egyrészt az egyezmény részes államai rövidtávon, a személyellenőrzés megkönnyítését célzó intézkedésekben állapodtak meg. Ezen intézkedések közül néhány már az egyezmény megkötését követő napon életbe lépett (pl. a vizuális ellenőrzés megkönnyítése érdekében az EU állampolgárok egy legalább 8 cm átmérőjű zöld korongot ragaszthatnak a gépkocsi szélvédőjére).

Ezzel az egyezménnyel ugyanakkor a hosszú távú intézkedések között a közös határok (belső határ) lebontásával együtt járó biztonsági deficit elleni kompenzációs intézkedéseket segítő programot határoztak meg.

Az egyezmény programja képezte később azoknak a tárgyalásoknak az alapját, amelyek a Schengeni Végrehajtási Egyezmény megkötéséhez vezettek.

Az SE- ben foglalt forgatókönyv végrehajtása alapján 1990. június 19-én lehetővé tették az öt alapító tagállam számára a Schengeni Végrehajtási Egyezmény [4] megkötését.

A jogforrásnak kettős hatálybaléptetése volt. A kettősséget az okozta, hogy – többek között a második fejezetben szereplő belső határellenőrzés megszüntetése – a Végrehajtó Bizottság külön határozatával történt. Így gyakorlatilag az SVE 1993. szeptember elsején lépett hatályba, míg a második lépcsőre, azaz a belső határok lebontására csak 1995. március 26-án kerülhetett sor,[5] akkor már hét tagállam[4] részvételével.

Az egyezmény nyolc fő részt (Címek) tartalmaz:

I. Meghatározások
II. Az ellenőrzés megszüntetése a belső határokon a személyforgalomban
III. Rendőrség és biztonság
IV. *Schengeni Információs Rendszer*
V. Szállítás és áruforgalom
VI. Adatvédelem
VII. Végrehajtó Bizottság
VIII. Záró rendelkezések

Azaz a SVE-ben, mint jogforrásban került először nevesítésre egy nemzetközi, közös információs rendszer, melynek célja a határ- és az országon belül végzett rendőrségi és vámellenőrzések megkönnyítése, továbbá a vízumok és tartózkodási engedélyek kiállítása, valamint az idegenrendészeti jogszabályok alkalmazásának ellenőrzése.

2. INTEGRÁLT HATÁRBIZTONSÁGI RENDSZER

Az Európai Közösség - a Hágai Programban foglaltaknak megfelelően - az integrált határbiztonsági modell /Integrált határmenedzsment (IBM – Integrated Border Management)/ elfogadásával a közösségi határrendészet egy teljesen új határellenőrzési politikát hozott létre. Korábban a határigazgatással összefüggő elgondolások, koncepciók fogalmi meghatározásai sem voltak egységesek az egyes schengeni tagállamokban, így azok 2002-től történt újraértelmezésével már egységes gondolkodásmódot honosított meg. Ez abból a szempontból

[3] Franciaország, Németország, Belgium, Hollandia, Luxemburg
[4] Spanyolország és Portugália csatlakozott az ötökhöz

fontos, hogy a határellenőrzés, mint első pilléres joganyag, minden tagállam számára kötelező érvényű.

Integrált határbiztonsági modellnek a Schengeni Megállapodás Végrehajtását Értékelő Munkacsoport által összeállított „Az ajánlások és az élenjáró gyakorlat katalógusa" volt az alapja, mely négy, egymást kiegészítő szintet fogott át:

1. Harmadik országban, különösen a származási és tranzitországokban végzett tevékenység, beleértve az összekötő tisztviselő segítségével történő információgyűjtést,
2. Nemzetközi határőrizeti együttműködés,
3. Intézkedések a külső határokon: határigazgatás,
4. További tevékenységek a schengeni államok területén és a schengeni államok között.

Az átfogó határmodell a belső biztonság megőrzésének és mindenekelőtt az illegális migráció, mint biztonsági kockázat megakadályozásának fontos eszköze. A gyakorlatban ez azt jelenti, hogy egymást kiegészítő intézkedéseket kell végrehajtani, különböző szinteken. Az általános határmodell sikerének kulcsát az intézkedések egymásra épülése, koherenciája jelenti, valamint az, hogy azokat a schengeni államok azonos módon alkalmazzák.

Magyarország 2007. december 21 óta teljes jogú schengeni tagállam. Ennek eléréséhez szükséges volt a hazai határbiztonsági rendszer kialakítása és működtetése. Az európai uniós határbiztonsági elemeket több, kisebb egységre bontotta (kiemelések tőlem):

1. politikai, gazdasági és egyéb tájékoztató eszközök a migráció kezelésében;
2. *egységes vízumrendszer alkalmazása*;
3. kihelyezett okmányszakértők, okmánytanácsadók;
4. összekötő tisztviselők alkalmazása;
5. szállító vállalatok felelőssége;
6. az illegális migrációban érintett tranzitállamok határellenőrzési rendszere;
7. biztonságos harmadik országok;
8. *külső határok ellenőrzése* (szigorú határőrizet és egységes határforgalom-ellenőrzés);
9. *kiegyenlítő (kompenzációs) intézkedések* rendszere az ország mélységében;
10. belső határon végzett rendészeti tevékenységek.

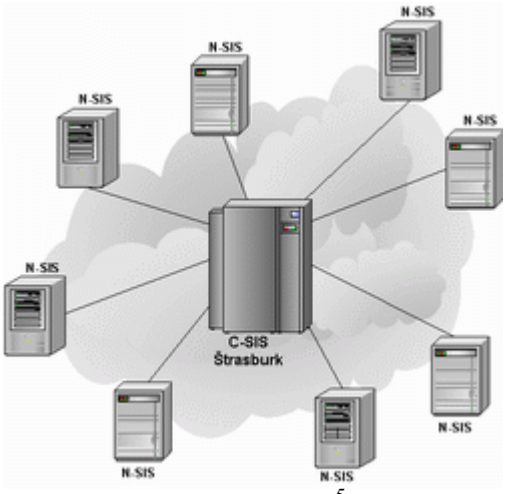
Az egyes szintek szerves részei a hazai határbiztonsági rendszernek. A határbiztonsági rendszerből adódó honi határellenőrzési feladatokat a Rendőrség hajtja végre. Az ORFK utasítás [6] leírja, hogy „a határbiztonsági rendszer működését és hatékonyságát minden, a határbiztonsággal összefüggésben feladatot végző szervezet biztosítja." Természetesen ez alapvetően a Rendőrség feladata, de a rendszer működtetése során a korábban kialakított rendszerhez hasonlóan együttműködik a Bevándorlási és Állampolgársági Hivatallal, a Külügyminisztérium egyes szervezeti elemeivel, a Vám- és Pénzügyőrséggel, az Országos Munkavédelmi és Munkaügyi Főfelügyelőséggel valamint a Nemzeti Közlekedési Hatósággal.[7]

3. A SCHENGENI INFORMÁCIÓS RENDSZER

A Schengeni Egyezmény céljaként megfogalmazott a személyek szabad mozgása, illetve a Schengeni Végrehajtási Egyezményben a személyek mozgására vonatkozó rendelkezéseinek alkalmazásához kapcsolódó feladatok ellátása érdekében a részt vevő országok közös információs rendszert (Schengeni Információs Rendszer - SIS) hoztak létre.

A rendszer a közös, központi egységből (mely Strasbourgban található), valamint az egyes országok nemzeti egységéből és a technikai támogatóegységből áll. A rendszerben tárolt adatokhoz a szerződő felek által kijelölt hatóságok számára lehetővé teszi, hogy automatizált lekérdezési eljárás révén hozzáférjenek a személyekkel és tárgyakkal kapcsolatos figyelmeztető jelzésekhez a határellenőrzések, és egyéb, az országon belül végzett rendőrségi

és vámellenőrzések céljából. Ugyancsak hozzáférés engedélyezett a belépési és tartózkodási tilalom miatt elrendelt figyelmeztetőjelzés-kategória esetében vízumok és tartózkodási engedélyek kiállítása, valamint az idegenrendészeti jogszabályok alkalmazása céljából is az arra kijelölt hatóságoknak.



SIS felépítése[5]

Az egyes nemzeti egységek adatállománya a technikai támogatóegység segítségével tartalmilag azonos. Adatbevitel minden nemzeti egységben alkalmazható, amely a központi egységen keresztül eljut minden nemzeti egységbe, ahol a technikai támogató egységek adatállományai személyekre és tárgyakra vonatkozó figyelmeztető jelzéseket tartalmaznak. Minden hatóság csak a saját nemzeti (támogató) egységeiből kérdezhet le.

A rendszerhez tartoznak még a SIRENE Irodák, melyek a Schengeni Információs Rendszer Kiegészítő Információinak Cseréjét Biztosító Nemzeti Hatóságok. Azaz amennyiben valahol a SIS-ben figyelmezető jelzést fednek fel, és a felfedéssel kapcsolatban további információkra van szükség, úgy azt a SIRENE Irodákon keresztül lehet megszerezni. Feladatuk továbbá a figyelmeztető jelzéshez csatolt megjelölés elhelyezése, a találat kezelése, valamint a többszörös figyelmeztető jelzéselhelyezések elkerülése érdekében közvetlenül kapcsolatot tartása a SIS-t alkalmazó államok SIRENE Irodáival.

A SIS-ben személyekre, tárgyakra és járművekre[6] lehet figyelmeztető jelzést elhelyezni. A figyelmeztető jelzések elhelyezésének okai közt:

- olyan személyekre vonatkozó adatok lehetnek, akiknek a letartóztatását kiadatás céljából kérik (95. cikk), [7]
-olyan személyekre vonatkozó adatok lehetnek, akikkel szemben beléptetési tilalmat rendeltek el (96. cikk),
- olyan személyekre vonatkozó adatok lehetnek, akik eltűntek, vagy akiket saját védelmük, esetleg fenyegető veszély elhárítása érdekében átmenetileg rendőri védelem alá kell helyezni (97. cikk),
- olyan személyekre vonatkozó adatok lehetnek, akiknek a tartózkodási helyét vagy lakóhelyét tisztázni kell a büntetőeljárás céljából (98. cikk),

[5] Kép forrása: http://www.europeum.org/doc/obrazky/cislo8/obr1.gif 2010. június 10-i letöltés
[6] SVE 100. § alapján A SIS-be be kell vinni az olyan tárgyakra vonatkozó adatokat, amelyeket lefoglalás vagy büntetőeljárásban bizonyítékként való felhasználás céljából keresnek. Ezek: 50 cm3-t meghaladó hengerűrtartalmú gépjárművek; 750 kg-t meghaladó önsúlyú utánfutók és lakókocsik; lőfegyverek; kitöltetlen hivatalos okmányok; kiállított személyazonosító iratok; és feljegyzett sorszámú bankjegyek.
[7] SVE 95. § - Ezen figyelmeztető jelzés ugyanolyan hatállyal rendelkezik, mint az 1957. szeptember 13-i Európai kiadatási egyezmény (SVE 64. §)

- olyan személyekre vagy járművekre vonatkozó adatok lehetnek, akiknek, amiknek leplezett figyelése vagy célzott ellenőrzése szükséges (99. cikk),
- olyan tárgyakra vagy járművekre vonatkozó adatok lehetnek, amelyeket lefoglalás vagy büntetőeljárásban bizonyítékként való felhasználás céljából keresnek (100. cikk).

4. A SIS II FEJLESZTÉSE

A Schengeni Információs Rendszer működik, folyamatosan fejlesztik. Jelenleg SISone4all a neve, ugyanis a SIS II még mindig nem készült el. Elméletileg a teljes jogú schengeni tagság elnyeréséhez a 2004-es bővítési körben belépett államoknak nemcsak a megszabott feltételeket kellett teljesítenie, hanem a SIS II-nek is készen kellett volna állnia technikai okok miatt. Ugyanis a SIS I rendszer csupán 18 nemzeti egységre volt tervezve, így csupán 3 taggal bővülhetett volna az informatikai rendszer használóinak száma. Már 2001-ben számítottak Egyesült Királyság és Írország csatlakozására, és az EU bővítésére, ezért döntöttek a fejlesztésről.[8] A rendelet alapján valószínűleg 2006-os indításra gondoltak a SIS II tekintetében, hiszen azon év végén automatikusan hatályon kívül helyezték volna. A lejárat előtt újabb rendeletet [9] alkottak a rendszer létrehozásáról. Ez már konkrét rendelkezéseket tartalmazott és új elemként például bevezetése került a rendszerben a tartalék központi egység.[8] A korábbi rendelkezésekhez képest, üzemeltetési igazgatóságot hoztak létre, mely a biztonságért is felel. Nemcsak naplózni kell a lekérdezéseket, hanem ellenőrizni is azokat.

A SIS II-ben személyekhez köthetően az alábbi adatokat lehet feltüntetni a figyelmezető jelzéshez kapcsolódó adatként:

a) családi név(nevek) és utónév(nevek), születési név(nevek) és korábban használt nevek, valamint bármely álnév(nevek), adott esetben külön bejegyzésben;*
b) bármely különleges, objektív és nem változó testi ismertetőjel;
c) születési hely és idő;
d) nem;
e) fényképek;*
f) ujjlenyomatok;*
g) állampolgárság(ok);
h) az érintett személynél van-e fegyver, erőszakos-e, vagy megszökött-e;
i) a figyelmeztető jelzés oka;
j) a figyelmeztető jelzést kiadó hatóság;*
k) a figyelmeztető jelzés alapjául szolgáló határozatra való hivatkozás;*
l) a foganatosítandó intézkedés;
m) a SIS II-ben kiadott egyéb figyelmeztető jelzésekkel való kapcsolat(ok).*

A fenti felsorolásban csillaggal jelölt adattartalom a korábbi, SIS I-hez képest bővítést jelent. A lajstromban szereplő biometrikus azonosítók[9] pedig minden kétséget kizáró azonosítást tesznek lehetővé, elkerülve azon tévedéseket, melyek abból adódtak, hogy egy ország állampolgárai közül ugyanazon néven többen születhettek ugyanazon a napon. Igaz ugyanakkor, hogy a fényképes és ujjlenyomatos azonosítást csak úgynevezett harmadik országbeli állampolgárok[10] esetében használhatók fel.

A SIS II rendelet előírta a Bizottságnak, hogy 2009. első félévétől kezdődően tegyen félévente jelentést a SIS II-re átállásról. A legutolsó jelentés [10] megállapítja, hogy a SIS II fejlesztését a jelenlegi SIS II projekt alapján a fejlesztési fővállalkozó folytatja, és a projekt

[8] Sankt Johann im Pongauban (Ausztria)
[9] biometrikus azonosító: a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004/EK Tanácsi rendelet (2004. december 13.) alapján az arcképmás és az ujjlenyomat
[10] Nem uniós államok polgárai

támogatásához szükséges időszak készenléti terveként megtartja a SIS II megvalósításának alternatív technikai megoldását is (SIS 1+RE néven). Az elvégzett átfogó architektúra-felülvizsgálat során a SIS II szakértők leszögezték, hogy a rendszer architektúrájának nincsenek nagyobb hiányosságai. Megállapította a Bizottság azt is, hogy ugyan a jogszabályi (mind rendelet, mind határozat rendelkezésre áll) háttér az átálláshoz biztosított, de azokat módosítani szükséges, mert 2010. június 30-án hatályukat vesztik, azaz a rendszer végleges elindítása még mindig várat magára.

Mivel – ahogy azt már említettem -, a SIS II nem készült el időre, Portugália ötlete alapján a rendszert szabad részeinek klónozásával tágították, amelyre nemcsak a 2007-es bővítési kör államai, hanem 2008-ban Svájc, sőt valószínűleg 2011-ben Románia és Bulgária is még a SIS I+ vagy közkeletűbb nevén a SISone4all-hoz csatlakozhat.

Az interneten keringő hírek - mely szerint a SIS II fejlesztés egy feneketlen kút [11]- részben igaznak bizonyulnak a jelentés alapján, eddig több mint 50 millió Euro elköltését ismeri el a Bizottság – jelenleg látszat nélkül.

Be kell látni ugyanakkor, hogy a Schengeni Információs Rendszer a rendvédelmi szervek mindennapi életét megkönnyíti és elég eredményes. Például Svájcban átlagosan naponta 30 felfedést érnek el a hatóságok,[12] (a magyar eredményeket lásd az 1. sz. táblázatban).

A határok nélküli Európában a bűnözés is határok nélkülivé vált, mindenki szabadon mozoghat. Jól ismerték fel a Schengeni Egyezmény aláíró államai, hogy szükség lehet egy egységes, minden ország számára elérhető rendszerre. Alapvetően jól és megbízhatóan működik, bár néhányszor roppant lassú: időnként 15 perc is eltelik a visszajelzésre.[13]

Magyarországon külön törvényt [14] hirdetek ki a SVE keretében történő együttműködésre, mely gyakorlatilag a SVE-ben foglalt szabályokat, fogalmakat tartalmazza a SIS rendszer tekintetében. A vonatkozó kormányrendelet [15] a Nemzeti SIS hatóságnak, az informatikai központ feladatait ellátó szervként a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalát jelölte ki.[11] A Schengeni Információs Rendszer Kiegészítő Információinak Cseréjét Biztosító Nemzeti Hatóság (SIRENE Iroda) feladatait a Rendőrség szervezetébe tartozó Nemzetközi Bűnügyi Együttműködési Központ (NEBEK) látja el.[12] A SIRENE Iroda Magyarországon az Országos Rendőr-főkapitányságon található, rendőrökön kívül a feladat ellátásra vezényelt vám- és pénzügyőr teljesít szolgálatot.

5. A SCHENGENI INFORMÁCIÓS RENDSZERBEN TÖRTÉNŐ ELLENŐRZÉS

Amint azt már korábban kifejtettem a rendszerben tárolt adatokhoz a kijelölt hatóságok számára lehetővé tették, hogy automatizált lekérdezési eljárás révén hozzáférjenek a személyekkel és tárgyakkal kapcsolatos figyelmeztető jelzésekhez a határellenőrzések, és egyéb, az országon belül végzett rendőrségi és vámellenőrzések céljából. Ezen kívül a vízumok és tartózkodási engedélyek kiállítása, valamint az idegenrendészeti jogszabályok alkalmazása céljából is az arra kijelölt hatóságoknak is lehetőségük van a rendszerben ellenőrizni.

[11] Korm.r. 1. §

[12] Az Európai Unió bűnüldözési információs rendszere és a Nemzetközi Bűnügyi Rendőrség Szervezete keretében megvalósuló együttműködésről és információcseréről szóló 1999. évi LIV. törvény 3. § (4) bekezdés

	2008	2009
SVE 95. §	68	83
SVE 96. §	2697	3206
SVE 97. §	83	74
SVE 98. §	832	1145
SVE 99. §	550	839
SVE 100. §	494	586
összesen	**4724**	**5933**

1.sz. ábra Magyarországon felfedett SIS jelzések[13]

Az integrált határbiztonsági rendszer felépítése alapján a - vízumköteles országból származó - harmadik országbeli állampolgárt először a nagykövetségeken, esetleg a konzuli irodákon dolgozó személyek ellenőrzik a vízum kiadása, kiállítása előtt. Ebbe az ellenőrzésbe beletartozik a személy SIS-ben történő kontrollja is, a tekintetben, hogy nem áll-e beutazási és tartózkodási tilalom alatt. Amennyiben nem, úgy az egyéb feltételek (pl. anyagi fedezet) megléte esetén kiállítják számára a vízumot. Ha a személy ellen valamely ország fenti tilalmat rendelt el, úgy még indokolt esetben területileg korlátozott vízum állítható ki a számára.

A harmadik ország állampolgára legnagyobb eséllyel a külső határon határátlépésre jelentkezéskor kerül ellenőrzésre a SIS-ben. Határátlépéskor ugyanis őt alapos ellenőrzésnek kell alávetni, [16] mely magában foglalja a beutazási feltételek kontrollját. Ezek a következők (kiemelés tőlem): [14]

> - úti okmány érvényességének, a szükséges vízum vagy tartózkodási engedély meglétének ellenőrzése;
> - az úti okmány alapos átvizsgálása hamisításra utaló jelek tekintetében;
> - engedélyezett tartózkodás maximális időtartamának ellenőrzése;
> - indulási és célországának, valamint a tervezett tartózkodás céljának vizsgálata, és szükség esetén a megfelelő igazoló okmányok ellenőrzése;
> - beutazáshoz vagy átutazáshoz szükséges fedezet igazolásának ellenőrzése;
> - *annak vizsgálata, hogy az érintett harmadik országbeli állampolgár, a járműve és a birtokában lévő tárgyak nem jelentenek-e veszélyt valamely tagállam közrendjére, belső biztonságára, közegészségügyére vagy nemzetközi kapcsolataira. A vizsgálat a SIS-ben és a nemzeti adatállományokban tárolt, személyekre, és – amennyiben szükséges – tárgyakra vonatkozó adatoknak és figyelmeztető jelzéseknek, valamint a figyelmeztető jelzés esetén végrehajtandó intézkedésnek a közvetlen lekérdezését foglalja magában.*

A SIS-ben történő ellenőrzésre kisebb esély az ország területén, mivel itt az ellenőrzések száma kisebb, mint a határellenőrzések során. Ebben az esetben ez az ellenőrzés a Robotzsaru ügyeleti modulján, a TETRA-rádió vagy mobiltelefon SMS-en keresztül, vagy közvetlenül a Hermon körözési rendszeren keresztül lehetséges. Valamennyi esetben a rendszer automatikusan ellenőriz a Schengeni Információs Rendszerben.

Talán a legkevesebb az esélye Magyarországon a SIS-ben történő ellenőrzésnek, és azon keresztül a felfedésnek, amikor a Bevándorlási és Állampolgársági Hivatal tartózkodási, vagy letelepedési engedélyt állít ki és ehhez ellenőrzi a személyt a rendszerben.

Magyarországon – mint az 1. sz. táblázatból kiderül – SIS rendszerben a legtöbb felfedés a személyekkel szemben elrendelt beutazási tilalom miatt történt.

[13] Adatok forrása: ORFK Rendészeti Főigazgatóság, Rendészeti Elemző-értékelő Osztály; megjegyzés: csak a határrendészeti szakterület által jelzett adatok

[14] Schengeni határ-ellenőrzési kódex 7. cikk (3) bekezdés

A felfedési helyeket tekintve a román határszakaszon történik a SIS felfedések több mint harmada (2008: 1719 eset -36%; 2009: 2066 eset -35%).

Állampolgárság	95. §	96. §	97. §	98. §	99. §	100. §	Összesen
szerb	21	1229	9	276	188	47	**1770**
román	28	108	30	395	274	82	**917**
magyar	2	3	6	54	14	31	**110**
egyéb	32	1866	29	420	363	426	**3136**
összesen	**83**	**3206**	**74**	**1145**	**839**	**586**	**5933**

2.sz. táblázat SIS felfedések állampolgárság szerint[15]

Ami ennél is érdekesebb, hogy a második legtöbb SIS felfedés a román állampolgárok körében (nagy valószínűséggel a román szakaszon fedik fel ezeket) történik (ld. 2. sz. táblázat). Természetesen nem a beutazási tilalom alatt álló személyek felfedése a jelentős (3,5%), hiszen EU tagország állampolgáraival szemben nagyon kivételes esetben lehet elrendelni ilyen tiltást. A SIS-ben olyan személyek felfedése történt, akik a tartózkodási helyét vagy lakóhelyét tisztázni kell a büntetőeljárás céljából (395 fő, az összes ilyen 35%-a); valamint a figyelőztetett személyek, járművek észrevételezése (32%), melyek messze a legnagyobb számú eredményességet okozták az országban. De a kiadatási célú körözések körében is a legtöbb elfogott román állampolgárságú.

Amennyiben a SIS nem létezne (csak a magyar nyilvántartási rendszerek) valószínűleg a 2009. évben felfedett 5933 SIS figyelmezető jelzés töredéke, véleményem szerint nagyjából a fele kerülne felfedésre, köztük a magyar állampolgárok. Miért mondom ezt? Ha megnézzük a SIS figyelmeztető jelzés kategóriákat, akkor láthatjuk, hogy a külföldiek ellen, más Uniós országokból elrendelt lakcím megállapítás okából, vagy figyelőztetett személyek, járművek vagy a tárgyakra kiadott körözés felfedése pusztán a magyar rendszerek alkalmazásával lehetetlen lenne. A SIS-ben olyan figyelmeztető jelzések vannak benne, mely alapján egyes személyek nem léphetnek az EU területére, vagy egyes bűncselekmények bizonyításához a személyek, járművek leplezett figyelése és speciális intézkedések foganatosítása szükséges. Ezzel pedig a SIS hozzájárul Magyarország és az Európai Unió biztonságához, az integrált határbiztonsági rendszer eredményes működéséhez.

Továbbfűzve a gondolatmenetet, ha csak a magyar rendszereket alkalmaznánk, a felfedések közt a beutazási és tartózkodási tilalom ugyanúgy meghatározó lenne, állampolgárság tekintetében pedig a szerb, ukrán, moldáv hármas vezetne, hiszen ők követik a tiltott határátlépések zömét, amelynek „mellékbüntetése" a beutazási és tartózkodási tilalom megsértése (ld. következő szövegrész).

Románia a tervek szerint 2011. március 2-án teljes jogú schengeni taggá válik, a határellenőrzés a magyar-román határon megszűnik. Ezzel együtt várhatóan a SIS-felfedések száma is drasztikusan csökkeni fog (a 2009-es 2066 főről) nagyjából a századára.

A másik befolyásoló tényező szintén a beutazási tilalomhoz köthető. 2009. december 19. óta három balkáni ország – Macedónia, Montenegró, Szerbia – állampolgárai vízummentesen utazhatnak az Európai Unió tagállamaiba. Ezeket az országokat hamarosan követi két újabb Nyugat-Balkánon található ország: Albánia és Bosznia- Hercegovina. [17] Jelen cikkem szempontjából azért bír ez relevanciával, mert a beutazási tilalom elrendelésére a törvény [18]

[15] Adatok forrása: ORFK Rendészeti Főigazgatóság, Rendészeti Elemző-értékelő Osztály; megjegyzés: 2009. évben, csak a határrendészeti szakterület által jelzett adatok

alapján többek közt tiltott határátlépés miatt kerülhet sor[16], amelyek egy része pedig anyagi okok miatt következik be (az EU-ba vízumot kell váltani, ahhoz pedig újabb anyagi fedezetet kell igazolni). Azaz feltevésem szerint, ha a szerb állampolgároknak (melyek a SIS beutazási tilalom felfedések majdnem négytizedét teszik ki – ld. a 2. sz. táblázat) nem kell vízum, szabadon beutazhatnak és nem követnek el tiltott határátlépést, akkor velük szemben nem lesz elrendelve beutazási tilalom és így a SIS-be sem kerül figyelmeztető jelzés elhelyezésre, végső soron a felfedések száma fokozatosan csökken. Ennek ellenkező irányú folyamata lehetne, ha a szabályosan belépő személy később válna jogellenes tartózkodóvá (tartózkodási idő túllépése, vagy engedély nélküli munkavállalás) és emiatt rendelnének el beutazási tilalmat. Azért a feltételes mód, mert ritka az ilyen elrendelés. Összességében tehát a szerb állampolgárok körében történő felfedések száma is fokozatosan csökkenni fog Magyarországon.

ÖSSZEFOGLALÁS

Cikkemben megmutattam az első közös, rendvédelmi célból is felhasználható információs rendszer, a Schengeni Információs Rendszer létrejöttének rövid történetét. A SIS-t a határellenőrzések miatt létrejövő biztonsági deficit egyik kompenzációs elemének tervezték, minden teljes jogú schengeni tagállamban működik, beleértve Svájcot, Norvégiát és Izlandot is, melyek nem EU tagállamok.

Az integrált határbiztonsági rendszert röviden bemutattam, kiemeltem azt a három területét, melyek során szükséges a SIS alkalmazása. Ezek a következők:

- egységes vízumrendszer alkalmazása,
- külső határok ellenőrzése,
- kiegyenlítő (kompenzációs) intézkedések.

Ezen elemekben a SIS felhasználása megvalósul, úgymint vízumok kiállítása, külső határok átlépése során harmadik országbeli állampolgárok alapos ellenőrzése, és mélységi migrációs (idegenrendészeti) ellenőrzések. Ezeken kívül a SIS-ben történő ellenőrzés a nem idegenrendészeti célú rendőri ellenőrzések, valamint a letelepedési, bevándorlási engedélyek kiállítása során valósul meg.

Ismertettem a SIS felépítését, annak fejlesztését. Megállapítottam, hogy a SIS II adattartalma a SIS I-hez képest kibővül, azonban a fejlesztések végkimenetele ma még bizonytalan.

Bemutattam a SIS tekintetében az Európai Uniós és a magyar szabályozást, a magyar felhasználói kört ismertettem.

Végezetül ismertettem a magyar felfedéseket, megállapítottam, hogy a legtöbb SIS találat a román határszakaszon történik, állampolgárságot tekintve pedig a szerb és a román állampolgárok felfedése jelentős.

Bebizonyítottam, hogy a SIS hozzájárul Magyarország és az Európai Unió biztonságához, hiszen olyan figyelmeztető jelzések vannak benne, mely alapján egyes személyek nem léphetnek az EU területére, vagy egyes bűncselekmények bizonyításához a személyek, járművek leplezett figyelése és speciális intézkedések foganatosítása szükséges.

Románia teljes jogú schengeni csatlakozásával, valamint a szerb állampolgárok vízum nélküli beutazásának lehetőségével valószínűleg ezek az eredmények nagy része el fog tűnni.

A határok nélküli Európában a bűnözés is határok nélkülivé vált, mindenki szabadon mozoghat. Jól ismerték fel a Schengeni Egyezmény aláíró államai, hogy szükség lehet egy egységes, minden ország számára elérhető rendszerre. A SIS alapvetően jól és megbízhatóan működik.

[16] Harm.tv. 43. § (2) a) pont alapján

FELHASZNÁLT IRODALOM:

[1] Dr. Virányi Gergely: Az EU, a Schengeni Egyezmények és a magyar határrendészet in: Határellenőrzés az Európai Unióban (szerk.: Dr. Virányi Gergely) HSA Budapest, 2000.

[2] Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról,

Forrás: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:HU:HTML 2010. szeptember 30-i letöltés

[3] Pontos címe: Egyezmény a Benelux Gazdasági Unió tagállamainak kormánya, a Német Szövetségi Köztársaság kormánya és a Francia Köztársaság kormánya között a határokon történő ellenőrzések fokozatos megszüntetéséről, röviden Schengeni Egyezmény (SE)

[4] Megállapodás a Benelux Gazdasági Unió tagállamainak kormánya, a Német Szövetségi Köztársaság kormánya és a Francia Köztársaság kormánya között a határokon történő ellenőrzések fokozatos megszüntetése tárgyában 1985. június 14-én létrejött Schengeni Egyezmény végrehajtásáról (SVE), vagy más néven Schengen II. Egyezmény

[5] Masika Edit - Harmati Gergely: Egységes belbiztonsági és jogi térség Európában ISM Budapest, 1999.

[6] Országos Rendőrfőkapitány 21/2008. (OT 11.) utasítása az illegális migrációval összefüggő jogsértések kezelésével kapcsolatos rendőri feladatok végrehajtására 2. sz. melléklet

[7] Az illegális migráció és az ahhoz kapcsolódó más jogellenes cselekmények elleni hatósági fellépés hatékonyságának növeléséről, illetve összehangolásáról szóló 8/2010. (II. 19.) IRM-SZMM-PM-KHEM együttes utasítás

[8] A Tanács 2424/2001/EK rendelete (2001. december 6.) a Schengeni Információs Rendszer második generációjának (SIS II) kifejlesztéséről

[9] Az Európai Parlament és a Tanács 1987/2006/EK rendelete (2006. december 20.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról

[10] A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak a Schengeni Információs Rendszer második generációjának (SIS II) fejlesztéséről Brüsszel, 2010.5.6. COM(2010)221 végleges

[11] SIS II - a pénznyelő, 2009. 10. 26. Forrás: http://www.sg.hu/cikkek/70565/sis_ii_a_penznyelo 2010. június 14-i letöltés

[12] Schengen Information System proves its worth Forrás: http://www.swissinfo.ch/eng/specials/switzerland_schengen/Schengen_Information_System_proves_its_worth.html?cid=653810 2010. június 15-i letöltés

[13] Stephen Kabera Karanja: Transparency and proportionality in the Schengen information system and Border Controll Co-operation, Koninklijke Brill NV, Leiden, The Netherlands, 2008. 206. o. ISBN 9789004162235

[14] A Schengeni Végrehajtási Egyezmény keretében történő együttműködésről és információcseréről szóló 2007. évi CV. törvény

[15] Az N.SIS informatikai központ feladatait ellátó szerv kijelöléséről, a SIS-be történő adatbevitel elrendelésének és végrehajtásának, valamint az N.SIS Hivatal és a SIRENE Iroda technikai és adminisztratív feladatai ellátásának részletes szabályairól szóló 242/2007. (IX. 21.) Kormányrendelet

[16] Az Európai Parlament és a Tanács 562/2006/EK rendelete (2006. március 15.) a személyek határátlépésére irányadó szabályok közösségi kódexének (Schengeni határ-ellenőrzési kódex) létrehozásáról

[17] Lipics László: A balkáni országok vízumkönnyítése 2010.02.20 Elérhetőség: http://www.biztonsagpolitika.hu/?id=16&aid=836&title=A_balk%C3%A1ni_orsz%C3%A1gok_v%C3%ADzumk%C3%B6nny%C3%ADt%C3%A9se

[18] A harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló 2007. évi II. törvény

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Miskolczi Ildikó
miskolczi.ildiko@gmail.com

ELLENŐRZÉSI ÉS VIZSGÁZTATÁSI LEHETŐSÉGEK BŐVÍTÉSE A MOODLE RENDSZERBEN

Absztrakt

A Moodle LMS rendszer képes menedzselni az egész tanulási folyamatot, a kurzusszervezéstől, a lebonyolításon át az adminisztrációig. Számos olyan funkciója van, amely nem csak tananyagtárként működteti a rendszert, de valódi egyéni és csoportos online munka lehetőségét is támogatja. Azonban az eLearning szerves részét képező online tanári ellenőrzés, vizsgáztatás során a biztonságos és egyértelmű felhasználói azonosítást nem támogatja teljes körűen. Vannak kiskapuk, melyeket a rendszer felhasználói kihasználva, a vizsgákon nem tudjuk biztosítani a tanári ellenőrzések és vizsgák tisztaságát.
Ezen hiányosságok kiküszöbölésére mutat be megoldásokat a szerző.

The one of the excellence of Moodle LMS – among other things – is able to promote all of the learning process, from the organization of course, through the transaction until the administration. It has a number function like that, that not runs the system as a curriculum collection only, but favours the opportunity of real individual and collective online work. But in a present moment this is a big problem with the system that it doesn't help the real online exams. There are some points where we cannot able to assure the safety of exams.
Now I show and give some answers to this problem.

Kulcsszavak: *felhasználók azonosítása, online vizsga, Moodle, eLearning ~ eLearning, Moodle, online exam, user identificaion*

BEVEZETÉS

A XX. és XXI. század oktatási rendszere [1] és módszertana jelentős átalakuláson megy keresztül. A múlt század utolsó évtizedeiben megjelenő távoktatás és annak az internet széleskörű elterjedésével megjelenő eLearning módszerekkel való alkalmazása, nem csak a tanulási, de a tanítási szokásokat is jelentősen átalakította és formálja folyamatosan.

Az LLL[1] igényének megjelenésével, a távoktatásban tanulók száma folyamatosan és jelentősen megnövekedik. A felsőoktatásba jelentkezők száma egyre nagyobb, az

[1] LLL – lifelong learning, élethosszig tartó tanulás

elsajátítandó ismeretek egyre komplexebbek és összetettebbek, ugyanakkor az óraszámok, a konzultációs alkalmak száma egyre kevesebb.

Az oktatás egyre inkább elveszíti személyes jellegét, és az oktatókat arra ösztönzi, hogy olyan technikákat, módszereket alkalmazzanak, amelyek a tanulók növekvő, ugyanakkor folyamatosan változó és alakuló igényeit kielégítik. Ennek elemei közé tartoznak azok az eszközök, amelyek a tanulási folyamatot térben és időben függetlenné teszik, és *bárhol*, *bármikor*, *bárki* számára elérhetővé teszik *reális időn belül* [2], [3].

Ugyanakkor a távoktatási forma kezdetektől fogva feltételezi a hallgató nagyfokú önállóságát a tananyag feldolgozása során. Az eLearningben tehát olyan eszközöket célszerű választani a hallgatói munka megkönnyítésére, amelyek minimális tanári támogatás mellett maximális tanulói támogatást nyújtanak. Nem gondolom, hogy erre egyetlen jó módszer létezne csupán. Magam is többféle módszert kipróbáltam már, és tapasztalataim azt mutatják, hogy az alkalmazott eszközökben a tanár személyiségének is éppoly szerepe van, mint a hallgatói elvárásoknak, vagy az elsajátítandó ismereteknek.

Meglátásom szerint, olyan eszközt célszerű a hallgatók számára biztosítani, amelyet egyéni tempóban, tanári segítség, felügyelet mellett, önállóan tudnak alkalmazni. Az eLearning keretrendszerek legnagyobb előnye, hogy két fontos dolgot adnak a diák kezébe: azt, hogy mit kell megtanulni, és hogy mit fognak számon kérni, vagyis a tudásért való célba futás rajt és célpozícióját. A két mérföldkő közötti út keretrendszerenként változik, mind szolgáltatásában, mind pedig árában. [4]

Saját kutatásaimban a Moodle LMS rendszert használom. A több hasonló rendszer közüli választásomban a Moodle mellett való döntésemet többek között az motiválta, hogy a teljes tanítási-tanulási folyamatot támogatja, menedzseli, valamint online munka szervezhető vele egyénileg és csoportosan is.

1. FELHASZNÁLÓI AZONOSÍTÁS RENDSZERE A MOODLE-BAN

Alapvető, mint minden zárt rendszerbeli mozgás esetében, hogy minden felhasználó azonosítható legyen. Így tudunk azonnal a rendszer kapujában már jogosítványt adni a kezébe, ami meghatározza, hogy az adott felhasználó milyen tevékenységeket végezhet a rendszerben. Természetesen ennek feltétele, hogy egy adott felhasználói körhöz a rendszergazda hozzárendelje a felhasználót annak rendszerbe való belépése előtt. Ehhez előtte meg kell határoznia, hogy az adott felhasználói körnek hol milyen jogosultságai lesznek.
A Moodle jelenlegi 1.9-es verziójában 6 féle szerepkör különíthető el. (1. ábra)

Ezek:

- rendszergazda
- kurzuskészítő
- tanár
- nem szerkesztő tanár
- tanuló vendég
- hitelesített felhasználó

Név	Leírás	Rövid név	Szerkesztés
Rendszergazda	A rendszergazdák a portálon az összes kurzusban általában bármit tehetnek.	admin	
Kurzuskészítő	A kurzuskészítők új kurzusokat hozhatnak létre és oktathatják őket.	coursecreator	
Tanár	A tanárok egy kurzuson belül bármit megtehetnek, beleértve a tevékenységek módosítását és a tanulók pontozását.	editingteacher	
Nem szerkesztő tanár	A nem szerkesztő tanárok taníthatnak kurzusokat és osztályozhatnak tanulókat, de a tevékenységeket nem módosíthatják.	teacher	
Tanuló	A tanulók egy kurzuson belül általában kevesebb joggal rendelkeznek.	student	
Vendég	A vendégek általában kevés jogosultsággal rendelkeznek és nem tudnak sehova szöveget beírni.	guest	
Hitelesített felhasználó	Minden bejelentkezett felhasználó.	user	

1. ábra A felhasználók definiálása

Felhasználói név és jelszó
A vendégeken kívül a regisztrált felhasználók, felhasználónévvel és jelszóval férnek hozzá a rendszer szolgáltatásaihoz, a rendszergazda által előzetesen beállított jogosultságaiknak megfelelően. Az, hogy egy konkrét személy (felhasználó) mit tehet a rendszerben, az a belépése pillanatában dől el. (milyen jogokkal felruházott névvel lép be).
Azonban az, hogy ki használja az adott felhasználói nevet és jelszót nem ellenőrizhető.

Kurzus beiratkozási kulcs
Attól, hogy valaki bejut a zárt rendszerbe, nem biztos, hogy minden kurzus minden tananyagához és tevékenységéhez hozzá kell, hogy férjen. Ezért magukat a kurzusokat is külön belépési kulccsal, jelszóval védhetjük az illetéktelenek elől.
Természetesen ennek akkor is nagy jelentősége lehet, ha vannak a rendszerben olyan anyagok, amelyek szabadon, vendégként a zárt rendszerbe történő belépés nélkül is böngészhetők. Ekkor fokozottan indokolt lehet egy-egy kurzus tartalmának kulccsal történő védelme.

Tevékenységekhez kötődő jelszavak
Ugyanezen logika alapján bizonyos tevékenységeket is jelszóval védhetünk, például csoportosan megoldandó feladatokat, fórumtémák kezelését, és gyakorlatilag bármely tevékenységi formát.

Vizsgáztatás a Moodle-ban
(a probléma megfogalmazása)

Felhasználói oldal

A felhasználók ilyen „látszólagos” azonosítása nem probléma mindaddig, amíg a felhasználó elsődleges érdeke a rendszer biztonságos használata. Abban a pillanatban azonban, amikor olyan rendszerhasználat megvalósítása a cél, amely problémás lehet számukra (pl. vizsga), igyekeznek a rendszer hiányosságait, hibáit kihasználni. Természetesen itt nem a hacker-kedésre gondolok, hanem a „legegyszerűbb” megoldásra, a vizsgán nem megengedett eszközök használatára. Egy online virtuális rendszer esetén az első lehetőség adódik abból, hogy a vizsgáztató nem látja, ki ül a gép előtt, és mit csinál. Bárki ülhet ott, a felhasználói név és jelszó szabadon átadható, hisz nem ellenőrizhető a használó személyazonossága. (és ez igaz akkor is, ha több szintű azonosítást végzünk)

Rendszergazdai oldal

A rendszergazda feladata (és oktatási rendszerek esetén ez fokozottan igaz), hogy biztosítsa minden felhasználó számára a rendszer hibamentes és rendeltetésszerű használatát, ugyanakkor „védje” a rendszert a jogosulatlan felhasználóktól, a jogosulatlan tevékenységektől, biztosítsa vizsgák alkalmával a vizsga „tisztaságát”.

Véleményem szerint a Moodle rendszerben jelen pillanatban nem megoldott az online vizsga lehetősége, a hallgató vizsgán tanúsított magatartásának és tevékenységének egyértelmű és minden kétséget kizáró azonosítása. Nem tudja a vizsgáztató hogy valóban a regisztrált felhasználó van-e a rendszerben, vagy végez-e nem megengedett tevékenységet a vizsga során.

Kutatásaimban erre a problémára keresek megoldást: Hogyan valósítható meg egy LMS rendszerben az online vizsga, ha maga a rendszer nem tudja kezelni ezt az opciót?

2. MEGOLDÁSI LEHETŐSÉGEK AZ ON-LINE VIZSGA SORÁN

A következőkben arra mutatok be példákat, hogy hogyan lehet on-line számonkérés és vizsgáztatás, során alkalmazni az internetes lehetőségeket. A kidolgozott rendszer működésének tesztelésében a Szolnoki Főiskola távoktatási tagozatának két kis létszámú csoportja segítette munkámat.

A TANULÁSI KÖRNYEZET

Távoktatásos módszerrel tanuló hallgatók vizsgáztatását a Szolnoki Főiskolán már két vizsgaidőszakban oldottam meg így. A tantárgyak, amely ismereteinek számonkérése történt, a természet- és környezetvédelem illetve a pénzügyi-számviteli informatika. A hallgatók – a távoktatásban megszokott módszer szerint - előre kiadott tananyag alapján tanultak a félév során. A tananyagot nyomtatott formában (tankönyv) kézhez kapták, illetve CD-n a tananyaghoz készített tanulási útmutatót, amely tanulási egységenként különböző feladat-típusokkal önellenőrző feladatokat és megoldásaikat is tartalmazta. A félév során két dolgozatot kell elkészíteniük és felküldeniük a főiskola távoktatási rendszerébe az Iliasba, tutoruk címére. Ezen kívül tanulástámogatás szerepét tölti be tantárgyanként egy másfél órás személyes konzultációs lehetőség a tutorral. A saját Moodle rendszeremben helyeztem el az általam készített és a tanulási folyamatot támogató előadások prezentációit, anyagait, amelyek

nem tartoznak a főiskola „hivatalos” tananyagai közé, de tapasztalataim alapján a hallgatókat nagyban segítik az ismeretek értő elsajátításában. E mellett az egyes tananyagokhoz a Moodle által támogatott, annak rendszerébe tevékenységmodulként beépített tesztkészítő rendszert használtam (Tesztek, HotPotatoes, Quandary) a megszerzett ismeretek önellenőrzésének biztosítására. Minden tananyagrész, témakör végén kidolgozott példák, gyakorlati feladatok, külön megoldással, illetve „szorgalmi feladatként” elvégezhető feladatok álltak a hallgatók rendelkezésére. Ezek megoldásával éltek is jó néhányan, és beküldték értékelésre a megoldott feladataikat.

Az on-line vizsgáztatásban egy merőben új típust választottam, mintegy ötvözve a szóbeli és írásbeli vizsgáztatást. Előre kiadott témák közül kellett kiválasztani a hallgatónak egyet, majd azt egy prezentációban feldolgozni. A vizsga során pedig on-line bemutatnia a témát, előadást tartani a feldolgozott ismeretekből. (emellett jó néhányan választották a Skype-os video kapcsolaton keresztül a tételsor alapján való felkészülést és szóbeli vizsgát)

TECHNIKAI LEBONYOLÍTÁS, TECHNIKAI KÖRNYEZET

1. megoldás

A zárt tanulási környezet kialakítása adott volt egy korábbi munka alapján. A weboldalamon működtetett Moodle LMS rendszer[2] a hallgatók által rendszeresen használt és ismert már. Bárki, bármilyen tananyaghoz, segédanyaghoz szabadon hozzáfér, regisztráció és kurzuskulcs nélkül, vendégként bejelentkezve, így szabadon böngészhetnek más képzési formák tanulási segédanyagai között is egy-egy tantárgyon belül. A rendszer másik részét a Google Alkalmazások (GoogleApps) rendszer lehetőségeinek kihasználása alkotta. Harmadik, nem kevésbé jelentős eleme a rendszernek a video kapcsolat biztosítását szolgáló Skype rendszer volt. Bár a Google-nak is van beépített csevegő rendszere, és a levelező rendszerén keresztül is lehet szöveges kapcsolattartást biztosítani, valamint a Live Messengeren keresztül is lehet akár szöveges, akár video kapcsolatot is létesíteni – előzetes tesztjeim alapján a Skype bizonyult a legstabilabbnak. Ezen felül a Skype 25 főig konferenciabeszélgetéseket is lehetővé tesz, amit kihasználva a hallgatók egymás előadásait meghallgathatták, azokon aktívan részt vehettek.

Első lépésként a domain[3]t kellett a Google Alkalmazásokkal[4] összekapcsolni. Miután a http://mail.miskolczi.net levelező tárhelyet kialakítottam, a tárhelyet közvetlenül a Moodle rendszerből elérhetővé tettem (így nem kellett újabb webcímet megjegyezni a hallgatónak) (2. és 3. ábra).

[2] www.miskolczi.net/moodle
[3] www.miskolczi.net
[4] A Google Alkalmazások (naptár, dokumentumtár, levelezés) használatával lehetőségünk van saját dokumentumtárat létrehozni, az abban tárolt dokumentumtípusokat (word,exel, powerpoint) másokkal megosztani, másokkal közösen szerkeszteni.

2. ábra A Moodle rendszerből közvetlenül elérhetőek a GoogleApps szolgáltatásai

3. ábra Az online dokumentumtár bejelentkező oldala

Ezután megtörtént a felhasználói azonosítók kiosztása. A hallgatók számára az egyszerűbb kezelhetőség miatt ez a zárt rendszerben is a NEPTUN kódjuk lett.

Az első hallgatói belépésre a rendszerben létrehoztam és a hallgatóknak szerkesztési jogot adtam egy táblázathoz (4. ábra), amelyben mindenki megtalálta önmagát, néhány általam előre beírt vizsgaidőponttal. A hallgatónak a megfelelő dátumhoz – amely számára vizsgázásra megfelel – csak konkrét időpontot kellett rendelni. Így láthatták egymás időpontjait, és biztos nem jelentkeztek be többen ugyanarra a vizsgaidőpontra. Ugyanakkor, ha valakinek nem felelt meg az általam javasolt időpont, ő maga is javasolhatott vizsgaidőpontot.

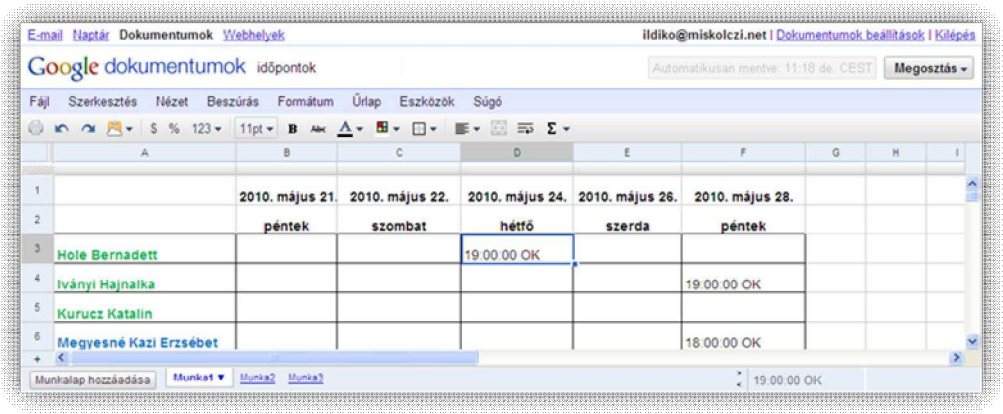
Ez a módszer azért is bizonyult hasznosnak, mert az összes időpontot látva, konferencia létrehozásával kiválaszthatták a hallgatók, hogy melyik csoporttársuk előadását hallgatnák meg szívesen, és az adott időpontban csak be kellett lépniük a rendszerbe és akár Skype kapcsolattal együtt, akár az online prezentációhoz való csatlakozás esetén a beépített csevegő használatának segítségével kapcsolatot létesíteni.

Az *tapasztalatok* igen pozitívak voltak.

A csoportlétszám 22, illetve 16 fő volt. Az aláírást szerzett 8, illetve 12 főből 6, illetve 10 fő jelezte online vizsgázási szándékát az első felhívást követő egy héten belül.

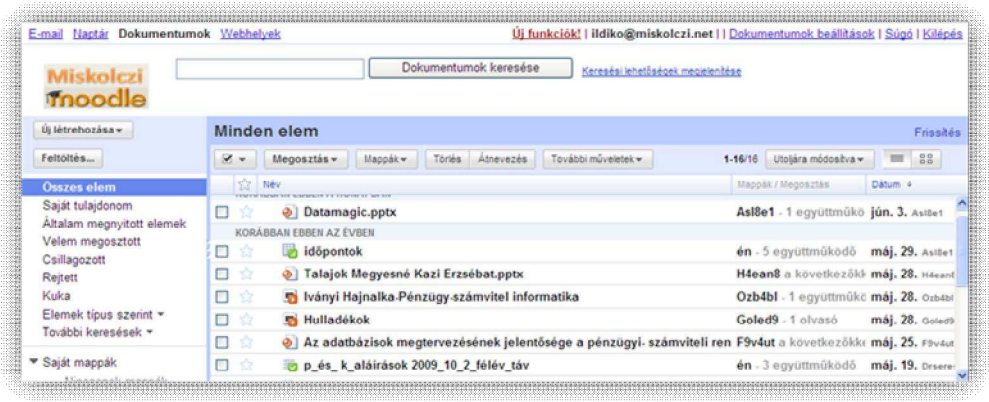
Tantárgy	Csoportlétszám	Vizsgára jogosult	Online vizsgára jelentkezett	Online vizsgát választók
Pénzügyi és számviteli informatika	16	12	10	≈ 84 %
Természet- és környezetvédelem	22	8	6	75%

1.táblázat Az online vizsgát választók aránya a csoportlétszámokhoz viszonyítva (saját készítésű táblázat)



4. ábra A hallgatói jelentkezések és oktatói visszajelzés („OK”) táblája

A rendszerhez tartozó azonosítók kiosztása után hamarosan beléptek a hallgatók a tárhelyre, és az írásos, előre kiadott tájékoztató alapján gyorsan és ügyesen ismerkedtek a dokumentumtár használatával. (szerencsére a Google rendszer mindenki által használatos, így annak ismertetésére nem kellett külön gondot fordítani) Jó néhányan próba-anyagokat tettek fel és on-line szerkesztéssel is próbálkoztak már az első alkalmakkor. (5. ábra)



5. ábra A hallgatók által a rendszerbe feltöltött és megosztott vizsgaanyagok

A vizsga során, Skype kapcsolat mellett az előzetesen a dokumentumtárba feltöltött, és az oktatóval megosztott prezentációt elindítva, követhető volt a hallgató előadása. Az interaktív

kapcsolat lehetővé tette, hogy közvetlen kérdésekre válaszoljon a hallgató, így ellenőrizhető volt a témában való jártassága. (6. ábra)

6. ábra Online vizsga részlete

További videofelvételek megtekinthetők az online vizsgákról a www.youtube.com/drmiskolczi oldalon.

A hallgatók értékelése szerint ez a vizsgáztatási forma nem csak újszerűsége miatt volt érdekes és kellemesnek mondható, de szinte mindannyian értékelték a lehetőséget, hogy csoporttársaik munkájába is betekintést kaphattak. Többször alakult ki beszélgetés a többi hallgatóval vizsga során, vagy a hallgatók csak megfigyelőként hallgatták-nézték végig csoporttársuk vizsgáját. Bár lehetőség volt saját jegyzetek használatára feleletkor, azonban szinte senki nem használt előre leírt jegyzeteket. Illetve ha volt is, nem tekintettek bele a beszélgetés során.

További pozitívuma a módszernek a hallgatói visszajelzések alapján a rendszer rugalmassága. Sem időhöz, sem helyhez nincs kötve senki, csupán internet kapcsolat szükséges. Este 10-kor és délelőtt 9-kor csakúgy vizsgáztak hallgatók, mint szombat délelőtt vagy vasárnap délután. Két hallgató külföldről vizsgázott munkahelyi ebédszünetében.
Bár az előzetes elképzelések szerint egy-egy vizsga kb. 10-15 percesre volt tervezve egy vizsga sem lett rövidebb fél óránál. Volt, aki 50 percet is beszélt önállóan a kiválasztott témájáról.

Következtetések, feladatok

Bár a rendszer kipróbáltan működik, a visszajelzések és tapasztalatok pozitívak, a fejlesztés itt még koránt sem ért véget.

Figyelni kell az időkorlátokra, az egyes vizsgák időbeosztására a csúszások miatt. Szorgalmazva a konferenciabeszélgetéseket, a rendszer továbbfejleszthető más irányokba is. Más típusú feladatok, írásbeli vizsgák lebonyolítására is alkalmassá kell tenni, illetve minél több feladattípust alkalmazni a vizsgáztatás során.

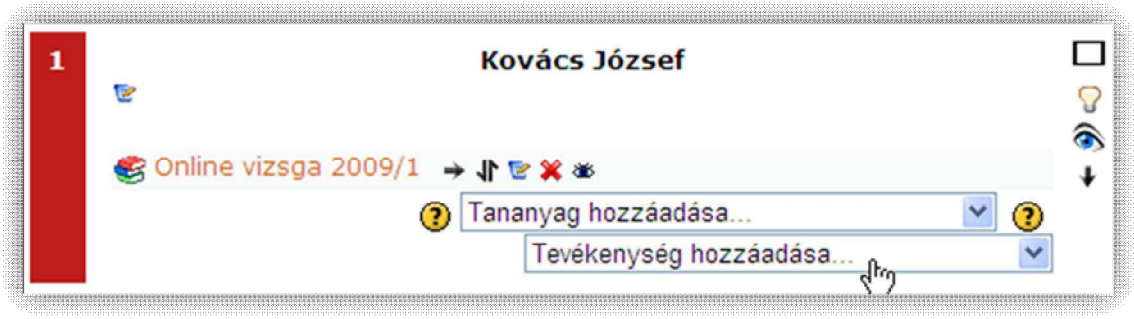
2. megoldás

A Moodle LMS rendszer tevékenységei közé tevékenységmodulként beépített lehetőség a WIZIQ portálra meghirdethető online munka lehetősége. Ez a megoldás a Moodle virtuális tantermeként működik. (bár beépített lehetőség az óra, vizsga, konzultáció meghirdetése, de

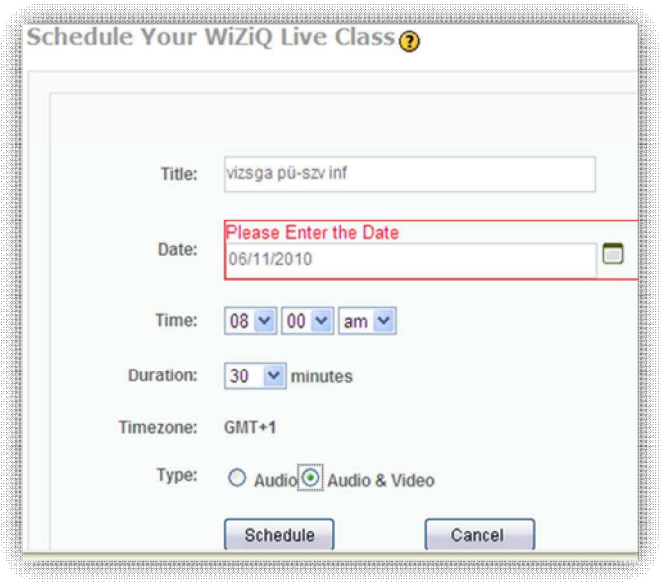
az alkalmazás maga egy külső portálon valósul meg. Jelen esetben a WIZIQ portál egy virtuális tábla, ahol mind az oktató, mind a hallgató rajzolhat, írhat, prezentálhat, magyarázhat és vetíthet.

Kiválóan alkalmas ez a vizsgáztatási módszer a valódi online feladatok megoldására, hisz a csalás lehetősége gyakorlatilag kizárt. Video- és hangkapcsolat biztosítja a „face to face" kapcsolatot jelen esetben is. Az oktató kérdez, feladatot, ábrát ír, rajzol a táblára, a hallgató pedig azonnal válaszol, magyaráz.

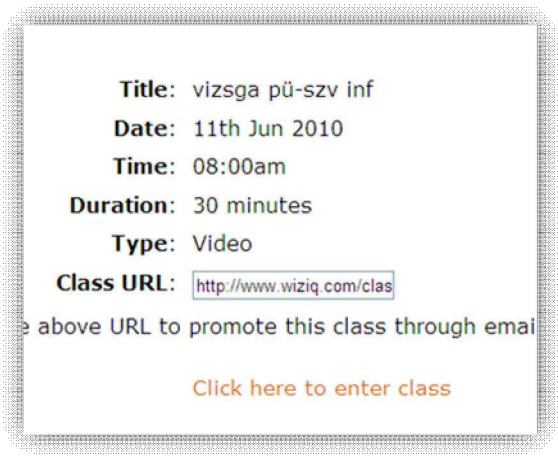
7. ábra A Moodle szerkesztési funkcióinak bekapcsolása



8. ábra Tevékenység hozzáadása: WIZIQ LIVE CLASS



9. ábra WIZIQ találkozó meghirdetése a Moodle rendszerben



10. ábra Belépés a virtuális tanterembe a Moodle portálról

11. ábra Egy vizsga felvétele a WIZIQ tantermében

A WIZIQ-en meghirdetett vizsgához mindazok csatlakozhatnak, akik számára a tanár lehetővé tette az eléréshez szükséges információkat. Láthatja és hallhatja az előadást és az előadót.
A tanár vizsgán beállít olyan jogosultságot, hogy a hallgató részvétele aktív legyen, írhasson, rajzolhasson. A virtuális teremben való vizsga előnye továbbá, hogy a vizsgáról felvétel készülhet, amit később a hallgatók is visszajátszhatnak, és tetszőleges időben megnézhetnek a WIZIQ-portálon.

„Prémium" funkciókkal az oktató nem csupán elmenteni tudja az vizsgát, hanem le is töltheti, és a Moodle portálba videóként beágyazhatja, adatrögzítőre rendezheti.

3. megoldás

A WIZIQ rendszerben konferencia keretében is, a SKYPE rendszerben pedig egyszerű kétfős video beszélgetés esetén lehetőség nyílik, az un. képernyőmegosztás funkcióra, mely alkalmazásával a vizsgáztató valós időben látja, hogy a hallgató mit csinál a saját gépe képernyőjén, hogyan old meg egy feladatot. Természeten emellett élő video kapcsolat tartható, azaz nem csak a hallgató képernyőjét, de magát a hallgatót is láthatjuk munka

közben. A kommunikáció lehetősége pedig szintén interaktívvá teszi a vizsgát. A vizsga folyamatát videóra rögzítve, archiválható, később weboldalba is beágyazható.

4. megoldás

A módszer szintén a GoogleApps dokumentumtárának felhasználását feltételezi. Ebben az esetben a rendszerbe belépve, az oktató a kijelölt vizsgaidőpontban tölti fel és osztja meg szerkesztésre is a hallgatóval a vizsgafeladatot, a hallgató pedig azonnal, online megnyitja és megoldja azt. Az oktató követni tudja a képernyőn a hallgató megoldását, a megoldás folyamatát, logikáját. Skype videó kapcsolattal pedig látja is a hallgatót feladatmegoldás közben. Ez a módszer hasznos lehet olyan írásbeli vizsgák lebonyolítására, amikor a hallgató nem tud a csoportjával együtt vizsgázni, hanem egyénileg vizsgázik (például külföldről).

ÖSSZEFOGLALÁS

A www.miskolczi.net oldalon működő Moodle LMS rendszer használatával az elsőleges célom az volt, hogy megalkossak és bemutassak egy olyan virtuális intranet környezetet, amely lehetővé teszi a világ bármely pontján tartózkodó felhasználó számára, az ott elhelyezett tananyagokhoz való hozzáférést, az online kapcsolattartást és munkát és az elsajátított ismeretek komplex számonkérését. Úgy hoztam létre ezt a zárt környezetet, hogy ne csak az egyéni munkát támogassa, ne csak a tananyagok elérhetőségét biztosítsa, de alkalmas legyen konzultációra, kapcsolattartásra, együttes, vagy önálló online feladatmegoldásra, dokumentum-szerkesztésre – legyen az szöveg, táblázat vagy bemutató –, és online vizsgáztatásra (tantárgyi kollokviumok, szemináriumok követelményi teljesítésének ellenőrzésére) egyaránt. Az interaktivitás biztosítása ugyanakkor a kapcsolattartás, véleménycsere, tapasztalatok megosztásának alapvető követelménye is, így feladatomnak tekintettem ennek biztosítását is.

Jelen pillanatban portál tehát nem csupán a tananyagok elérhetőségét szolgálja és biztosítja, de konzultációra és online vizsgáztatásra is lehetőséget ad. Alkalmas a távoktatás és az eLearning legmodernebb, de mégis bárki számára bárhol elérhető alapvető eszközrendszerének kezelésére, összekapcsolására és alkalmazására.

Ugyanakkor a rendszer használata során nagyon hamar rájöttem arra, hogy Moodle rendszer önmagában nem alkalmas az online vizsgák bonyolítására. Ezért – tapasztalataim szerint - más lehetőségeket, megoldásokat is be kellett építenem, társítanom, ha a Moodle-t akartam használni vizsgáztatásra. Ez azonban időben és energiában is sok ráfordítást, előkészítést igényel oktatói oldalon. Viszont a hallgatók nagyon kedvelik ezeket az új megoldásokat, és valóban kezdik távoktatásnak érezni a távoktatást.

Ahhoz, hogy ezek a megoldások számonkérésként, vizsgaként is megállják helyüket, fontos a hallgató egyértelmű azonosításának lehetőségének biztosítása a rendszerben. Hiába van regisztráció, hiába védjük kurzusainkat, feladatainkat jelszóval, ha nem tudjuk, ki használja az azonosítót, a jelszót. Mindenképp szükséges tehát valamilyen video kapcsolat biztosítása.

Megoldás lehet rendszerfejlesztői oldalon egy olyan modul létrehozása, amely utólag is telepíthető, beépíthető meglévő Moodle rendszerekbe.

Azonban az általam alkalmazott és javasolt megoldások sem tekinthetők teljes értékű megoldásnak. Jól használhatók kis létszámú csoportok, szóbeli vagy egyéni írásbeli vizsgák esetén. Ugyanakkor nem felejthetjük el, hogy egy oktatási intézményben egy LMS rendszert adott esetben több száz, több ezer hallgató használ. Egy-egy kurzus létszáma is lehet több

száz fő. Az ő vizsgáztatásukat is meg kell tudni oldani. Szóban szinte lehetetlen, tehát az írásbeli vizsgáztatás azonosítási lehetőségeinek kidolgozása a feladat.

Jelen pillanatban erre keresek megoldásokat.

Felhasznált irodalom:

[1] Sipos Marianna: Szándék és Valóság. In: Pethő Attila, Herdon Miklós (szerk.) Informatika a felsőoktatásban 2008. Debrecen, Magyarország, 2008.08.27-2008.08.29. Debrecen: Debreceni Egyetem, *Paper A15.* (ISBN:978-963-473-129-0) http://www.agr.unideb.hu/if2008/kiadvany/eloadasok.htm (letöltés: 2010. május 20.)

[2] György Kende - Erzsébet Noszkay –György Seres: Role of the Knowledge Management in Modern Higher Education – the e-Learning *AARMS, Vol. 6, Issue. 4 (2007) p. 559-573* http://www.zmne.hu/aarms/docs/Volume6/Issue4/pdf/01kend.pdf (letöltés: 2010. május 15.)

[3] Prof. Dr. Kende György – Prof. Dr. Seres György: Egy interaktív e-learning portál első tapasztalatai Előadás az MTA Vezetés- és Szervezéstudományi Bizottságának Tudásmenedzsment Albizottsága 2008. évi workshopján. http://vati.szie.hu/files/vati/mta-2008.pdf (letöltés: 2010. május 15.)

[4] Tibenszkyné Dr. Fórika Krisztina: Interaktív programozás oktatás Moodle keretrendszer segítségével a ZMNE-n in: IV. Évfolyam 2. szám - 2009. június http://hadmernok.hu/2009_2_tibenszkyne.pdf (letöltés: 2010. május 20.)

[5] Miskolczi Ildikó – Seres György: A tudásprezentálás elmélete és gyakorlata az e-learningben. Hadmérnök, 2009/2. http://hadmernok.hu/2009_2_miskolczi.pdf

[6] Kende György – Seres György – Miskolczi Ildikó – Hangya Gábor – Fórika Krisztina: Az e-tanulás lehetőségei a külszolgálatot teljesítő katonák képzésében, ZMNE BJKMK RLI Repüléstudományi konferencia, Szolnok http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/Kende_Gyorgy-Miskolczi_Ildiko_stb.pdf

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Molnár Mihály
molnar.mihaly@zmne.hu

ALKALMAZÁSFEJLESZTÉSI KÉRDÉSEK PORTÁL-RENDSZEREKBEN A MAGYAR HONVÉDSÉGBEN

Absztrakt

Jelen publikáció az alkalmazás és az alkalmazásfejlesztés portálokhoz kapcsolódó fogalmának tisztázása után megvizsgálja azt a három, a magyarországi gyakorlatban alkalmazott portálrendszert, melyek honvédségi alkalmazása is szóba jöhet a jövőbeni fejlesztéseknél a Magyar Honvédségben. Ezt követően megvizsgálja az alkalmazásfejlesztési lehetőségek irányát a meglévő portálrendszerekben a Magyar Honvédségnél.

Recent publication clarifies the concept of applications, and application development in the context of portals, and examines the three portal systems used in Hungary, that military use could be considered during future developments in the Hungarian Home Defence Forces. Then the author examines the possible directions of application development of the existing portal systems in HHDF.

***Kulcsszavak**: Internet, WEB, portál, szolgáltatások, alkalmazásfejlesztés ~ Internet, web portals, services, application development*

BEVEZETÉS

Az Internet mára egy olyan világméretű számítógépes hálózattá nőtte ki magát, amelyet több millióan használnak. Kezdetben a web csak statikus oldalak szolgáltatását tudta nyújtani. Ahogy növekedett az Internet úgy jelentek meg a különböző új technológiák, szabványok és ajánlások. A legújabb internetes szolgáltatások a közösségre építenek, ahol a felhasználók közösen építik fel, készítik el a tartalmakat, az információkat egymással megosztva. Ellentétben a korábbi szolgáltatásokkal, amelyeknél a tartalmat, a szolgáltatást nyújtó fél biztosította, az újabb szolgáltatásoknál a szerver gazdája csak a keretrendszert biztosítja, a tartalmat maguk a felhasználók hozzák létre, töltik fel, osztják meg és véleményezik. A felhasználók kommunikálnak egymással, és kapcsolatokat alakítanak ki egymás közt. Az interaktivitás és a fogyasztók egymás közti kommunikációja miatt ma már alig van olyan szájt (site), amely köré ne szerveződne valamilyen közösség. A tartalommegosztás (sharing) az információ elérhetővé tételét, mások számára való ajánlását jelenti. A tartalmakat létrehozó felhasználók számának

drasztikus növekedése az alkotás, a fogyasztás, a véleménynyilvánítás, és a kommunikáció demokratizálódásához, a világról szerezhető ismeretek minőségi változásához vezetet.

A Portál egy webes alapú szolgáltatás, amely egységes prezentációs felületet biztosít a webes tartalmaknak, illetve háttérrendszereknek. A Portál az oldalain elhelyezett linkek segítségével belépési pontként funkcionálhat az Internetre. Az új terminológiák ugyan egyik napról a másikra, szinte a semmiből bukkantak elő, az azokat megalapozó technológiák viszont hosszú és folyamatos fejlődés eredményeként jöttek létre. A portál-technológia valójában nem, vagy csak nagyon kevés, radikálisan új technológiához kötődik, inkább a meglévő technológiák használatának újragondolása vagy újszerű alkalmazása. A felhasználók többsége nem közvetlenül, hanem tartalomaggregátorok közvetítésével jut hozzá az információhoz úgy, hogy az eredeti forrással kapcsolatba sem kell kerülnie. Ezen tartalomaggregátoroknál a technikai szintű integráció – azaz a technológiai különbségek elfedése – mellett egyre inkább megjelenik a szemantikai különbségek feloldásának képessége, azaz a tartalmak szemantikai integrációja is.

Jelen publikáció alapvető célja három, Magyarországon elterjedt portál-technológia megvizsgálása abból a szempontból, hogy ezek a portál-technológiák miként teszik lehetővé a saját alkalmazások fejlesztését. Az általános célokon túl kiemelt figyelmet kívánok fordítani a Magyar Honvédségen belüli meglévő, illetve szükséges alkalmazási lehetőségekre.

Ennek érdekében:

- Tisztázom az alkalmazás, az alkalmazásfejlesztés fogalmát;
- Felmérem a három portál-rendszer alkalmazásfejlesztési lehetőségeit;
- Külön vizsgálom az alkalmazásfejlesztés lehetőségeit a Magyar Honvédségben;

ALKALMAZÁSFEJLESZTÉS A PORTÁL-RENDSZEREKBEN

Az **alkalmazói programok** egy konkrét alkalmazói funkció megvalósítását szolgálják. Kezdetben az alkalmazói programok az egyes alkalmazók, esetleg alkalmazói csoportok igényei alapján - mintegy " rendelésre" készültek. Ez napjainkra jelentősen megváltozott, mert az alkalmazói programok (legalábbis jelentős részük) az általános igények felmérése és elemzése alapján, mint egy gyári sorozat termék készül el.

A számítógépeken futó programokat eredetileg rendeltetésük szerint három csoportba sorolták. Ezek a következők voltak:

- a rendszerprogramok;
- a rendszerközeli programok;
- és az alkalmazói programok.

A rendszer- és rendszerközeli programok összefoglaló megnevezésére használják a **rendszerszoftver** kifejezést is, amely az alkalmazói programokkal szemben azokat a programokat foglalja magában, amelyek a számítógép (vagy a hálózat) működtetését, az erőforrások elosztását és igénybevételét vezérlik, illetve az informatikai fejlesztést és támogatást szolgálják.

A rendszerszoftverek mellett létezik egy másik típus is, a felhasználói, vagy pontosabban **felhasználó által készített szoftver.** Ezek alapvetően nem professzionális szoftverfejlesztők által készített kiegészítéseket, bővítéseket foglalnak magukban.

Az alkalmazói program kifejezés helyett egyre gyakrabban találkozhatunk az **alkalmazás** megnevezéssel is. Az új megnevezés bevezetésének egyik oka a szoftverek bonyolultságának növekedésében kereshető.

A számítógépes **alkalmazás** (*application, app)* egy olyan számítógépes program, amely az informatikai rendszer szolgáltatásait a benne végbemenő, az általa megvalósított adatfeldolgozási folyamatok (tevékenységek) segítségével nyújtják az alkalmazók részére[1].

Kezdetben egy feladat végrehajtását általában egy alkalmazói program támogatta, később azonban egyre gyakoribbá vált, hogy egy feladat néhány - összetartozó, egymást kiegészítő - program segítségével került megvalósításra, amelyeket együtt **alkalmazói programcsomag**nak neveztek. Az 1990-es években jelentek meg az úgynevezett **integrált programcsomagok,** amelyek egymástól eltérő, de kapcsolódó funkciójú alkalmazásokat - pld. szövegszerkesztőt, táblázatkezelőt és bemutató-készítőt - foglaltak magukba. A feladatorientált informatikai alkalmazások jó ideig a felhasználók egyedi igényei alapján, egyedi fejlesztés eredményeként készültek. Az informatika ugrásszerű fejlődésének, az általános célú alkalmazások képességei gyorsütemű bővülésének, következtében az egyedi fejlesztések helyébe a **kereskedelmi forgalomban kapható** (Commercial Off the Shelf, COTS) **szoftverek** alkalmazása, illetve beépítése lépett. Ebbe a csoportba a gyorsan beszerezhető és módosítás nélkül alkalmazható szoftverek tartoznak.[2]

Természetesen mindig akadtak olyan alkalmazói igények, melyek kielégítése ezekkel a kommersz szoftverekkel nem volt teljes mértekben elvégezhető. Ezért óhatatlanul megjelentek azok az igények, hogy a „gyári szoftvereket" első lépcsőben testre lehessen szabni, majd másodsorban azok az igények, hogy a feladatok végrehajtásához hiányzó speciális modulokat lehessen a felhasználók részéről kifejleszteni. Így egyre jobban tért hódítottak a saját alkalmazás-fejlesztések.

A testreszabás (paraméterezés), a **személyre-szabhatóság** elsődleges célja, hogy a felhasználók közvetlenül a nekik lényeges információkhoz jussanak hozzá, a számukra legmegfelelőbb formában. Ezek a testreszabási összetevők a következők lehetnek:

- a navigáció személyre szabása (könyvjelzők, kedvenc helyek kezelése);
- a tartalom személyre szabása (a megjelenítendő információk kiválaszthatósága);
- a megjelenés személyre szabása (elrendezés, formátum, színek, méretek beállíthatósága).

A személyre-szabhatóságot kétféle képen biztosíthatják a rendszerek. Vagy a fejlesztő által beépített lehetőségek kihasználásával, vagy valamilyen közismert programnyelven elkészíthető modulok beépítésével. Az első esetben egy kötött lehetőségeket biztosító választékból lehet a felhasználóknak válogatniuk, míg a második esetben elvileg tetszőleges, bármilyen igényt kielégítő modulok készíthetők. A gyári választék sok esetben csak néhány paraméterezési lehetőséget biztosít, első sorban úgynevezett skin-ek formájában. A saját készítés esetén viszont egy speciális programozói tudásra van szükség az igényesebb testreszabáshoz. A testreszabási beállítások a szervleteken tárolódnak, és a bejelentkezés és azonosítás után hajtódnak csak végre.

A **saját alkalmazás-fejlesztések** tesznek egy portál rendszert egyedivé, alakítják a standard gyári szolgáltatásokat a szervezet igényeihez.

A web portálok gyakran a World Wide Web-en megtalálható információk elérési pontjaként funkcionálnak. A portálok a különböző forrásokból származó információkat egységes

[1] Dr. Munk Sándor: Katonai informatika II. Katonai informatikai rendszerek, alkalmazások, ZMNE egyetemi jegyzet 2006, 36. oldal
[2] Dr. Munk Sándor: Katonai informatika II. Katonai informatikai rendszerek, alkalmazások, ZMNE egyetemi jegyzet 2006, 38. oldal

módon jelenítik meg. A web portálok a kereső szolgáltatások mellett más szolgáltatásokat is nyújtanak, mint elektronikus levelezés, hírek, tőzsdei információk, szórakoztatás, stb.[3]

A szervezeti portálokkal kapcsolatos első elképzelések technikai alapját az Internet-technológiára épülő szervezeti szintű belső hálózatok, az intranetek képezték. Ennek megfelelően a szervezeti portál egy olyan szervezeti intranet hely, amely felépítésében hasonló a népszerű Internet helyekhez, egy közös hozzáférési pontként szolgál a szervezeti információk egyesítéséhez, együttes felhasználásához, elosztásához.[4]

Az azonos alapokra (funkcionális és technológiai) épülő 'hagyományos', nyilvános portálok és szervezeti portálok között a hasonlóságok mellett már kezdetben jelentős **különbségek** is fennálltak. Ilyen különbségek lehetnek:

- a korlátozás nélküli felhasználói kör és az alapvető szolgáltatás;
- a speciális szervezet felhasználói köre és az alaprendeltetésnek megfelelő speciális szolgáltatás.

Az egyik jelentős portál-rendszer készítő cég a szervezeti portálok meghatározó tulajdonságait a következőképpen definiálta[5] (Plumtree Software):

- a web portálokhoz képest az adatformátumok szélesebb köréhez történő hozzáférés integrálása (***széleskörűség***);
- az elérhető információkhoz történő felhasználói hozzáférés szervezettsége (***szervezettség***);
- a kulcsfontosságú információk megjelenési formáinak személyre szabása és a felhasználók értesítése (elektronikus levélben és más módszerekkel) az új anyagok hozzáférhetőségéről (***személyre szabottság***);
- az adatokhoz való hozzáférés tárolási módtól független megszervezése (***tárolási hely függetlenség***);
- új információ típusokhoz tartozó kiterjesztések lehetősége (***kiterjeszthetőség***);
- az új tartalomhoz történő hozzáférés azonosításának és szervezésének automatizálása (***automatizáltság***);
- a belső szervezeti információkhoz való hozzáférés szelektív biztosítása (***védettség***);

Az alkalmazásfejlesztések a különféle portál típusok esetében más és más célt szolgálhatnak. A portálok típusai egyben determinálják a saját alkalmazásfejlesztési lehetőségeket. A lehetősségek feltárásához szükség van egy jól definiált portál típus besorolásra. A szakirodalomban a típusok meghatározása több szempontú:

- Felhasználói kör szerint:
    - Nyilvános portálok
        - Globális
        - Nemzeti-kormányzati (pl. Magyarország.hu)
        - Regionális
        - Települési
    - Szervezeti (zárt) portálok
        - Szervezetek, cégek, intézmények

[3] Webopedia: Online Dictionary for Computer and Internet Terms. – Jupitermedia Corporation, 2008.
[4] ANEJA, Atoul – ROWAN, Chia – BROOKSBY, Brian: Corporate Portal Framework for Transforming Content Chaos on Intranets. – Intel Technology Journal 2000/Q1 (21-28. o.)
[5] FIRESTONE, Joseph M.: *White Paper No. Thirteen. Defining the Enterprise Information Portal.* – Executive Information Systems Inc., 1999. július 31.
[www.dkms.com/papers/eipdef.pdf, 2009.10.31.; 4.page]

        - Nemzeti-minisztériumi (pl: Ügyfélkapu)
- Funkciócsoport szerint
    - Információszolgáltató- döntéstámogató
    - Együttes tevékenységet támogató (kollaboratív)
- Integráció szintje szerint
    - Tartalomportál (integráció a megjelenítés szintjén)
    - Alkalmazásportál (alkalmazás-szintű integráció)
    - Folyamatportál (az előzőek mellett rendelkezésre bocsátják a háttérben lévő rendszerek, alkalmazások funkcióit is)
- Szervezeti portálok - e-business funkciók szerint[6]
    - Alkalmazottak számára (B2E = business-to-employee (szervezet-alkalmazott)
    - Üzleti partnerek számára (B2B = business-to-business (szervezet-szervezet), vagy (B2G = business-to-government (szervezet-kormányzat)
    - Ügyfelek/fogyasztók számára (B2C = business-to-consumer (szervezet-ügyfél)

A fejlődési szakaszok, fejlettségi szempontok elemzése alapján egymást követően több **portál generáció** különíthető el.

- 1 generáció: tartalomkezelés, aggregálás, személyre szabás, keresés, kategorizálás
- 2 generáció: együttműködés támogatás, alkalmazás integráció
- 3. generáció: folyamat integráció, tudáskezelés, együttműködő keresés
- 4. generáció: fejlett web-szolgáltatások, JSR és WSRP szabványok, kompozit alkalmazások, többcsatornás interakció
- 5. generáció: kibővített együttműködés támogatás, JSR és WSRP szabványok, felhasználói tapasztalatkezelés
- 6. generáció: mindenütt jelenvalóság, felhasználó általi portál aggregáció, ügyfélkiszolgáló hosted alapú

Az információkhoz történő hozzáférés portálok általi támogatása egy idő után kiterjedt az informatikai rendszerekben, alkalmazásokban, adatbázisokban (szervezeti adattárházakban) rendelkezésre álló strukturált adatokra is. Ennek két alapvető formáját az adott rendszerek, alkalmazások által előre megtervezett módon biztosított jelentések, kimutatások, valamint az eseti (ad hoc) lekérdezések eredményei képezik. Az előbbiek elkészülhetnek előzetes ütemezés alapján, vagy az információigény felmerülésekor a legfrissebb adatok alapján. Az utóbbiak pedig a speciális érdeklődési köröknek megfelelően a portál saját fejlesztői környezetében, és az általa támogatott magas szintű programnyelven, vagy esetleg Java-ban, PPS-ben, illetve folyamatleíró nyelven programozva.

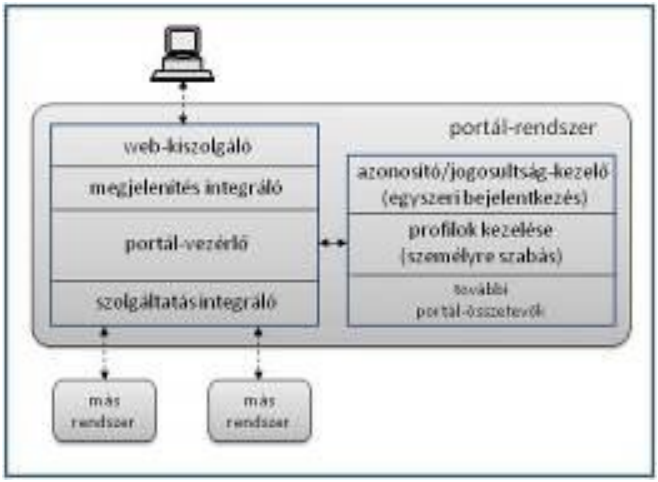
Az ***alkalmazásfejlesztés célja*** tehát egyfajta jobbítása, kiegészítése a meglévő portál rendszernek, és így irreveláns hogy, milyen szervezeti portálról van is szó.

[6] HONG Tuan Kiet Vo: *Engineering Corporate Portals. Dissertation.* – Der Fakultät für Wirtschaftswissenschaften der Universität Karlsruhe, 2007. [www.dkms.com/papers/eipdef.pdf, 2009.11.01. page:19.]

ALKALMAZÁSFEJLESZTÉSI LEHETŐSÉGEK AZ ISMERTEBB PORTÁL-RENDSZEREKBEN

Egy szervezeti portál megvalósításához, az általa nyújtott szolgáltatások biztosításához speciális informatikai rendszer-összetevők szükségesek, amelyeket portál-rendszereknek nevezhetünk. Egy **portál-rendszer** tehát hardver és szoftver összetevők, valamint adatok portál-szolgáltatásokat megvalósító, összetartozó együttese. A portál-rendszerek sajátossága, hogy általában nem csak saját szolgáltatásaikat nyújtják felhasználóiknak, hanem más rendszerek, alkalmazások szolgáltatásait is 'közvetítik', integrálják. Szervezeti portálok esetében ez utóbbiak lehetnek az adott szervezet saját, teljes körű, vagy viszonylagos önállósággal rendelkező rendszerei, alkalmazásai, de lehetnek az Interneten keresztül elérhető – a szervezet szempontjából – külső rendszerek, alkalmazások is.

A portál-rendszernek tartalmaznia kell egy web-kiszolgáló összetevőt, amely a felhasználók számára az Interneten, intraneten keresztül biztosítja a portál-szolgáltatások elérését. Mivel a portálok alapvető funkciója a különböző forrásokból származó információk integrálása, így a portál-rendszerek alapvető összetevői közé tartozik az egyes információforrások (alkalmazások) információit egy lapra integráló közös megjelenítő összetevő, valamint az egyes – külső és belső – forrásokat, alkalmazásokat bekapcsoló szolgáltatás-integrációs összetevő.



1. ábra: Portál-rendszer összetevői

További alapvető összetevők is azonosíthatóak, mint az egyszeri bejelentkezés lehetőségét biztosító felhasználó-azonosító és jogosultságkezelő összetevő; valamint a személyre szabhatóságot biztosító személyi profilokat kezelő összetevő.

A portál-rendszerek kialakítását a gyakorlatban ún. **portál-keretrendszerek** támogatják. A portál-keretrendszer portál-összetevők egy meghatározott együttese, amely (ritkábban) önmagában, vagy más rendszerekkel, alkalmazásokkal együttműködve biztosítja a kívánt portál-funkciók megvalósítását. A keretrendszerek által biztosított funkciók köre típusonként eltérő. Gyakran önálló – a keretrendszeren kívüli – összetevőként jelenik meg a web-kiszolgáló összetevő, vagy az alkalmazás-kiszolgáló formájában megjelenő szolgáltatás-integrációs összetevő. Szinte mindig önálló összetevőként kerül megvalósításra a tartalomkezelő, vagy ezen belül a dokumentumkezelő rendszer, mint a portál-rendszertől függetlenül is használható szolgáltatás.

A portálok egyik alapvető jellemzője, hogy egy lapon integrálva nyújtanak hozzáférési lehetőséget különböző forrásokból származó információkhoz, illetve alkalmazásokhoz. Egy

portál-lap önálló – általában kisebb ablakformátumú – részekből épül fel. Ezekben az ablakokban önálló, egymástól jellemzően független információforrások, alkalmazások tartalma jelenik meg, amelyeket gyakran portleteknek neveznek.

A **portlet** egy alkalmazás, amely meghatározott résztartalmat (információt, vagy szolgáltatást) generál egy portál-lap részeként történő felhasználásra. A portlet lehet önálló alkalmazás, vagy egy csatoló-összetevő egy külső/háttér alkalmazáshoz. A portlet valójában Java-alapú web-összetevőt jelent, azonban a portletet felhasználó összetevők[7] és a portletek közötti interfész szabványosításával ez már nem jelent igazi követelményt. A portlet szabványnak megfelelő környezetet biztosító portál-rendszerek számos, készen rendelkezésre álló portletet és ezzel szolgáltatásaikat (e-mail, naptár, hírcsatorna, stb.) integrálhatják magukba. A portál-rendszerek között többségben vannak a Java-alapú web-alkalmazás környezetre épülő típusok.[8] A Java szervezeti szintű platformja[9] a Java nyelven történő kiszolgáló-oldali szoftverfejlesztés széles körben alkalmazott környezete. Ez a futtatási környezet a standard Java környezet kiegészítése hibatűrő, elosztott, többrétegű, moduláris komponensekből felépülő, alkalmazás-kiszolgálókon futó web-alkalmazásokat támogató funkciókkal. Ilyen funkció többek között a dinamikus weblap-tartalmak előállítását biztosító JavaServer Pages technológia is.

A portál-rendszerek második csoportját a Microsoft ASP.NET technológiájára épülő rendszerek alkotják.[10] Ebben a környezetben hasonlóképpen megtalálható a web-alkalmazásokat támogató környezet, a .Net keretrendszer, valamint a dinamikus weblap-tartalmak előállítását támogató .NET-alapú Active Server Pages technológia. Míg a Java-alapú megoldás gyakorlatilag minden platformon elérhető, addig az .NET teljes kiépítésében csak Windows alapon, szűkített funkciókkal pedig LINUX-on és Macintosh-on áll rendelkezésre. Végül találkozhatunk még PHP és ASP-alapú portál-rendszerekkel is.[11]

Az 1990-es évektől kezdődően különböző szoftver cégek ajánlanak portál-rendszereket különböző célú és típusú portálok kialakítására és működtetésére. Ezek közé tartoznak többek között a Microsoft, az Oracle, és a Plumtree cégek termékei is. A portál-technológia fejlődése 2005 környékén új irányokat vett. Az önálló portál-rendszerek helyébe egyre inkább az infrastruktúra alapú rendszerek lépnek, az előbbiek egyszerűen beépülnek az utóbbiak összetevői közé.

A **Microsoft Office SharePoint** az intranet felhasználók közös munkáját támogató (kollaborációs) portál, amely belső kommunikációra, dokumentumok biztonságos megosztására, és a közös munka széleskörű támogatására alkalmas, amelynek első verzióját a Microsoft 2001-ben jelentette meg. A rendszerre épülő megoldások egy portálon belül ún. webhelyek egymásba ágyazásával jönnek létre. A fő portálról webhelyek nyithatók, melyekben további webhelyek hierarchikus rendje alakítható ki. Az MS Office család tagjaként, mint vállalati portál jelent meg a felhasználók igényeinek kielégítésére. A Microsoft Office SharePoint stabil megoldást kínál azoknak a kis- és középvállalatoknak, amelyeknek biztonságos és megbízható csoportmunka-eszközre van szüksége. Külföldön már számos szolgáltató kínál SharePoint termékeket, míg Magyarországon csak néhány éve indult az első ilyen szolgáltatás. A SharePoint a belső kommunikációra, a dokumentumok megosztására, és a közös munka támogatására alkalmas. A SharePoint webhelyeken a felhasználók nem csak az állományaikat tárolhatják és oszthatják meg, hanem többek között tárolhatják és megoszthatják naptárjaikat, a kapcsolattartók adatait, az internetes hivatkozásokat. A portál segítségével indíthatók vitafó-

[7] Portlet container = portlet befogadó (portlet környezet).
[8] Pld. IBM WebSphere Portal Server, Oracle Portal 10g, Oracle (BEA) WebLogic Portal, Vignette Portal.
[9] Java Platform, Enterprise Edition (JEE), korábban Java 2 Platform, Enterprise Edition (J2EE).
[10] Köztük természetesen a Microsoft Office SharePoint Server.
[11] Plumtree Portal Server ~ ASP, Joomla ~ PHP.

rumok, közzétehetők listák, közlemények. A feltöltött fájlokon, dokumentumokon akár egyszerre többen is dolgozhatnak[12].

Az **Oracle Portal** a vállalati portálok fejlesztését, üzembe helyezését és felügyeletét szolgáló teljes körű, integrált keretrendszer. Az Oracle cég, mint adatbázis-kezelő rendszerek kidolgozója, 2000-ben kezdett el vállalati keretrendszerek kialakításával foglalkozni. Kidolgozója és fő terjesztője a szolgáltatásorientált architektúrának (SOA), melytől azt várják, hogy a vállalatok áttekinthetetlen alkalmazási és informatikai környezeteit egyszerűsíti. Az Oracle Portal lehetővé teszi a biztonságos információ-elérést, az önkiszolgáló tartalom-közzétételt, az online csoportmunkát, és a folyamatautomatizálást. Az Oracle Portal az Oracle Fusion Middleware köztes-szoftvercsalád tagja, amely heterogén informatikai környezetekben is az eddigieknél nagyobb rugalmasságot, hatékonyabb döntéshozatalt, illetve alacsonyabb költségeket és kockázatot biztosít. Az Oracle Application Server az egyetlen olyan platform, amelyet számítógép-hálózatra terveztek, és teljes életciklus-támogatást nyújt a szolgáltatásorientált architektúra számára. Az Oracle Corporation a fejlesztők egyre növekvő igényeinek kielégítése érdekében létrehozta az Oracle portálkatalógust, amely több mint kétszáz portletet tartalmaz. A felhasználók így a kiválasztott portletekkel bővíthetik személyes igényeik szerint kialakított portállapjaikat. A katalógus az Oracle portálpartneri kezdeményezés (OPPI) tagjai által kifejlesztett, valamint független tartalomszolgáltatók, alkalmazásszolgáltatók vagy rendszerintegrátorok által regisztrált és az Oracle által elfogadott portleteket tartalmaz[13].

A **Plumtree Enterprise Portal** eszközeivel olyan vállalati portálmegoldások alakíthatóak ki, melyek támogatják a csoportmunkát, valamint a megosztott informatikai rendszerek és üzleti folyamatok összekapcsolását. A Plumtree Software-t 2005-ben felvásárolta a BEA Systems, majd később ezt az Oracle, így a Plumtree portál-rendszer utódai az Oracle termékvonalának részét képezik. A Plumtree portálja cross-platform eszköz, azaz a két cég – a Plumtree és a bevezető cég – szoftvereit összekapcsolva olyan infrastruktúra jön létre, amelylyel az ügyfelek kollaborációs és tranzakciós portál megoldásokat hozhatnak létre összetett platformokon és alkalmazásszereken. A Plumtree eszközei támogatják a nyílt, szabványos J2EE, .Net és szolgáltatás-orientált platformú megoldások kialakítását egyaránt. Piaci részesedése a legnagyobb volt Európában és Magyarországon is vezető helyet töltött be a portál rendszerek között. Két jellemző alkalmazása hazánkban a Paksi Atomerőmű Intranet portálja és a Magyar Honvédség Irodaautomatizálási Rendszere[14].

ALKALMAZÁSFEJLESZTÉSI FELADATOK, IRÁNYOK ÁLTALÁBAN ÉS AZ MH-BAN

A szervezeti portálok építésének ma már nem a portál-rendszer az ideális platformja, hanem egy olyan alkalmazás-készlet, amelynek az alapvető portál-funkciókat biztosító összetevő csak egyik része. A jövő szervezeti portáljai két alapvető szolgáltatás-készletre (és az ezeket megvalósító összetevőkre) épülnek majd, amelyek a hagyományos portál-funkciók jórészét átveszik, magukban foglalják. E két összetevő a felhasználóktól nagyobbrészt független hátteret biztosító **alkalmazás-kiszolgáló platformok** és a felhasználói kapcsolatot, előtér funkciókat biztosító **interakciós platformok**.

---

[12] *Az Office Sharepoint Server áttekintése.* – Microsoft Corp., 2009. [www.microsoft.com/hun/kozepvallalatok/products/wss/sps2007/default.mspx, 2009.01.17.]

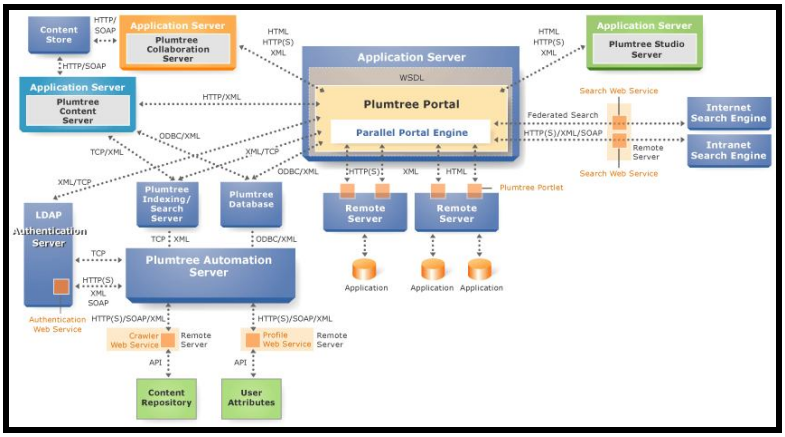
[13] *Oracle Portal 10g Release 2. Product Overview.* – Oracle Corp., 2004.

[14] Richard V. DRAGAN: Plumtree Corporate Portal 4.0. – *PC Magazine*, 2001 (20.)/11.

Az **MH Összhaderőnemi Parancsnokság**-án több éve üzemel valamilyen számítógépes hálózat. 2002-ben egy csapatgyakorlat megszervezésének ürügyén került kidolgozásra az első honvédségi alkalmazásra szánt hálózati szolgáltatás. Az akkor még Szárazföldi Parancsnokság hálózatában üzemelő rendszer, első tesztjére a Szablya 2002 gyakorlat alatt került sor. A teljes értékű üzembe helyezés a 2002. év végi telepítését követően történt meg, és működéséről immáron 7 éves üzemeltetési tapasztalat áll rendelkezésre[15]. Legelőször 2002. szeptemberében találkozhatott a Szárazföldi Parancsnokság tesztportáljának induló oldalával az a felhasználó, aki az MH hálózatának valamelyik számítógépén egy megadott címet meghívott a Web-böngészőjében. Az előzetes HM egyeztetéseken a különböző szakágak képviselői által felvetett igények kielégítésére ajánlották megoldásnak a portál technológia alkalmazásának lehetőségét, a Plumtree® cég portál rendszerének alkalmazását. A portálszerverek e tanulmány írásakor Székesfehérváron az MH. 43. Nagysándor József Híradó és Vezetéstámogató Ezred Összhaderőnemi Informatikai Főközpontjában üzemelnek. Szintén itt üzemel, a helyőrségben lévő alakulatokat kiszolgáló **DHCP, DNS** és **Exchange Server** melyek alá van rendelve az Összhaderőnemi Parancsnokság szerver parkja. A székesfehérvári kiszolgáló szerver a budapesti Hálózat Felügyelet kiszolgáló szervere alá van rendelve, és annak kiesése esetén képes átvenni az MH gerincháló üzemeltetési funkcióit.

A Plumtree Corporate Portal kapcsolja össze az alkalmazásokat és munkafelületeket valódi Vállalati Intranetté, indexeli és szervezi a tartalmakat, kezeli a biztonsági és felhasználói információkat. A portál tartalmazza a felhasználói felületet, akárcsak az adminisztrációs keretrendszert. A portál egész architektúrája teljes egészében web-szolgáltatásokon alapul. A felhasználók portletekből építik fel saját oldalaikat, olyan konfigurálható komponensekből, amelyek a leghasznosabb információkat és szolgáltatásokat integrálják a vállalati rendszerekből és az Internetről – például a levelezést, a raktárjelentéseket vagy az Internetes híreket. A portletek dokumentumok frissítését, felhasználói profilokat és a Tudáskönyvtár portletjeit is be tudják ágyazni, akárcsak a határidőnaplót, fórumokat vagy feladatlistákat a Collaboration Server-ből.

A portálhoz alkalmazott számítógépek nagyteljesítményű szervergépek. Kiépítettségüket mindig az éppen aktuális technikai szint szerint kell összeállítani, tehát a jelenlegi gépeket is folyamatosan bővíteni szükséges. Minden portálszolgáltató cég felépít egy általa javasolt hierarchiát arról, hogyan érdemes összeállítani a rendszer szervergépeit és melyikre mit kell telepíteni. Ez többnyire a kiépítettségtől, a várható kihasználtságtól és a felhasználók várható számától függ.



2. ábra: A Plumtree Vállalati Intranet csomag architekturális felépítése

[15] Bátor Tamás: Az irodaautomatizálásról mindenkinek, Szárazföldi Haderő, Székesfehérvár, 2006. IV. évfolyam I. rész, 23.old.

A Plumtree Vállalati Portálhoz számtalan integrációs és önálló portlet csomag létezik. A három legnépszerűbbek, az SAP, az Excel és az Exchange integrációs portlet készletek.

Az MH ÖHP vonatkozásában már több alkalmazási területet lehet felsorolni, mely saját alkalmazásfejlesztési keretek között valósult meg. A harcérték jelentés és riasztási feladatokat támogató alkalmazások, a jelentések nyilvántartása, a szabadságok, útba indítások rögzítése és nyilvántartása, az információ menedzsment rendszer (IMR) mind a hatékony munkavégzést segítik a törzsben dolgozó személyi állománynál. A csoportmunka területen az egyes főnökségek saját belső és állandó feladatait menedzselhetik, a speciális feladatokra létrehozott projektekben (pl.: missziók szervezése, erőforrások tervezése, stb.) pedig az érintett szervezetek delegált személyei tudnak együtt dolgozni. A hang-adat integrációs törekvések kivitelezése egyelőre még csak a tervezés, próbaüzemeltetés stádiumában létezik. A Magyar Honvédségen belüli csoportmunka, a tudásmenedzsment és az alkalmazás integrációs feladatok hátterét biztosító portál alapú technológia lehetővé tette a napjainkban is folyó irodaautomatizálási rendszer kialakulási folyamatát. A jelenleg működő portál webes technológiák segítségével lehetővé teszi rendezett formában történő, hatékony és gyors információkezelést, a szervezeten belüli egységesen használt alkalmazások elérését, a dokumentumok rendezését, rendszerezését és publikálását.

A **Párbeszéd portál** a Magyar Honvédség egyik olyan portál kezdeményezése, amely a B2E kategóriába (*Business to business)* sorolható, és egy speciális igényt kiszolgáló, zárt rendszerű, belső alkalmazói állományt megszólító, tájékoztató portál. A portálok jellemző funkcionális komponensei közül megvalósul a tartalomstruktúra (könyvtár szerkezetű hierarchia), a tartalomböngészés, keresés, a regisztráció utáni egy jelszavas beléptetés. 2003-ban kezdődött meg a Magyar Honvédség belső kommunikációjának vizsgálata. Míg a magyar haderő létszámában, struktúrájában, feladatrendszerében gyökeresen átalakult, addig a belső tájékoztatás gyakorlata nem tartott lépést a szükségletekkel, esetenként komoly kommunikációs zavarhoz vezetett. Igény mutatkozott egy olyan kommunikációs koncepció kidolgozására, amely a vezetői-szakmai információ-áramlás mellett megoldja a belső tájékoztatás problémáit, egyben elősegíti egy új szolgálati kultúra kialakulásának kezdeti lépéseit. 2005. szeptemberében útjára indult a Párbeszéd kommunikációs folyamat, melyben a teljes személyi állomány megismerte az elképzeléseket, a közép és hosszú távú terveket, és véleményt kértek tőlük a megoldási javaslatokról. A Párbeszéd portál a Magyar Honvédség tagjainak szóló, jelszóval védett, zárt, belső rendszer információk közlésére az Interneten keresztül. A megcélzott állomány a hivatásos, a szerződéses, a köztisztviselői és közalkalmazotti állomány mellett a hallgatói állomány és a nyugdíjasok köre. Hármas kitűzött célt, funkciót kellett megvalósítania: ***Tájékoztatás*** – ***Szolgáltatás*** (aktualizált tartalmi elemekkel), és ***Fórum*** (interaktív információ cserével).

Az MH és HM meglévő belső intranet hálózata erre a célra nem felhasználható, mert országos szintű lefedettséggel nem rendelkezik, és a külhoni szolgálatot teljesítő állomány részére sem biztosítana folyamatos, naprakész elérhetőséget. Ezért az Internetes megjelenítés volt az, amely az első pillanattól kezdve szóba jöhetett. Technikailag ezt az üzemeltetési formát három szerverrel oldották meg, mely szervereket az Informatikai Főközpontban (IFK) helyeztek el. Üzemeltetését, karbantartását, adatállományainak archiválását az IFK állománya látja el. Szintén Ők azok akik telepítették és folyamatosan frissítik – az SQL adatbázist, valamint a PlumTree típusú portál motort. A Párbeszéd portálon megjelenő adatok, információk hitelességéért a szakági felelősök – adatgazdák -, míg a naprakészségért az adat szervezet kommunikációs tisztjei a felelősek.

Párbeszéd portál Párbeszéd portál Kommunikációs oldal

3. ábra: A Párbeszédportál megjelenése

A fejlesztések várható irányai és feladatai

Az **MH Összhaderőnemi Parancsnokság**-án a távlati tervekben, első sorban a portáltechnológia kiterjesztése a cél. A minél szélesebb körben való alkalmazások elterjesztése, a speciális alkalmazások kibővítése, saját alkalmazások készítése. Ez a típusú fejlesztés két irányba indulhat el. Elsőként a már megvalósult és hatékonyan működő alkalmazások kiterjesztése minden szervezeti egységre (alakulatokra). Másik ágon pedig a bonyolultabb alkalmazások kifejlesztése, bevezetése a portállal már megismertetett szervezetek felhasználói részére. A fejlesztéseknek van személyi, és technikai vonzata egyaránt. A technikai fejlesztések körében gyorsabban és egyértelműben lehet megfelelő lépéseket tenni. Ilyenek lehetnek a portál üzemeltetést lehetővé tevő szerverbővítések, illetve a hálózatépítések folytatása. A személyi érdeklődések, alkalmazások tapasztalatai előrevetítik az egyre nagyobb alkalmazói kör kialakulásának lehetőségét. Feltétele a folyamatos képzés és önképzés fenntartása. Az alkalmazások körében is több alkalmazást kell a portálon keresztül elérhetővé tenni, és ezek alkalmazására a személyzetet kiképezni. Ez esetben a fő irány mindenképen az irodaautomatizáláshoz kapcsolódó feladatok megvalósítása lenne. Ezen kívül nagy hangsúlyt kell fektetni a döntéstámogató alkalmazások bevezetésére és a vezetői állomány bevonására mind az alkalmazások használata, mind fejlesztésük során. A szolgáltatások mindeddig zárt hálózaton voltak elérhetők, és egyenlőre úgy néz ki, hogy a továbbiakban sem lépett fel annak vezetői igénye, hogy a szolgáltatásokat az interneten keresztül is el lehessen érni, illetve, hogy extranetes szolgáltatásokkal bővítsük ki a rendszert. A NATO-s vagy az EU-s hálózatokra való csatlakozás egy teljesen új koncepciója lehet a további fejlesztési lépéseknek.

A **Párbeszéd portál** információs bázisát alapvetően három részre bonthatjuk. Első nagyobb rész a **naponta változó híranyagok** csokra, beleértve a honvédség egészét érintő katona-politikai, a csapat és missziós híreket. A másik részt a lap „statikusabb” oldalát képező, **szakági adatbázis** alkotja. A harmadik rész pedig maga a **fórum**, melynek sikeres üzemeltetése a szakágak, a kommunikációs tisztek, az üzemeltető személyzet és nem utolsó sorban, minden szintű parancsnok és vezető állomány közös felelőssége. A jövőre nézve kulcsfontossággal bír, hogy a kommunikációs tiszti állomány tagjai szakbeosztásukba kinevezve, megfelelőképpen felkészítve és folyamatosan képezve, minimális rotációval láthassák el feladatukat. Technikai ellátottságuk terén (számítógép, internet hozzáférés, fényképező, telefon) a múlt év példaadó eredménnyel szolgált, hisz ezen eszközök hiányában nem beszélhetünk hatékony munkáról. A szakági megjelenés tartalmi gazdagságában, naprakészségében változó a kép. A lap indulása alapvetően mindenki számára lehetőséget adott arra, hogy szervezetét, szakmáját, feladatrendszerét megjelentesse. Két év működésének tapasztalatait levonva mára szükségessé vált az információs bázis újragondolása, strukturális átértékelése, újrafogalmazása, kvázi közérthetőbbé, átgondoltabbá, áttekinthetővé tétele. Mindamellett nagyon fontos, hogy hatéko-

nyan tudjuk bemutatni a jövőbeni megvalósítandó szolgáltatásokat, amelyeket a rendszer alapjául szolgáló Plum Tree program képes biztosítani.

A Magyar Honvédségen belül egyenlőre nem tudunk beszélni egy, az MH teljes személyi állományát átfogó rendszerről, melynek lehetőségeit kihasználva teret tudnánk adni egy közösség működésére, legyen ez bármilyen közösség , nem csak szakmai, hanem szabadidős vagy akár egyéb érdekeltségből létrehozott. A párbeszéd lap alkalmas ezeknek az igényeknek a kielégítésére, hiszen ma is léteznek a lapon közösségek. Ha a szakmai oldalát tekintjük, akkor a jogász, kommunikációs tiszti csoportok már régóta használják a lapot zárt közösségként is, de akár egy-egy feladatra is létrehozható külön csoport, amelyre jó példa az éppen aktuálisan létrehozott Adatvédelmi Felülvizsgáló Bizottság felülete és jövőbeni tervek között szerepel egy Tiszti Kaszinó oldal kidolgozása is, mely szintén a megadott vizuális és funkcionális felhasználói igények beépítésével fog megvalósulni.

Egyes esetekben nem csak a felhasználói oldalon jelentkeznek a meg nem értés jelei, hanem a válaszadóin is. Mindez azt bizonyítja, hogy nem alakult még ki a kultúrája a tájékoztatás ezen formájának a Magyar Honvédségen belül. Ki, kit és milyen témában szólít(hat) meg és milyen választ vár el a felvetett kérdésekre, ne teljen el „beláthatatlanul" hosszú idő a kérdés és a válasz között, egyáltalán legyen válasz a kérdésre, stb. Az eszköz mindehhez adott, a személyi feltételek is nagyrészt biztosítottak, de alapvetően elmondható, hogy az elért eredmények ellenére is, jelentős áttörésre van szükség a belső tájékoztatás területén.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK, JAVASLATOK

A portál technológiai generációk az elsődleges információ elérés/tartalom aggregálás szintjét már jelentősen túllépték. A generációs fejlődés következő fokán álló alkalmazás integráció szintje az a szint, ahol ma áll a Magyar Honvédség webalapú szolgáltatása. A portál-alkalmazások vizsgálata során több szakemberrel is beszélgetve megfogalmazódik az az igény, hogy ma már elengedhetetlen egy olyan portál kialakítása és üzemeltetése, mely az alábbi funkciókat támogatja, és ezeket a funkciókat a szervezet feladatainak végrehajtása érdekében biztosítja:

- A szervezeti információkhoz való hozzáférés

A portál a szervezet összes olyan munkakörét támogatja, amelyben a tevékenység végrehajtásához szervezeti információkra van szükség. Az ilyen típusú információ lehet strukturált és nem strukturált egyaránt. A strukturált információk az adatszerű (numerikus, logikai, karakteres, stb.), általában adatbázisokban tárolt, és formatizált információk. A nem strukturált információk a kötetlen formájú, általában multimédiás jellegű információk (képek, hangok, animációk, stb.)

- A tartalomkezelés (content management)

A tartalomkezelés a szervezeti folyamatokhoz kapcsolódó tartalmak és dokumentumok megszerzése, kezelése, tárolása, megőrzése és rendelkezésre bocsátása során alkalmazott technológiák összessége. A tartalomkezelés alapvető jellemzője, hogy biztosítani kell a különböző verziók kezelését (tárolását, összevetését, visszaállítását) is.

- A szervezeti rendszerek és alkalmazások elérése

Ez tulajdonképpen az alkalmazás-integráció. Lényege, hogy a szervezeti tevékenységet támogató alkalmazások funkciói a portálon keresztül, egységes megjelenésben is elérhetőek legyenek. A megoldás alapját a portál-rendszer és az egyes alkalmazások közötti kapcsolatot megvalósító csatoló összetevők a portletek képezik.

- Az együttműködés támogatása (collaboration support)

A különböző dokumentumok elkészítése jellemzően több, különböző funkciókat megvalósító munkatárs együttműködését igényli. Az együttműködő felek közötti párbeszéd, információcsere számos lehetőséget biztosít. Ezek közé tartozhatnak például: elektronikus levelezés, valósidejű párbeszéd (chat), azonnali üzenetküldés, konferencia-szolgáltatások, levelező fórumok, internetes naplók (blogok), közösségi hálózatok, vagy virtuális környezetek.

Munkafolyamotok támogatása

A portál-szolgáltatások között egyre növekvő szerepet töltenek be az úgynevezett munkafolyamat (workflow) funkciók is.

A *szervezeti rendszerek és alkalmazások elérése* a belső, zárt intranet hálózatban a jelenlegi MH rendszeren a hozzáférési jogoknak megfelelően korrektül megvalósul. A felhasználói kör jelenleg jelentősen szűk, kiterjesztése a jövő feladata. Felül kell vizsgálni, és döntést kell hozni az Intranetes alkalmazás kitágításáról. Ennek egy kezdeti lépése lehet a bizonyos kiemelt személyek felhasználói jogkörének kibővítése. A távoli elérést is lehetővé tevő VPN alkalmazások segítségével a kiemelt szerepköröket betöltő felhasználók számára meg kell nyítni a távoli munkavégzés lehetőségét.. Ennek kiterjesztése nem szerepel a távolabbi fejlesztésekben, mert igen komoly veszélyforrásokat hordoz magában, amit a megfelelő védelmi berendezésekkel és intézkedésekkel ma már korrektül meg lehet oldani.

Az *együttműködés támogatása* ma még csak részben valósul meg. Az információcsere olyan formái mint az e-mail szolgáltatás, vagy bizonyos fokig a fórum kezdeményezések már beindultak, de a folyamatos, interaktív tevékenységekre még várni kell.

A *munkafolyamatok nyomon követése*, a vezetői beavatkozás lehetősége, a feladat kiosztás, vagy újraosztás biztosítása az a terület amelyet a leggyorsabban meg kellene valósítani. Ha a tevékenységek ütemezése, a logikai egymásra épültsége engedi, akkor ezt a workflow-t kellene a leggyorsabban megvalósítani az alapvető tartalomkezeléssel együtt.

A meglévő portál-rendszer felülvizsgálata (PlumTree) a több éve tartó teszt üzem, illetve a helyi elszórt kezdeményezések után napjaink egyik informatikai feladata. A PlumTree portál-rendszere mellett szoba jöhet a Microsoft Office SharePoint rendszere is, melynek alkalmazhatósági vizsgálata napjainkban is folyik a budapesti Informatikai Főközpontban. Bármely gyári rendszer mellet teszik is le a voksukat a megfelelő döntéshozók, a rendszereket az informatikai szakembereknek a speciális igények figyelembe vétele mellett szervezetekre igazítva kell üzembe helyezniük. Az üzembe helyezések során a helyi fejlesztések, alkalmazások elérését, a rendszerbe integrálását portleteken keresztül el kell végezniük. A fejlesztéseknek egységes szemléletben, egységes portál-technológiára alapozottan, és főleg az alkalmazások egységesítésével kell lezajlaniuk. Ehhez jelenleg nagyon kevés informatikai szakember áll rendelkezésre, és még a felhasználói igények felmérése is hiányzik. A technikai feltételek úgy, ahogy adottak, a szoftver-rendszerek rendelkezésre állnak, és az alkalmazói igények is már egyre erősebben jelentkeznek.

Jelen kidolgozás is ezt a célt szolgálja, nevezetesen a lehetőségek felmérése és vizsgálata után egy figyelemfelkeltő, igényt megfogalmazó szakanyagként kíván funkcionálni.

FELHASZNÁLT IRODALOM

[1] Dr. Munk Sándor: Katonai informatika II. Katonai informatikai rendszerek, alkalmazások, ZMNE egyetemi jegyzet 2006

[2] Webopedia: Online Dictionary for Computer and Internet Terms. – Jupitermedia Corporation, 2008.

[3] ANEJA, Atoul – ROWAN, Chia – BROOKSBY, Brian: Corporate Portal Framework for Transforming Content Chaos on Intranets. – Intel Technology Journal 2000/Q1 (21-28. o.)

[4] FIRESTONE, Joseph M.: *White Paper No. Thirteen. Defining the Enterprise Information Portal.* – Executive Information Systems Inc., 1999. július 31. [www.dkms.com/papers/eipdef.pdf, 2009.10.31.; 4.page]

[5] HONG Tuan Kiet Vo: *Engineering Corporate Portals. Dissertation.* – Der Fakultät für Wirtschaftswissenschaften der Universität Karlsruhe, 2007. [www.dkms.com/papers/eipdef.pdf, 2009.11.01. page:19.]

[6] *Az Office Sharepoint Server áttekintése.* – Microsoft Corp., 2009.

[www.microsoft.com/hun/kozepvallalatok/products/wss/sps2007/default.mspx, 2009.01.17.]

[7] *Oracle Portal 10g Release 2. Product Overview.* – Oracle Corp., 2004.

[8] Richard V. DRAGAN: Plumtree Corporate Portal 4.0. – *PC Magazine*, 2001 (20.)/11.

[9] Bátor Tamás: Az irodaautomatizálásról mindenkinek, Szárazföldi Haderő, Székesfehérvár, 2006. IV. évfolyam I. rész, 23. oldal.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Munk Sándor
munk.sandor@zmne.hu

HÁLÓZATOK FOGALMA, ALAPJAI

Absztrakt

A hálózatok napjaink divatos kifejezései közé tartoznak: "a hálózatok mindenütt ott vannak". A hálózatok között kiemelt szerepet játszanak a társadalom, a technika és a természet komplex hálózatai, amelyek a katonai és a polgári alkalmazásban is egyre növekvő jelentőséggel bírnak. A katonai alkalmazásban ezt bizonyítja a hálózatközpontú megközelítések előtérbe kerülése. A különböző jelzőkkel ellátott hálózat-kifejezések sok szakterületen alapvető szerepet játszanak, azonban értelmezéseik általában nem támaszkodnak közös fogalmi alapokra. A közös fogalmi alapok meghatározása talán leginkább az integrálódó, konvergáló információs hálózatok esetében szükséges. Ennek érdekében jelen publikáció az általános hálózat fogalom vizsgálatát, értelmezését tűzte ki céljául. Ezen belül: áttekinti a hálózat köznapi értelmezéseit; bemutatja különböző alkalmazási területek hálózattípusait; és elemzi a hálózat fogalmának általános értelmezését.

Networks are among the 'trendiest' words of our days: "the networks are everywhere". Of networks the complex networks play a crucial role in society, technology, and nature, and have increasing importance in military and civilian application. In military application this is demonstrated by network centric approaches. Networks with different adjectives play essential role in many specialties, but their interpretations do not rely on a common conceptual basis. This common conceptual basis is perhaps the most necessary in case of integrating, converging information networks. For this reason this publication aims to analyse, and interpret the general concept of network. In particular: overviews the everyday interpretations of network; presents different network types of different application areas; and analyses the general interpretation of the concept of networks.

***Kulcsszavak**: hálózat, általános fogalom, hálózattudomány, komplex rendszerek, ~ network, general concept, network science, complex systems*

BEVEZETÉS

A hálózatok napjaink divatos, gyakran használt kifejezései közé tartoznak. Mint azt a hálózatok neves magyar kutatója, Barabási Albert-László megfogalmazza: "Hálózatok mindenhol vannak. Az agy axonok által összekötött idegsejtek hálózata, maguk a sejtek pedig biokémiai reakciók által összekötött molekulák hálózatai. A társadalmak szintén hálózatok, olyan emberek hálózatai, akiket a barátság, a családi kapcsolatok és szakmai kötelékek kötnek össze. Magasabb szinten a táplálékláncok és ökoszisztémák a fajok hálózataiként ábrázolhatók. A hálózatok átjárják a technológiát is: az internet, az elektromos hálózatok, valamint a szállítási rendszerek csupán néhány példa erre. Még a nyelv is, amit gondolataink közvetítésre használunk, önmagában véve nem más, mint szintaktikai kapcsolatokkal összekötött szavak hálózata." [1, 1298.o.]

Egy, a hálózattudomány kereteit elemző tanulmány szerint "Olyan fontos hálózatok, mint az Internet és a villamos-energia hálózatok egyre nagyobbak lesznek, több százmillió, vagy akár milliárdnyi csomópontot foglalnak magukban. Csomópontjaik között összetett és gyakran dinamikus kapcsolati mintázatok találhatóak. Az egyes hálózatok egymással – sokszor rekurzív módon – is kapcsolatban állnak. Társadalmi hálózatok építenek információs hálózatokra, amelyek kommunikációs hálózatokra, azok pedig fizikai hálózatokra épülnek." [2, vii.o.]

A hálózatközpontú megközelítések az 1990-as évek végétől a katonai elméletben és gyakorlatban is előtérbe kerültek. Az Egyesült Államok haderejében megjelent a hálózatközpontú hadviselés (Network Centric Warfare), majd a tagállamok hasonló elképzeléseit összegezve született meg a NATO Hálózatalapú Képesség (NATO Network Enabled Capability) koncepciója. Ezek alapját egyrészt az informatika forradalmi ütemű fejlődése, a világméretű hálózatok kialakulása, valamint a polgári alkalmazás erre épülő eredményei, a hálózatközpontú szervezeti struktúrák és megoldások képezték.

A különböző minősítő jelzőkkel ellátott hálózatok a legkülönbözőbb szakterületek fogalomrendszerében megtalálhatóak, fontos szerepet játszanak a tudományos kutatásokban és a gyakorlati alkalmazásban egyaránt. Kiemelten igaz ez az információszerzést, információáramlást (információcserét), információhoz történő hozzáférést támogató hálózatok esetében. A hálózat fogalmak ilyen jelentős szerepe ellenére az egyes szakterületi értelmezések általában nem támaszkodnak közös fogalmi alapokra, nem építenek általánosan érvényes megállapításokra.

Mint azt egy korábbi publikációban már megfogalmaztam "a kommunikáció (távközlés, hírközlés, híradás), az informatika (számítástechnika), illetve az információtechnológia más, szélesebb körben elterjedő szakterületei … egységes fogalomrendszerének kialakítása szükségessé teszi a valamennyi szakterületen alkalmazott alapfogalmak meghatározását, rendszerezését, egységesen elfogadott értelmezésük kialakítását." [3, 62.o.]

A fentiek alapján jelen publikáció alapvető célja, egy nagyobb kutatás részeként, a hálózat általános – valamennyi szakterület számára alapul szolgáló – fogalmának vizsgálata, értelmezése. Ennek érdekében:

- áttekinti a hálózat kifejezés köznapi értelmezéseit;
- bemutatja a különböző alkalmazási és szakterületek egyes hálózat-típusait;
- elemzi a hálózat fogalom általános értelmezését.

A HÁLÓZAT KÖZNAPI ÉRTELMEZÉSEI

A *hálózat kifejezés a magyar nyelvben* a háló szóból, az általában a sajátosan szervezett dolgok összességére alkalmazott -zat/-zet gyűjtőnévképző alkalmazásával keletkezett. A háló elsődleges jelentései a Magyar Nyelv Értelmező Szótára szerint:

"1. Ált. fonalból, csomózással készített, nagy likacsú szövedék.
2. erős fonálból csomózott, kisebb-nagyobb méretű, különféle alakú és szerkezetű halászó eszköz.
3. földön futó v. alacsonyan repülő madarak, ritk. apróbb vadak megfogására használt, karókra, rudakra erősített, hosszú széles szövedék. …" [4, 72.o.]

Hasonló értelmezés szerepel az 1990-es évek végén kiadott Magyar Nagylexikonban: "olyan rácsszerű anyag (pl. textil, drót), amelynek egységnyi felületén az anyag sokkal kisebb részarányt képvisel, mint az általa közrefogott nyílás. Régebben főként a kötélből v. zsinórból, csomózással előállított háló volt használatban. …" [5, 157.o.] A finnugor eredetűnek tartott szó eredeti jelentése a halászatban alkalmazott eszköz volt.

A hálózat kifejezés jelentése a Magyar Nyelv Értelmező Szótára szerint:

"1. egymást átszelő egyenes v. görbe vonalak sűrű, szabályos szövedéke, rendszere.
2. nagy területet behálózó műszaki (közlekedési, villamossági, hírközlő, csatorna, stb.) létesítmények összefüggő rendszere.
3. (átv.) egymással összefüggésben levő, hasonló v. azonos intézmények egységesen szervezett, kiterjedt rendszere." [4, 76.o.]

A Magyar Nagylexikonban a hálózat meghatározása nem szerepel, helyette csak utalás van a villamos hálózat és a kereskedelmi hálózat fogalmakra. [5, 164.o.] Az 1960-as években kiadott Új Magyar Lexikon részletesebb és általánosabb meghatározást tartalmaz: "(műsz.) a másodlagos energiahordozók (pl. villamos áram, városi gáz, stb.) szállítására szolgáló vezetékrendszer (drót-, ill. cső-), mely a termelő telepek és a fogyasztó között biztosít kapcsolatot. – Tágabb értelmezésben nagyobb területen fekvő, egymással összefüggő, azonos jellegű létesítmények láncolata (pl. üzlet~, vasút~, stb.)" [6, 189.o.]

Az 1910-es évek Révai Nagy Lexikonában még erdészeti tartalommal találkozhatunk: "(erdészeti) az ültetéssel való erdősítésnél a csemetéknek bizonyos rendszer szerint való kiültetése." [7, 428.o.] Az 1930-as évek végén kiadott Új Idők Lexikona már a villamos energia hálózat jelentést tartalmazza: "(elektromos H.) összeköttetést létesít a fogyasztóberendezések és az áramtermelő telep között. … a vezetékrendszer egészen hálószerű, innen a neve. …" [8, 02971.o.]

A *hálózat kifejezés (network) az angol nyelvben* hasonlóképpen a háló (net) származéka. A 'net' jelentései a Webster's és az Oxford szótárakban a következőek:

"1. csipkeszerű, egyenletes likacsos karton, selyem, műselyem, nylon, stb. anyag, amely gyakran különböző csipkék alapjául szolgál;
2. speciális célra, például ütővel játszott játékok játékterének felosztására, vagy rovarok elleni védelemre szolgáló likacsos szövetanyag;
3. erős zsinórból, vagy kötélből készült, likacsos zsák, vagy más eszköz halak, madarak, vagy más állatok elfogására." [9, 960.o.]

"1. zsinegből, zsinórból, vagy valami hasonlóból készült nyitott szemű anyag, jellemzően halak, vagy más állatok elfogására;
2. keretre szerelt hálóból álló szerkezet, amely olyan játékok célját képezi, mint a labdarúgás;

3. nyitott szövésű finom anyag;
4. …" [10]

A hálózat kifejezés különböző jelentései a két előbb említett szótárban a következőek:
"1. szálak, vonalak, erek, vezetékek és más hasonló dolgok hálószerű együttese;
2. épületek, hivatalok, állomások, stb. egymással kapcsolatban álló rendszere, különösen egy nagyobb területen, országban, tartományban, vagy régióban." [9, 960.o.]
"1. egymást metsző függőleges és vízszintes vonalak elrendeződése;
2. egymással kapcsolatban álló emberek, vagy dolgok csoportja, rendszere.
- vasútvonalak, közutak, vagy más utak komplex rendszere;
- szakmai, vagy társadalmi célokból információt cserélő emberek csoportja;
- ugyanazon program továbbítását szolgáló műsorszóró állomások csoportja;
- összekapcsolt számítógépek, gépek, vagy műveletek;
- csatlakozó elektromos vezetékek." [10]

Az angol nyelvben vannak más kifejezések is hasonló tartalommal. Ezek közé tartozik a hálószerű anyag, háló szeme (mesh), a szövedék (web), valamint a rácsozat (grid). A 'web' napjainkban már az Interneten működő hypertext rendszer (World Wide Web) közszóvá vált megnevezése. A 'grid' kifejezéssel pedig sokszor lehet találkozni a technikai jellegű hálózatok megnevezésében: pld. országos áramhálózat, az Egyesült Államok haderejének Globális Informatikai Hálózata, vagy a számítási gridek, grid-alapú számítások.[1]

A *hálózat kifejezés más nyelvekben* a magyartól és angoltól sokszor eltérően jelenik meg. A német nyelvben a hálózat kifejezés egyes változataiban a német nyelvben eredetileg csak az angol 'net' szóval azonos gyökerű 'Netz' szerepelt[2]. Ezek mellett ma már találkozhatunk a 'Netzwerk' változatokkal is. Egyes vélemények szerint a 'Netzwerk' kifejezés csak Tannenbaum: Számítógép-hálózatok című könyvének németre fordításával jelent meg. Napjainkban a két kifejezés már nem minden helyzetben cserélhető fel: pld. [digitális] hálózati kártya (Netzwerkkarte) és [elektromos] hálózati tápegység (Netzteil). A francia nyelvben eltérő kifejezés jelöli a pókhálót (toile), a halászhálót (filet) és a különböző (ér-, vasút-/közút-/telefon-, kereskedelmi, kém-) hálózatokat (réseau). Mint látható, ez utóbbi nem az előzőekből képzett kifejezés, eredete a latin 'rete' = háló kifejezésre vezethető vissza. Az orosz nyelvben a magyarban részben eltérő háló és hálózat tartalmak megnevezésére egyaránt a 'сеть' kifejezés szolgál, a hálózat megkülönböztetésére nem alakult ki új kifejezés.

HÁLÓZATFOGALMAK, TÍPUSOK

A tapasztalat azt mutatja, hogy a hálózat (egyelőre részletesebb értelmezés nélkül használt) fogalma a természet, a technika és a társadalom számos rendszerének, objektumának, jelenségének leírására alkalmas. Ennek megfelelően széles körben, a legkülönbözőbb szakterületeken találkozhatunk a különböző jelzőkkel ellátott hálózat kifejezésekkel. A fogalom általános értelmezése előtt tekintsünk át röviden néhány jellemző példát szakterületi hálózat-fogalmakra és egyes sajátosságaikra.

[1] Global Information Grid (GIG), grid computing.
[2] Stromnetz = villamoshálózat, Telefonnetz = telefonhálózat, Computernetz/Rechnernetz = számítógép-hálózat

A *természeti, molekuláris és biológiai hálózatok* között számos példát találhatunk egymáshoz csatlakozó vonalas összetevőkből felépülő hálózatokra, amelyek sok esetben hierarchikus szerkezetűek. Ilyenek például:

- a természeti környezet vízhálózatai (folyórendszerei), amelyek egy adott térség egymásba ömlő felszíni vízfolyásainak együttesei;
- a növények gyökérhálózata (gyökérzete), amely főgyökerek, vagy mellékgyökerek, majd azokból kiinduló oldalgyökerek és hajszálgyökerek rendszere;
- a keringési rendszer részét képező érhálózat, amely főverőerek, verőerek, kiserek, hajszálerek, gyűjtőerek és vénák összessége;
- az idegrendszer részét képező neurális (ideg-) hálózat, amely az idegsejtek elektromos és kémiai kapcsolódási pontok (szinapszisok) segítségével összekapcsolt csoportja.

Az előzőekben felsoroltak mellett az élővilágban olyan folyamatokat is találhatunk, amelyek szintén hálózatként jellemezhetőek, vizsgálhatóak. Ezek közé tartoznak többek között a következőek:

- a sejtek anyagcsere-hálózatai, amelyek az élő szervezetben lejátszódó reakciók, egymásra épülő reakció-utak összefüggő rendszerei;
- az ökoszisztémák táplálékhálózatai (egyszerűbb esetben táplálékláncok), amelyek egy élőhely fajainak táplálkozási kapcsolatait írják le.

Ezek esetében a hálózatot alkotó utak (kapcsolatok) már nem megfogható módon létező dolgok, hanem felismert kapcsolatok, összefüggések, ami a hálózatjellegből és a hálózatorientált szemléletmód használhatóságából semmit sem von le.

Az *épített környezet és a technika világa* az előzőeknél is több példát nyújt hálózatokra. Ilyenekkel találkozhatunk például a közlekedés, illetve a vezetékes szállítás (köztük a közüzemi szolgáltatások) területén:

- az úthálózatok (általában) a használat során kialakult, vagy mesterségesen kialakított utak összefüggő rendszerei, ezen belül a közúthálózat az országos közutak és helyi közutak együttese;
- a vasúthálózatok (vagy vasúti pályahálózatok) fővonalak, mellékvonalak, összekötő és csatlakozó pályák összefüggő rendszerei, amelyek csomópontjait vasútállomások, pályaudvarok képezik;
- a vízi közlekedési hálózatok vízi közlekedési útvonalak kikötőkkel összekapcsolt rendszerei;
- a légiközlekedési hálózatok légiközlekedési útvonalak repülőterekkel összekapcsolt rendszerei;
- a villamos energia szállítását biztosító átviteli és elosztó hálózatok az erőműveket, átalakító- és kapcsoló-berendezéseket, csatlakozási pontokat, valamint a fogyasztói helyeket összekötő különböző vezetékek rendszerei;
- végül a különböző gáznemű és cseppfolyós anyagok (ivóvíz, szennyvíz, gáz, kőolaj, stb.) szállítására szolgáló csővezeték-hálózatok forrás-, továbbító (szivattyú/kompresszor), szabályozó/lezáró, valamint célállomásokat összekötő csővezetékek rendszerei.

Napjaink technikai hálózatai között egyre növekvő jelentőséggel bírnak az *információkat továbbító, elosztó hálózatok*, amelyek közül – mivel egy későbbi publikációban részletesebben fogunk velük foglalkozni – szemléltetésképpen csak felsorolásszerűen említjük meg a következőket: távíró-, rádió-, távbeszélő-, műsorszóró, számítógép-, szenzor-, stb., általánosabb értelemben pedig távközlési és informatikai hálózatok.

A technikai hálózatok sajátos formáját képviselik az úgynevezett *áramköri (villamos) hálózatok*, amelyek egy vagy több áramforrásból, egy vagy több fogyasztóból és további áramköri (kapcsoló, szabályozó, stb.) elemekből, valamint az ezeket összekötő átviteli vonalakból (vezetékekből és/vagy vezetéknélküli összeköttetésekből) felépülő rendszerek.

Napjainkban már a *társadalmi szféra hálózatai* is a tudományos kutatás és a mindennapi élet középpontjába kerültek. Központi összetevőiket a társadalmi szféra szereplői (az egyes emberek és ezek tartós csoportjai) alkotják, amelyeket különböző szociális kapcsolatok rendeznek hálózatokba. Ilyenek például a következőek:

- a településhálózatok egy adott térség egymással sokrétű (pld. együttműködési, alá-fölérendeltségi) kapcsolatban álló településeinek összességei;
- az intézményhálózatok egy adott funkciójú, adott szolgáltatási (pld. kereskedelmi, oktatási, művelődési, egészségügyi, stb.) körbe tartozó, különböző helyekre telepített intézmények rendszerei (ezen belül beszélhetünk egy adott tulajdonoshoz, szervezetrendszerhez tartozó intézmények hálózatáról is);
- végül a közösségi (ismeretségi) hálózatok egyének és a köztük fennálló szociális kapcsolatok (barátság, rokonság, közös érdeklődés, stb.) összességei.

A HÁLÓZAT FOGALOM ÉRTELMEZÉSE

Az előzőekben láthattuk, hogy a hálózat fogalom köznyelvi definíciói általában nem egy átfogó meghatározást, hanem több párhuzamos értelmezést tartalmaznak. A szakterületi lexikonokban, fogalomjegyzékekben, dokumentumokban ezzel szemben a hálózat minősítő jelzővel ellátott, vagy jelző nélküli kifejezésével és mindkét esetben az ehhez tartozó szakterület-specifikus meghatározásokkal találkozhatunk. Napjainkban gyakorlatilag csak az egyre növekvő népszerűségű hálózatelméleti, hálózattudományi[3] kutatások foglalkoznak a hálózat általános tartalmú meghatározásával.

Az előző pontban bemutatott *hálózat-fajták közös jellemzőit* keresve megállapítható, hogy valamennyien összekapcsolt elemek, objektumok rendszerei. Az egyes hálózatok elemei sokfélék lehetnek: folyók, erek, anyagcsere reakciók, fajok, utak, villamos energia erőművek és fogyasztók, áramköri elemek, intézmények, vagy emberek. Hasonlóképpen sokfélék az egyes elemek között fennálló kapcsolatok is: folyók, erek egymásba folyása; reakciók egymásra épülése; fajok táplálkozási kapcsolatai; utak csatlakozása; villamos energia vezetékek; áramköri kapcsolatok; intézmények közötti kapcsolatok; vagy szociális kapcsolatok.

Bár ezzel a hálózatokat általában vizsgáló tudományok ritkábban foglalkoznak, a különböző hálózatok két nagy csoportba sorolhatóak. Az első csoportot a vonalasnak nevezhető hálózatok képezik, amelyekben az alapvető, elsődleges elemek vonalas objektumok (folyók, erek, utak, stb.) és kapcsolataikat ezek találkozásai képezik. A második csoportba tartozó hálózatok központi elemei a csomópontok és a kapcsolatokat az ezek között fennálló fizikai, vagy absztrakt összeköttetések, összefüggések alkotják. A vonalas hálózatok esetében az egyes vonalas objektumok több csatlakozási ponton át is megőrzik azonosságukat (pld. folyók, közutak, stb.), míg a csomópont hálózatok összeköttetései két csomópont között léteznek. A hálózatok fenti csoportosítás szerinti besorolása nem mindig egyértelmű, mivel csomópont hálózatok esetében is van lehetőség az egyes kapcsolatok összetett kapcsolat-sorozatokba, láncokba rendezésére.

[3] Network Theory, Network Science.

Az összekapcsoltság, a kapcsolatrendszer a hálózatok alapvető összetevője, azonban köznapi értelemben nem minden kapcsolatrendszert nevezünk hálózatszerűnek. A hálózat és a *hálózatszerűség* fogalmaihoz – ha nem is kizárólagos értelemben – hozzákapcsolódik a kapcsolatrendszer összetettsége, komplexitása. A hálózatszerű kapcsolatrendszer egyik megkülönböztető jellemzője lehet az erősen összekapcsoltság, hogy a különböző elemek között több összeköttetés létezik, vagyis a kapcsolatrendszer nem fastruktúrájú.[4]

A szervezeti struktúrák esetében a *hálózati jelző* például egy autonóm együttműködő szervezetek közötti, összetett, laza, dinamikusan változó kapcsolatrendszert jelez. A hálózatközpontú katonai megközelítések esetében (pld. hálózatközpontú hadviselés, hálózatalapú képesség) pedig a *hálózati jelleg* mindenekelőtt különböző elemek, összetevők – korábban nem létező – összekapcsolásában és ennek révén képességeik, szolgáltatásaik hatékonyabb kihasználásában, a feladatmegosztás és a végrehajtás magasabb szintű rugalmasságában rejlik. A hálózati kapcsolatok alapvetően információcserét és szolgáltatásnyújtást biztosítanak. A hálózatközpontú megközelítések gyakran használt fogalmai közé tartoznak a 'hálózatosítás/hálózatba kapcsolás' és a 'hálózatos/hálózati' jelző, amelyeket gyakran kiegészít az 'erőteljes' minősítés is, ami az összetett kapcsolatrendszerre utal.[5] [11, 88-91.o.; 12, 17.o.].

A *hálózat fogalma* a hálózattudományban matematikai, ezen belül gráfelméleti alapokra épül. Ennek megfelelően a hálózat csúcsok/csúcspontok (csomópontok) és az ezeket páronként összekapcsoló élek (kapcsolatok) összessége.[6] Az ezzel lényegében megegyező tartalmú gráf fogalom azonban csak a hálózatok legegyszerűbb változatainak leírására alkalmas. Az előzőekben bemutatott hálózatok ennél sok szempontból összetettebbek. Lehetséges például, hogy a hálózat csomópontjai nem egyneműek, különböző csoportokba sorolhatóak és a köztük fennálló kapcsolatok, élek is eltérő típusokhoz tartoznak. Ezen kívül mind a csomópontokhoz, mind az élekhez különböző – numerikus és más – tulajdonságok kapcsolódhatnak. A hálózatok továbbá változhatnak, új csomópontok és élek keletkezhetnek, meglévő csomópontok és élek szűnhetnek meg. Végül a hálózatok esetében a topológiai tulajdonságok mellett lényegesek lehetnek a térbeli, földrajzi jellemzők is.

A felsorolt sajátosságok kezelésére a gráfelmélet és az operációkutatás is bevezetett új fogalmakat, mint az irányított gráfok, súlyozott gráfok, véletlen gráfok, hálózati folyamok, stb. és folytatja ezek vizsgálatát, azonban ezek is csak korlátozott mértékben felelnek meg a valós hálózatok problémáinak vizsgálatára. A *hálózat a gráfelméletben, operációkutatásban* (a hálózati folyamokhoz kapcsolódóan) olyan irányított gráf, amelyben az élekhez alsó korlát, kapacitás és költség értékek, a csomópontokhoz pedig kínálat/kereslet értékek tartoznak. [13, 95.o.; 14, 3.o.] Ez a modell lehetővé tette számos leíró ('mi van'), előrejelző ('mi lesz') és előíró ('minek kell lennie') jellegű probléma, feladat megoldását.

A *hálózat a hálózattudomány fogalomrendszerében* a valóságban létező fizikai, biológiai és társadalmi objektumok absztrakciója, vagyis "a hálózat mindig a megfigyelhető valóság egy reprezentációja, vagy modellje és nem a valóság maga". Ebből következik az is, hogy ugyanazon rendszernek, folyamatnak, jelenségnek létezhet több különböző reprezentációja, leírható különböző hálózatok formájában is. [2, 27.o.] Ennek megfelelően "a hálózattudomány a fizikai, biológiai és társadalmi jelenségek hálózat reprezentációit vizsgáló tudományterület",

[4] Lásd például a szekvenciális, hierarchikus és 'hálós' adatszerkezetek megkülönböztetését.
[5] Networking, networked, robust networking, robustly networked.
[6] Vertex, node, edge, link.

amelynek célja különböző területeken alkalmazható modellek, technikák, eszközök kialakítása. [2, 28.o.]

A *hálózat és rendszer* fogalmak szoros kapcsolatban állnak egymással. A rendszerek általánosítható tulajdonságainak (struktúrájának, viselkedésének, stb.) vizsgálatával a múlt század közepén létrejött rendszerelmélet foglalkozik. A rendszer egy értelmezés szerint egymással kölcsönhatásban, kapcsolatban álló elemeknek olyan együttese, amely meghatározott körülmények között egészként szemlélhető. A struktúra pedig az elemek elrendeződésének, kapcsolódásának módja, formája. [15]

A hálózattudomány éppen a rendszerek, ezeken belül a komplex rendszerek struktúráját (struktúráit) tanulmányozza. [16] Ez megjelenik a hálózattudomány egyik, már hivatkozott alapvető dokumentumában is, ahol igényként fogalmazódik meg "egy hálózattudománynak nevezett új kutatási terület létrehozása, amely bővíti a komplex rendszerekre és a hálózati viselkedést megjelenítő folyamatokra vonatkozó tudást". [2, 26.o.]

A *komplex rendszer* meghatározása már a rendszerelmélet első anyagaiban megjelent, de elsődlegesen a fizikában került alkalmazásra olyan rendszerek esetében, ahol az alkotóelemek nagy száma és a közöttük lévő kölcsönhatás révén a rendszer viselkedése az egyes egységekétől lényegesen eltérő sajátosságokat mutat. [17] Tehát a komplex rendszer egyes tulajdonságai (viselkedése), nem vezethetőek le összetevői tulajdonságaiból. Az ilyen tulajdonságokat emergensnek (hirtelen megjelenőnek) is nevezik, amelynek lényegére különböző értelmezésekkel találkozhatunk. Ezek közül témánk szempontjából a következők használhatóak: egyszerű alacsony szintű mechanizmusok egyszerű módon történő kombinálódása révén bonyolult és érdekes magas szintű funkciók jönnek létre; egy rendszerben a tervező céljai között nem szereplő érdekes tulajdonságok jelennek meg. [18, 49-50.o.]

A *komplex hálózatok* egy meghatározás szerint nem triviális topológiai jellemzőkkel rendelkező – vagyis nem egyszerű, szabályos (pld. rács-) és nem is véletlenül kialakult – hálózatok. [2, 62.o.] Más megfogalmazások szerint a komplex hálózatok olyan hálózatok, amelyek struktúrája nem szabályos, összetett és időben dinamikusan változó, a hálózattudomány célja pedig a kis hálózatok elemzése helyett a több ezer, vagy millió, köztük dinamikusan működő csomópontokból felépülő rendszerek vizsgálata. [19, 177.o.] A fogalom jelentőségét mutatja, hogy az ilyen komplex hálózatok közé tartozik a legtöbb társadalmi, biológiai és technikai hálózat.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az előzőekben elmondottakra építve megfogalmazható, hogy a legáltalánosabb értelmű – jelző nélküli – 'hálózat' fogalom valamely létező, vagy elképzelt objektum (rendszer, folyamat, jelenség, stb.) valamilyen szintű absztrakciója, amelynek lényege az objektum elemeinek és az azok között fennálló kapcsolatoknak – vagyis az objektum (valamely) struktúrájának – a megjelenítése, leírása. A legmagasabb szintű absztrakció eredménye a matematikai gráfok formájában történő reprezentáció. A hálózatok szélesebb körben hasznosítható értelmezése ennél valamivel alacsonyabb szintű absztrakciót, vagyis az adott objektum több sajátosságának megjelenítését igényli.

A hálózat fogalom reprezentációként történő értelmezése természetesen nem veszi el a létjogosultságot valós rendszerek hálózatoknak nevezésétől, azonban látni kell, hogy egy valós

rendszer mindig több mint egy 'hálózat', sőt ugyanazt a rendszert különböző vizsgálati szempontok, nézőpontok alapján különböző 'hálózatok' írják le, különböző hálózatoknak tekinthetők.

A fentiek alapján a *hálózat általános fogalma* a következő formában határozható meg: meghatározott tulajdonságokkal rendelkező elemek (csomópontok) és az ezek között fennálló, meghatározott tulajdonságokkal rendelkező kapcsolatok összessége. A definícióból következően egy adott hálózat esetében:
- meg kell határozni, hogy melyek a hálózat csomópontjait alkotó elemek;
- melyek ezen elemek releváns típusai, tulajdonságai;
- melyek az elemek között fennálló kapcsolatok;
- és melyek ezen kapcsolatok releváns típusai, tulajdonságai.

A hálózatok – a definícióból láthatóan – önmagukban is eleget tesznek a rendszerfogalom kritériumainak, így a rendszerelméletben megfogalmazott elveknek megfelelően a hálózat elemeinek, kapcsolatainak és ezek figyelembe veendő tulajdonságainak meghatározása vizsgálati cél-függő. Ezenkívül esetükben is nyilvánvalóan értelmezhetőek a részhálózat (alhálózat[7]) fogalmak. Részhálózat alatt egy hálózat kiválasztott elemeinek és kapcsolatainak olyan összességét értjük, amely maga is hálózatot alkot. A részhálózat körülhatárolása során szűkülhet az elemek és tulajdonságaik, illetve a kapcsolatok és tulajdonságaik köre.

A fentiekben megfogalmazott definícióra építve a hálózatok adott típusai (köztük az információs folyamatok, tevékenységek támogatásához kapcsolódó, információs szolgáltatásokat nyújtó hálózatok) fogalmi alapjainak vizsgálatához a további kutatások során először össze kell gyűjteni a szakmai és tudományos irodalomban leggyakrabban előforduló kifejezéseket és ezek rögzített, vagy kikövetkeztethető értelmezését. Fel kell tárni a szinonimákat (azonos tartalmú, de eltérő megnevezésű fogalmak) és a homonimákat (azonos megnevezésű, de eltérő tartalmú fogalmakat).

Ezt követően – a tudományos fogalom-alkotás szabályainak megfelelően – meg kell határozni az adott csoportba, illetve ezen belül különböző alcsoportokba tartozó hálózatok közös megkülönböztető jegyeit. Ez teszi lehetővé a gyakorlatban előforduló számos, jelzővel ellátott hálózat-fogalom rendszerezését, egymáshoz való viszonyuk tisztázását, az alapvető fogalmak kiválasztását és tartalmuk meghatározását. A magasabb szintű nem-fogalmon (hálózat) belüli fogalomképző jegyek sokfélék lehetnek és sokfélék lehetnek indokoltak, valamilyen célból hasznosak.

Végül az 'információs tevékenységek támogatásához kapcsolódó' hálózatok, legfontosabb hálózat-típusok esetében a fogalom-meghatározások után végre kell hajtani az adott típus esetében alapvetőnek tekintett elemek és kapcsolatok, valamint ezek lényeges tulajdonságai kiválasztását, meghatározását.

Az 'információs hálózatok' fogalmi alapjainak tisztázása során külön feladatként kell majd megoldani a hálózat – rendszer – infrastruktúra fogalmak tartalmának, összefüggéseinek feltárását is. Előzetes hipotézisként megfogalmazható, hogy ezek rész-egész viszonyban (is) vannak egymással, vagyis egy informatikai rendszer részét képezi egy informatikai infrastruktúra

[7] Az alhálózat-részhálózat fogalmak megkülönböztetése többféle kritérium alapján is lehetséges, amelyek közül az egyik szerint alhálózatról funkcionális szempontok szerinti elkülönítés (összetartozás) esetén beszélhetünk.

(amely egyben lehet a rendszer határait meghaladó átfogó infrastruktúra része is) és az informatikai infrastruktúra részét (vagy egészét?) képezi egy informatikai hálózat.

Kiemelésre fontos, hogy a fenti megállapításokat érdeklődési körünknek megfelelően a továbbiakban már az információs tevékenységekhez kapcsolódó hálózatokra szűkítve célszerű meggondolni, mivel ezek a kérdések eltérő módon jelentkeznek, vagy részben nem is értelmezhetőek más hálózat-fogalmak esetében. Infrastruktúráról például gyakorlatilag csak a technikai szféra hálózatai esetében van értelme beszélni. Más területeken pedig a rendszer és hálózat fogalmak szinte szinonimaként használatosak, tartalmi megkülönböztetésükre kevés lehetőség van.

FELHASZNÁLT IRODALOM

[1] BARABÁSI Albert-László: A hálózatok tudománya: a társadalomtól a webig. – *Magyar Tudomány*, 2006/11. (1298-1308. o.)

[2] *Network Science*. (by Committee on Network Science for Future Army Applications, National Research Council) – National Academies Press, Washington, 2005

[3] MUNK Sándor: A kommunikáció fogalomrendszerének keretei, az integrálódó információs technológiák korában. – *Kommunikáció 2009 konferencia kiadványa, 2009.10.14.*, Budapest, ZMNE (51-64.o.)

[4] *A magyar nyelv értelmező szótára. Harmadik kötet, H-Kh.* – Akadémiai Kiadó, Budapest, 1965.

[5] *Magyar Nagylexikon. Kilencedik kötet, Gyer-Iq*. – Magyar Nagylexikon Kiadó, Budapest, 1999.

[6] *Új Magyar Lexikon. III. kötet, G-J.* – Akadémiai Kiadó, Budapest, 1960.

[7] *Révai Nagy Lexikona. IX. kötet, Gréc-Herold.* – Révai testvérek Irodalmi Intézet Rt., Budapest, 1913.

[8] *Új Idők Lexikona. Tizenkettedik kötet, Gyalóka-Herczegh.* – Singer és Wolfner Irodalmi Intézet Rt., Budapest, 1938.

[9] *Webster's Encyclopedic Unabridged Dictionary of the English Language.* – Gramercy Books, New York/Avanel, 1996.

[10] Oxford Dictionaries Online. – Oxford University Press, 2010.

[www.oxforddictionaries.com, 2010.09.13.]

[11] ALBERTS, David S. – GARSTKA, John J. – STEIN, Frederick P.: *Network Centric Warfare. Developing and Leveraging Information Superiority. (2nd Edition)*. – CCRP Publication Series., 2000

[12] *NNEC Best Practices Handbook.* – Command and Control Centre of Excellence, 2009

[13] BANG-JENSEN, Jorgen – GUTIN, Gregory: *Digraphs: Theory, Algorithms, and Applications.* – Springer Verlag, 2007

[14] AHUJA, Ravindra K. – MAGNANTI, Thomas L. – ORLIN, James B.: *Network Flows.* – MIT Sloan School of Management, Cambridge, 1988

[15] NAGY József: *Rendszertudományok, rendszerkutatás*. – Zrínyi Miklós Katonai Akadémia, Budapest, 1978.

[16] NEWMAN, Mark E. J.: The structure and function of complex networks. – *SIAM Review*, 2003/2. (167-256.o.)

[17] KERTÉSZ János-VICSEK Tamás: Komplex hálózatok a természetben és a társadalomban. – *Magyar Tudomány*, 2006/5. (558-564. o.)

[18] CHALMERS, David J.: Az emergencia változatai. – *Világosság*, 2003/3-4. (43-51.o.)

[19] BOCCALETTI, S. – LATORA, V. – MORENO, Y. – CHAVEZ, M. – HWANG, D-U.: Complex networks: Structure and Dynamics. – *Physics Reports*, 2006/4-5. (175-308. o.)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Sándor Miklós
sandor.miklos@zmne.hu

Kuris Zoltán
zoltan.kuris@bm.gov.hu

A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA VÉDELEM ÉS A VÉDELMI CÉLÚ KATASZTRÓFAVÉDELMI HÍRADÁS KAPCSOLATRENDSZERE

Absztrakt

Az információs társadalom működésének zavarai, katasztrófavédelmi és különböző minősített helyzet kialakulásához vezethetnek. A szerzők a társadalmi szintű megközelítést követően, részleteiben fejtik ki a kritikus információs infrastruktúra működési zavarainak hatásait a létfontosságú infrastruktúrákra. Bizonyítani szeretnék, hogy a kialakuló katasztrófavédelmi és egyéb minősített helyzetekben, különösen fontos és nélkülözhetetlen az infokommunikációs rendszerek megbízható működésére alapozott katasztrófavédelmi híradás zavarmentes üzemelése. Az információs stabilitás fogalmának bevezetésén keresztül mutatják be a rendszerközpontú működtetés alapvető irányelveit.

A catastrophe might emerge from the disorders of the informational society. The social effects are analyzed. Then the disorders of the critical infrastructure of information is described in detail, how they affect the infrastructures of vital importance the authors describe it in detail. The significance and functioning of sending news are proved as well as the significance of notifying news.

Kulcsszavak: *kritikus információs infrastruktúra védelem, minősített adat, fizikai biztonság, elektronikai biztonság, dokumentum biztonság, személyi biztonság ~ critical information infrastructure protection, sensitive data, physical security, electronic security, document security, personal safety*

BEVEZETÉS

Ma már alapvető axiómának tekinthető az, hogy a biztonság újkori értelmezésének megfelelően, a biztonság dimenzióinak rendszere – az elemek közötti kapcsolatrendszer – alapvetően átalakult. Bizonyos biztonsági dimenziók felértékelődtek, más dimenziók pedig veszítettek súlyukból. Különösen igaz ez, amikor az utóbbi évtized változásait, az információs társadalom működésének tükrében vizsgáljuk. Ma a modern társadalmak nagy része felismerte annak jelentőségét, hogy a társadalom zavartalan működését biztosító „létfontosságú infrastruktúrák" működtetése alapvető biztonságpolitikai cél. Ennek megfelelően a modern társadalmak, a biztonsági stratégiájuk megfogalmazásakor különös figyelmet tanúsítanak az újkori kihívások, kockázatok és fenyegetések részletes feltárására. Az információs társadalmi formációban működő államoknak különös figyelemmel kell lenniük tehát a létfontosságú infrastruktúráik és információs infrastruktúráik védelmére, mert a védelmi rendszer egyenszilárdságának csökkenése alapvetően képes befolyásolni az adott ország geopolitikai és geostratégiai helyzetét egyaránt. A biztonsági stratégia a társadalom működésének biztosítására irányuló alapvető dokumentum. A hazai biztonsági stratégiát elemezve megállapítható, hogy hazánk a fent említett új kori követelményrendszerre építkező, megfelelő biztonsági stratégiával rendelkezik. Ha tovább vizsgáljuk az ágazati stratégiák rendszerét, megállapítható hogy igen ritka a pragmatikus, rendszerszemlélettel rendelkező ágazati stratégia.

Az általános biztonságpolitikai szemléletű megközelítést követően célszerű megvizsgálni azt, hogy a létfontosságú infrastruktúrák zavartalan működtetését célzó kritikus infrastruktúra védelem (a továbbiakban: KIV) milyen kapcsolatban van a katasztrófavédelmi területtel, illetve milyen szerepe van ezen a területen a kritikus információs infrastruktúrák (a továbbiakban KII) zavarmentes üzemeltetésének. Érdemes azt is vizsgálni, hogy ezen a területen hogyan valósul meg, vagy milyen igény mutatkozik a vezetési-irányítási, távközlési és informatikai, rendszerek komplex rendszerének alkalmazásának. Elfogadható állítás az, hogy a társadalom információs és infokommunikációs rendszereinek rendelkezésre állása ugrásszerűen felértékelődik, katasztrófavédelmi és a minősített időszak helyzetében. Célszerű tehát azt vizsgálni, hogy milyen jogalkotási, szabályozási és technológiai feladatok körvonalazódnak ezen a területen. A fentiekből következik, hogy azt is célszerű megvizsgálni, hogy a fentiekben kifejtett vezetés-irányítási, távközlési és informatikai rendszerek, milyen előfeltételekkel és környezetben tudják biztosítani azt az információs stabilitást, bonyolult katasztrófavédelmi és minősített helyzetben.

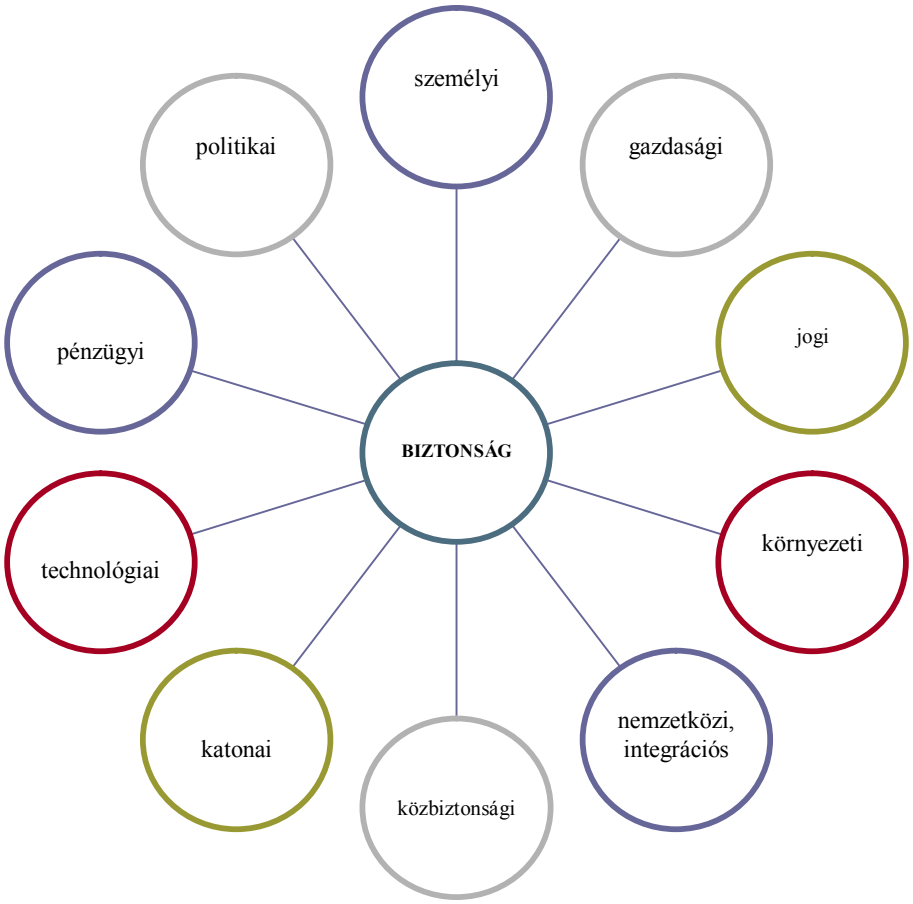
A BIZTONSÁG ÚJKORI DIMENZIÓI

A biztonságot az államok manapság komplex módon értelmezik. Az elemek fontossági sorrendben: a politikai, gazdasági szociális ökológiai és katonai területek. Természetesen ez béke állapotra jellemző fontossági sorrend és az adott körülményeknek megfelelően a súlypontok áthelyeződhetnek. A fenti elemeket megvizsgálva következtetés eredménye ként megállapítható, hogy a fenti elemek megjelenésének színterei a különböző létfontosságú infrastruktúrák és ezen belül a kiemelt fontosságú szektorok.

Ahhoz, hogy a biztonság hatókörét értelmezni tudjuk meg kell határozni a tartalmát. Ezzel összefüggésben a **biztonság szintjei**, *az egyének, csoportok, kisebbségek, nemzetek, államok, régiók és a nemzetközi rendszer.*

Ugyanakkor a 90'-es évektől elterjedt a biztonság fogalmának parttalan használata, kiterjedt azon jelenségek köre, amelyek kiváltói lehetnek a már elemzett biztonsági

hiányérzetnek. Ezért szükséges és elégséges értelmezés szerint az alábbi biztonsági dimenziók körvonalazódnak.



1. ábra. Jellemző biztonsági változatok (szerzők)

A társadalom biztonsági érzete összességében mérhető jelenség. E mérés és a biztonsági érzetek meghatározására hívták segítségül a biztonságpolitikával foglalkozó szakemberek a szociológia eszköztárát. A TIT HABE[1] (a honvédelmi tárca megbízásából) a Szonda Ipsos-sal közösen két ízben is végzett közvélemény-kutatást e terület vonatkozásában. 1999-ben ezer, míg 2008-ban háromezer főt kérdeztek meg „az utca emberei közül". A következő táblázat ennek rövid összefoglalását szemlélteti.

[1] A TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesületet életünk legfontosabb kérdéseivel, a biztonsággal és biztonságpolitikával foglalkozik az ország egész területén. A TIT HABE 1996-os megalakulása óta aktívan részt vesz az ország kül-és biztonságpolitikájával, NATO- és EU-tagságával és a nemzetközi biztonság erősítése érdekében végzett egyéb tevékenységével összefüggő kérdések elemzésében és publikálásában, hazai és nemzetközi rendezvények szervezésében, a lakosság különböző célcsoportjainak a tájékoztatásában és felkészítésében.

***2.* ábra.** (Forrás: Gondolatok és vélemények a biztonságunkról – a biztonságkultúra kérdései, TIT HABE, 2008)[2]

A biztonság a fejlődés előfeltétele

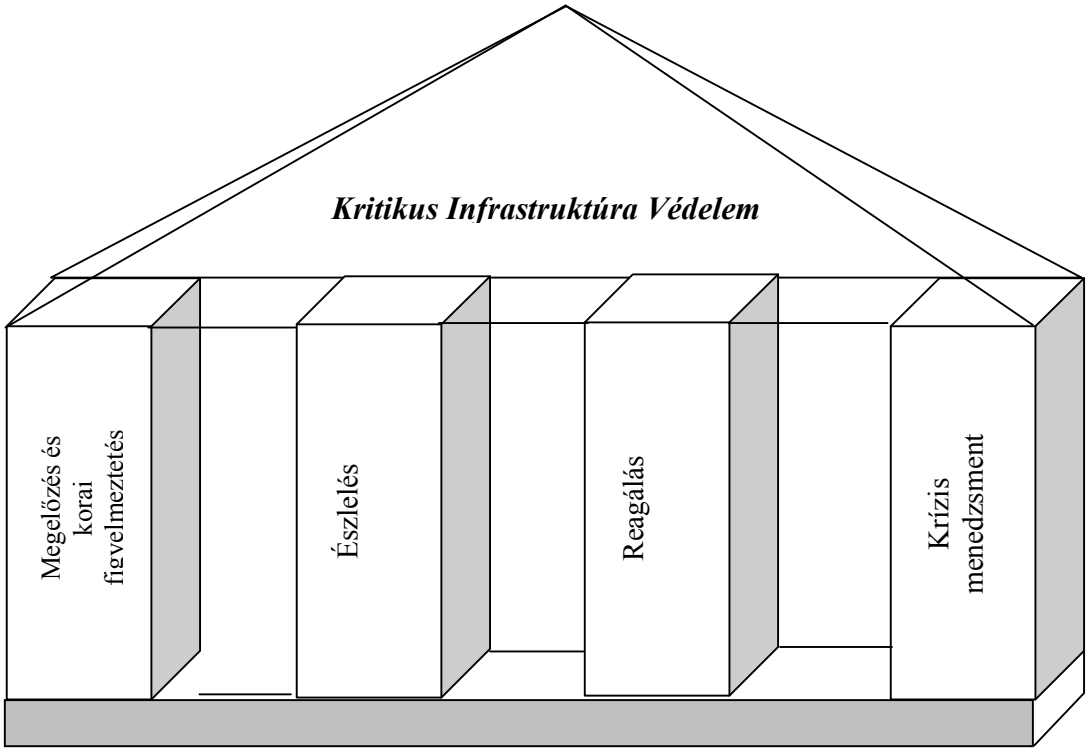
A konfliktusok nemcsak az infrastruktúrákat – így a szociális infrastruktúrákat – teszik tönkre, hanem ösztönzik a bűnözést, eltántorítják a befektetőket és lehetetlenné teszik valamennyi szokásos gazdasági tevékenység gyakorlását is. Számos ország és régió a konfliktus–bizonytalanság–szegénység ördögi körének a foglya.

A fenti rövid áttekintés jól példázza, hogy a társadalom működését biztosító infrastruktúrák működésében előforduló zavarok visszahatnak a társadalom biztonsági érzetére és alapvető hatással vannak a társalmi fejlődésre is!

A kritikus infrastruktúra védelmének négy alappillérét (3. ábra) értelmezve megállapítható, hogy a megelőzéstől a krízis menedzseléséig terjedő teljes vertikumban alkalmazásra kerülnek a különböző kritikus információs infrastruktúra elemek,(kommunikációs, infokommunikációs rendszerek).

Sok Európai Uniós tagállamban – köztük Magyarországon is – találkozunk kormányzati CERT–el, melynek feladata az állami információs rendszerek elleni támadásokra történő reagálás. A CERT-ek fontosságát alátámasztja az is, hogy irányadó szakemberek szerint a kritikus információs infrastruktúrák védelmének megvalósítása is a megelőzés és korai észlelés, valamint a reagálás és a krízismenedzsment négy pillérén kell hogy alapuljon.

[2] Dr. Radványi Lajos szociológus, biztonságpolitikai szakértő, a TIT Hadtudományi és Biztonságpolitikai Közhasznú Egyesület alelnöke *„A magyar lakosság biztonságfelfogásának változásai 1999 – 2008”* című előadásából. Veszélyhelyzetek kezelésének kormányzati koordinációja – munkaműhely, Göd, 2009. március 10.



3. ábra. A kritikus infrastruktúra védelem négy alappillére

Egy az amerikai kongresszus számára készült jelentés megállapítja, hogy a kritikus infrastruktúra besorolások nem olyan listák, amelyek örök érvényűek, és amelyeken nem lehetne változtatni attól függően, hogy milyen veszély fenyeget, illetve ezek milyen hatásokkal járnának a különböző szektorok vonatkozásában. [14]

A tanulmány táblázatban (4.. táblázat) foglalja össze azokat a szektorokat, amelyek a meghatározott kritériumok alapján kritikus infrastruktúrának minősülhetnek.

Infrastruktúra	**Kritériumok, amelyek meghatározzák a kritikusságot**			
	nemzetvédelem	***gazdasági***	***biztonság***	***közegészségügy***
telekommunikációs és információs hálózatok	***X***	***X***		
energia	***X***	***X***		
bank/pénzügy		***X***		
szállítás	***X***	***X***		
víz			***X***	
készenléti szervek			***X***	
kormányzat			***X***	
egészségügyi szolgáltatások			***X***	
nemzetvédelem	***X***			
külföldi hírszerzés	***X***			
igazságügy			***X***	
külügyi kapcsolatok	***X***			
nukleáris létesítmények és erőművek			***X***	
különleges események				***X***
élelmiszer/mezőgazdaság			***X***	
	nemzetvédelem	***gazdasági***	***biztonság***	***közegészségügy***

ipari gyártás		***X***		
vegyipar			***X***	
védelmi ipar	***X***			
Postai szolgáltatások			***X***	
nemzeti emlékművek és emlékhelyek				***X***

4. ábra. Szektorok értékelése és besorolása

AZ INFOKOMMUNIKÁCIÓS RENDSZEREK INFORMÁCIÓBIZTONSÁGI STABILITÁSÁT BIZTOSÍTÓ ÖSSZETEVŐINEK ELEMZÉSE

Az információs társadalom nagyon fejlett és hatékony társadalom, ugyanakkor meglehetősen sebezhető is. Sebezhetőségének alapját az adja, hogy működése szorosan kapcsolódik a globális, nemzeti, regionális és lokális információs környezethez [h 67.old.] Irányadó szakemberek szerint, napjainkban várhatóan felértékelődik az információs környezet átfogó védelme. A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (IV.15.) Korm. határozat [3] a fenyegetések, kockázatok, kihívások szakaszában (II.) nevesíti az információs társadalom kihívásait, ezen belül a telekommunikációs hálózatok sebezhetőségét és kockázatait emeli ki. A terrorizmus elleni védekezés szakaszban (III.3.1) külön kiemeli a kritikus infrastruktúrák védelmének feladatait is. Az információs rendszerek védelme szakaszban (III.3.7) pedig hangsúlyozza a kormányzati információs rendszerek védelmének szükségességét és felhívja a figyelmet a sikeres védelem érdekében szükséges együttműködésre, az érintett informatikai és távközlési szolgáltatókkal. Sajnos a Magyar Köztársság Nemzeti Biztonsági Stratégiájával összefüggő ágazati (távközlés, informatika) területét fellelő gyűjtő néven infokommunikációs doktrínának [8] nevezhető dokumentum a mai napig nem került kidolgozásra.

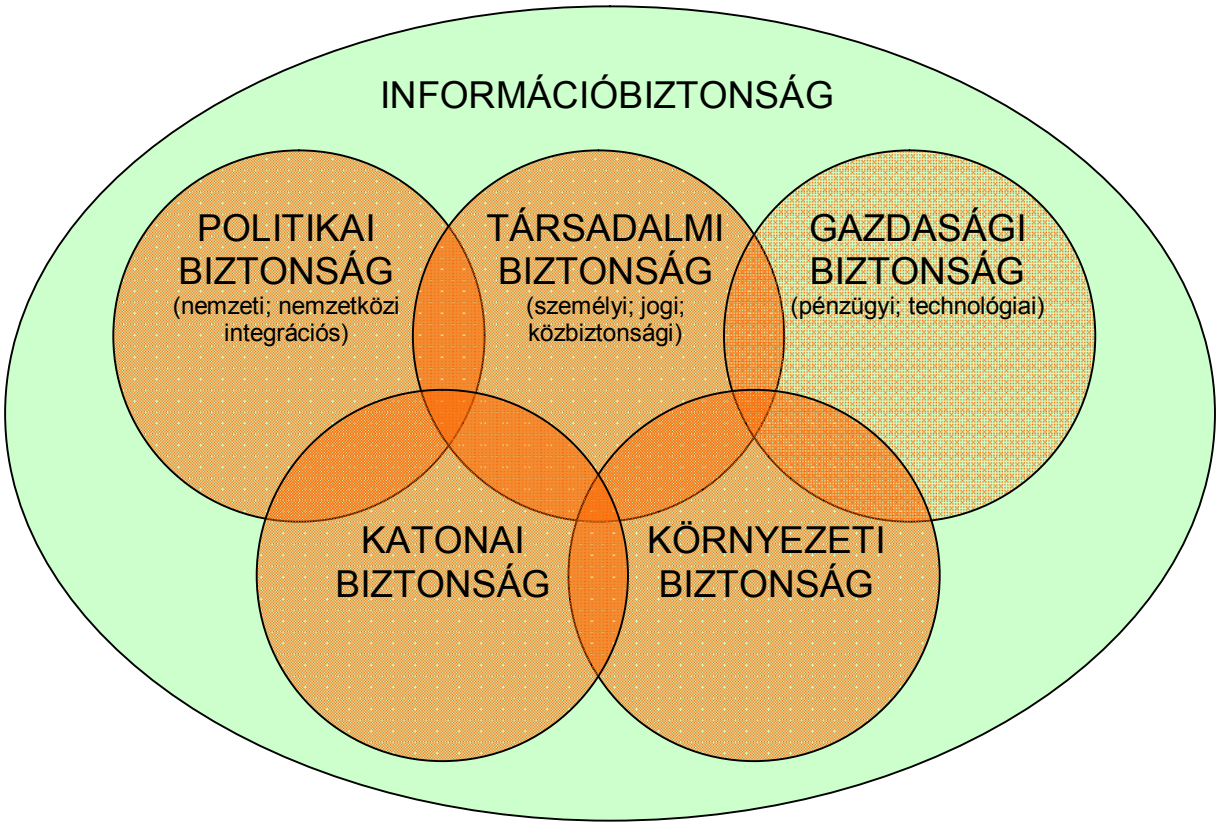
A Magyar Köztársaság kritikus információs infrastruktúrái az alábbiak:
- Informatikai rendszerek és hálózatok,
- automatizálási, vezérlési és ellenőrzési (SCADA, távmérő, távérzékelő és telemetriai) rendszerek,
- internet szolgáltatás és infrastruktúrája,
- vezetékes távközlési szolgáltatások és infrastruktúrái,
- mobil távközlési szolgáltatások és infrastruktúrái,
- műholdas távközlési szolgáltatás és infrastruktúrái,
- földfelszíni műsorszórás és infrastruktúrája,
- közigazgatási informatika és kommunikáció és infrastruktúrái,
- a kritikus infrastruktúrák létfontosságú infokommunikációs rendszerei.

A biztonság dimenzióiban értelmezett információbiztonsággal összefüggésben megállapítható, hogy a KIV szektoraiban gyűjtött, feldolgozott tárolt és továbbított információkat a különféle infokommunikációs eszközök alkalmazásával kezeljük. Infokommunikációs eszközök gyűjtőfogalom kőré csoportosíthatóak, az informatikai és a távközlés, illetve az egyéb információtechnológiai eszközök konvergenciájának következményeként alkalmazott „informatizálódott” eszközök. A fenti infokommunikációs rendszerek információbiztonsági stabilitásának biztosítása alapfeltétel, a katasztrófavédelmi

és egyéb minősített időszaki helyzetekben is. Az előző gondolatot tovább fűzve megállapítható, hogy a kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftverek, internet, GPS,stb.) [8]

A kritikus információs infrastruktúrák védelme tehát a tulajdonosok, gyártók, és felhasználók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani a kritikus információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat. [8] Az információs stabilitás elérésének érdekében komplex információbiztonsági elveket kell alkalmazni. Ezeket a komplex és integrált védelmi intézkedéseket tudati, információs és fizikai dimenziókban is érvényesíteni kell a kritikus információk védelmének érdekében. Ezzel összefüggésben elmondható, hogy ezen a területen a minősített adat védelméről szóló 2009. évi CLV. Törvény (a továbbiakban: MAV törvény) már egységes irányelveket szab.

A MAV törvény nyomán, a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet, és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet, viszont már egységes alapokra helyezi a minősített adatok védelme érdekében érvényesítendő, személyi, fizikai, dokumentum és elektronikai védelem komplex rendszerét.[10] Az elektronikai védelmi intézkedések keretei között megjelenik az átvitel út védelme, számítógép (szoftver, hardver és hálózat) védelme. [11] Egységesítésre kerültek a rejtjelzéssel összefüggő követelmények és megjelennek a kompromittáló kisugárzással kapcsolatos alapvető irányelvek. Sajnos a kompromittáló kisugárzás védelmének részletes szabályozását illetően megállapítható, hogy a magas színvonalú védelmi intézkedésekkel összefüggő követelményrendszert nem sikerült érvényesíteni. Ennek az is lehet az oka, hogy – ez a viszonylag új és bonyolult terület – a leg költségigényesebb védelmi intézkedések megvalósítását feltételezi és ezen a területen hazai tapasztalatok hiányában a nemzetközi irányelvekre figyelemmel kell kialakítani a hazai szabályozást! Ezen a területen, az irányadó hazai információvédelmi szakemberek bevonásával, további lépések szükségesek ahhoz, hogy az elektronikai védelem területén a maradvány kockázatot optimalizáljuk és növeljük az elektronikai rendszerek egyenszilárdságát. Az viszont egyértelmű eredménye a fenti törvényben és kormányrendeletekben megfogalmazott szabályrendszernek, hogy a minősített adat védelmével összefüggő komplex védelmi intézkedések többé-kevésbé koherensek lettek a nemzetközi szabályokkal, ennek okán az Európai Uniós és a NATO rendszereken belüli információáramlás (bizonyos szintig) egységessé és lehetővé vált.



5. ábra. A biztonsági dimenziók és az információbiztonság kapcsolata.

AZ ORSZÁGOS TÁVKÖZLŐ HÁLÓZAT (OTH) FELHASZNÁLÁSA A VÉDELMI FELADATOKKAL ÖSZEFÜGGÉSBEN

Annak érdekében, hogy a rendszerben keletkezett kritikus információk kellően támogassák a döntési helyzetben lévő felelős vezetőket, az információ továbbítására alkalmas és képes nemzeti Országos kommunikációs távközlési hálózat magas szintű rendelkezésre állását kell biztosítani. Meg kell határozni a szükséges és elégséges szolgáltatás mértékét. Ennek előfeltétele a megfelelő szintű és tartalmú törvényi szabályozás, amely lehetővé teszi ezt a rendelkezésre állást a bonyolult nemzetközi tulajdonosi rendszer esetén is. Különösen fontos abban az esetben jól szabályozni ezt a területet, amikor például a védelmi szektor zártcélú vezeték nélküli kommunikációját biztosító rendszer szolgáltatója egy olyan egyetemes szolgáltató, amely külföldi tulajdonosi rendszerben üzleti alapokon szolgáltat. Ezt a részterületet hivatott szabályozni a Miniszterelnöki Hivatalt vezető miniszter 4/2010. (III. 26.) MeHVM rendelete a védelmi feladatokban részt vevő elektronikus hírközlési szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról.

Az elektronikus hírközlésről szóló 2003. évi C. törvény 182. § (4) bekezdés l) pontjában kapott felhatalmazás alapján a Miniszterelnöki Hivatalt vezető miniszter feladat- és hatásköréről szóló 29/2008. (II. 19.) Korm. rendelet 1. § j) pontjában meghatározott feladatkörében eljárva, a miniszterelnöki hivatalt vezető miniszter az alábbiakat rendelte el [12]:

Az elektronikus hírközlés szolgáltatási tevékenységének a minősített időszakban történő ellátásához szükséges védelmi felkészülési feladatok előkészítésében és végrehajtásában való részvételre kijelölt, valamint az informatikai és elektronikus hírközlési, továbbá postai ágazat (a továbbiakban: ágazat) ügyeleti rendszerébe bevont elektronikus hírközlési tevékenységet

végző szervezetek (a továbbiak ban: szolgáltatók) felsorolását a rendelet 1. melléklete tartalmazza.

A riasztási és tájékoztatási feladat ellátásában részt vevő nem közszolgálati műsort sugárzó országos, körzeti, helyi rádió és televízióadók, az adókat üzemeltetők (engedélyesek) jegyzékét a rendelet 2. melléklete tartalmazza.

A kijelölés alapján a szolgáltatók a tevékenységi körüket érintően ellátják a minősített időszakban bekövetkező rendkívüli események megelőzésére, elhárítására, a következményeik csökkentésére, illetve megszüntetésére, valamint a helyreállításra irányuló védelmi felkészülési és végrehajtási feladatokat.

A rendelet alkalmazásában minősített időszak a Magyar Köztársaság Alkotmányáról szóló 1949. évi XX. törvény 19. §-a (3) bekezdésének h) pontjában meghatározott rendkívüli állapot és i) pontjában meghatározott szükségállapot, az Alkotmány 35. § (1) bekezdésének i) pontja és a polgári védelemről szóló 1996. évi XXXVII. törvény 2. § (2) bekezdése szerinti veszélyhelyzet, valamint az Alkotmány 19. § (3) bekezdés n) pontjában meghatározott megelőző védelmi helyzet, továbbá a 19/E. § (1) bekezdésében foglalt, a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig terjedő időszak.

Az elektronikus hírközlésért felelős miniszter (a továbbiakban: Miniszter), illetve a Nemzeti Hírközlési Hatóság (a továbbiakban: NHH) a védelmi felkészülés és a végrehajtás időszakában felmerülő egyedi védelmi feladatokat az érintett szolgáltatók számára külön jogszabály szerint határozza meg.

A védelmi felkészülési feladatok végrehajtásáért minden esetben a szolgáltató vezető tisztségviselője felelős.

A szolgáltatók – a minősített időszakra történő felkészülés keretében – az alábbiakban meghatározott tevékenységi körökből a saját szervezetük szakmai feladat- és hatáskörébe tartozó védelmi feladatokat látják el:

- a szervezeti készenlét előkészítésének és fenntartásának körében:
  - a védelmi felkészülési feladatok ellátásához szükséges személyi, szervezeti és anyagi-technikai feltételek megteremtése, folyamatos biztosítása,
- a védelmi felkészüléssel, műszaki, forgalmi, katasztrófa vagy egyéb veszély miatt keletkező üzemzavar elhárításával kapcsolatos intézkedések kidolgozása, tervek készítése és azok folyamatos aktualizálása,
  - a védelmi felkészüléssel összefüggő rendszeres képzési, továbbképzési és gyakoroltatási feladatok meghatározása és végrehajtása,
  - az ügyeleti szolgálatnak a külön jogszabályban foglaltak szerinti működtetése,
  - a külön jogszabály alapján a meghagyással kapcsolatos feladatok végrehajtása;
- a hálózatok felkészítésének és irányításának terén:
  - a gerinchálózati struktúra és az elektronikus hírközlési létesítmények védelmi, biztonsági feltételeinek biztosítása,
  - a zártcélú hálózatokhoz szükséges összeköttetések és kapcsolódó szolgáltatások előkészítésének és alkalmazásának biztosítása,
  - a meghatározó szerepű elektronikus hírközlési csomópontok, illetve felhasználók több útvonalon történő elérhetőségét segítő megoldások kialakítása,
  - a riasztási és tájékoztatási feladat ellátására létrehozott rendszerben szükséges elektronikus hírközlési összeköttetések biztosításában való közreműködés,
  - be) a honvédségi, kormányzati, rendvédelmi elektronikus hírközlési eszközöknek a szolgáltató hálózatához történő csatlakoztatásához szükséges hozzáférési pontok és jogosultságok biztosítása;
- az üzemviteli és tartalékolási rendszer kialakítása terén:
  - a nemzeti és a nemzetközi gerinchálózati irányító és üzemviteli funkciók működésének összehangolása,

- az illetékes hazai, valamint nemzetközi szervek és szervezetek közötti védelmi jellegű kapcsolattartás feltételeinek kialakításában és végrehajtásában való közreműködés,
- az elektronikus hírközlési szolgáltatások területén elrendelhető korlátozó vagy szüneteltető rendelkezések végrehajtására és következményeik kezelésére történő felkészülés,
- a védelmi feladatok ellátásához szükséges mértékű és összetételű tartalékkészletek biztosítása,
- a hálózati létesítmények és eszközök meghibásodása, rongálódása, sérülése, megsemmisülése esetére az elsődleges helyreállításhoz és az üzemszerű állapot visszaállításához szükséges feladatok megtervezése és végrehajtási feltételeinek folyamatos biztosítása;

❖ a szolgáltatási igények kielégítése terén:
- a védelmi felkészülésben részt vevő, külön jogszabályban meghatározott követelménytámasztó szervek minősített időszakra vonatkozó szolgáltatási igényeinek kielégítéséhez szükséges feltételek biztosítása, az összefüggő tervezési, szervezési tevékenység ellátása, szolgáltatási feladatok végrehajtása,
- a lakosság minősített időszaki elektronikus hírközlési igényeinek az egyetemes szolgáltatási, illetve koncessziós szerződésben meghatározott szinten és tartalommal történő kielégítéséhez szükséges feltételek biztosítása,
- a védelmi felkészüléssel kapcsolatos jogszabályok által meghatározott gazdasági és anyagi szolgáltatási kötelezettségek teljesítésére, illetve kezelésére való felkészülés,
- da kormányzat minősített időszaki szolgáltatási igényeinek kielégítéséhez és kommunikációs tevékenységéhez szükséges feltételek megteremtésében, fenntartásában való közreműködés,
- a Befogadó Nemzeti Támogatás tervezési és végrehajtási feladataiban történő részvétel;

❖ a nyilvántartások vezetése és az adatkezelés terén:
- a védelmi felkészülési feladatokkal kapcsolatos jogszabályokban meghatározott adatszolgáltatási kötelezettség teljesítéséhez szükséges nyilvántartási rendszer kialakítása és adatainak a követelményekhez igazodó pontosságú karbantartása;

❖ a műsorszórási tevékenység körében:
- a műsorszórási tevékenység folyamatosságához szükséges technikai és biztonsági feltételek megteremtése, a meghatározó szerepű létesítmények őrzés-védelmének biztosítása,
- a műsorszóró hálózaton a lakosság légi-, illetve katasztrófariasztásra és tájékoztatására létrehozott rendszer működésében való közreműködés,
- a lakosság légi-, illetve katasztrófariasztásának és tájékoztatásának elrendelésére illetékes szervek intézkedésére a riasztási és tájékoztatási közlemények leadásának – az elrendelő szervekkel kötött megállapodás szerinti, saját eszközökkel történő – biztosítása.

A riasztási és tájékoztatási feladat ellátásában külön jogszabály alapján – az illetékes honvédelmi és rendvédelmi szervek, valamint a közszolgálati rádió és televízió műsorszolgáltatók, műsorszóró adók és az adókat üzemeltető szolgáltatók mellett – részt vesznek:

❖ a Miniszter és az NHH;
❖ a rendelet 2. mellékletében meghatározott nem közszolgálati országos, körzeti és helyi rádió és televízió műsorokat sugárzó adók, az adókat üzemeltetők (engedélyesek);
❖ azok az elektronikus hírközlési szolgáltatók, amelyek összeköttetést, illetőleg modulációs vonalat biztosítanak

- a riasztási és tájékoztatási közlemény leadását kezdeményező szerv és az érintett rádió, televízió stúdiója között,
- a riasztási és tájékoztatási feladatban részt vevő stúdió és a részére sugárzást végző rádió, televízió adóállomás között, valamint
- a műsorszolgáltatók és a műsorszóró adók között;

❖ a riasztási rendszer technikai elemeit, a riasztási és tájékoztatási közlemények átvételére és továbbítására szolgáló átkapcsoló berendezések fenntartását ellátó gazdálkodó szervezet;

AZ EURÓPAI UNIÓ LÉTFONTOSSÁGÚ INFRASTRUKTÚRÁK FIGYELMEZTETŐ ÉS INFORMÁCIÓS HÁLÓZATA (CIWIN)

Vezetés irányítási rendszerek alapvető megközelítése

Az információbiztonsági stabilitást alapvetően befolyásoló OTH, magas szintű rendelkezésre állása és a minősített adatok védelmével összefüggő részterülteken túl, az alábbiakban célszerű megvizsgálni a globális, nemzetközi, nemzeti és regionális infokommunikációs rendszerekre épülő vezetés-irányítási rendszerekkel összefüggő alapvető ismereteket és követelményeket. Ennek nyomán célszerű áttekinteni - egy a kritikus infrastruktúra védelmével összefüggő- adattovábbítási értesítési és riasztási rendszerrel szembeni alapvető igényeket is. Különösen indokolt ez, annak fényében, hogy az összekapcsolódó (adott esetben globális) infrastruktúrákon keresztül – az incidens bekövetkezését követően- a működési zavarok felhalmozódnak, hatványozódnak az interdependencia jelenség miatt. Ebben a helyzetben indokolt egy nemzetközi (európai) adatok cseréjére alkalmas megosztott figyelmeztető és tájékoztató rendszer alkalmazása, amelynek segítségével a döntéshozók, az egységes és valós idejű adatok alapján rövid idő alatt a helyzettel összefüggő széleskörű adatszolgáltatás alapján képesek meghozni az optimális döntéseket. Az információs társadalomban alapvető igény fogalmazódik meg az infokommunikációs eszközökre épülő valós idejű globális döntés támogató rendszerek üzemeltetésére. Ezzel összefüggően megállapítható, hogy a kritikus infrastruktúra védelem területén is alapvető igény az információs fölény birtoklása, annak érdekében, hogy a fenyegetések előrejelzése, majd annak realizálódását követően a kár elhárítás és a működőképesség helyreállításának időszakában is optimális szinten tartható legyen a szükséges és elégséges szintű védelmi intézkedések alkalmazása.

A CIWIN kezdeményezés

A CIWIN létrehozására irányuló kezdeményezések már 2006 decemberére nyúlnak vissza. A létfontosságú infrastruktúra védelem Európai Programja (EPCIP) javaslatok célkitűzések értelmében fogalmazódott meg egy az infrastruktúra védelemmel összefüggő, biztonságos információcserére alkalmas eljárás kidolgozása. Ez a kezdeti lépés alapozta meg egy tagállamok közötti kölcsönös tájékoztató rendszer létrejöttét, illetve fogalmazta meg annak igényét. Erről az Európai Bizottság határozatban is gondoskodott ugyan, de a tagállamok CIWIN- hez történő csatlakozása nem kötelező. Ugyanakkor az EPCIP-vel kapcsolatos irányelveknek megfelelően a tagállamoknak az Európai Bizottság részéről rendelkezésre bocsátott információkat hozzáférhetővé kell tenniük a kijelölt ágazatok részére. A tagállamoknak viszont a saját területéről gyűjtenie kell az adatokat az európai létfontosságú infrastruktúrákról, a sebezhetőségi és függőségi pontjairól, a védelmi fejlesztésekről és ezt elérhetővé kell tenni az EU részére.

A CIWIN (szerver / kliens) rendszer funkcionalitását illetően, a Bizottság és a tagállamok közötti viszonylatban alkalmasnak kell lennie a két vagy többoldalú információ megosztásra,

illetve gyors riasztási funkció megvalósítására. A bizottsági felületen az ágazati területek jelennek meg. A rendszer kötött és dinamikus területi adatkezelésre egyaránt alkalmas.

A kötött területen jelennek meg a tagállami, szektor, vezetői, külső együttműködési területek és egy gyors információcserét biztosító RAS alrendszer.

Egy speciális esemény, vagy tagállami projektek, szakértői munkacsoport terület részésze, igény szerint dinamikus területek hozhatók létre.

Az elrendelt figyelmeztetés esetén lehetőség van egy ideiglenes RAS terület létrehozására, amely az együttműködés színtere az adott projektre vonatkozóan.

A kritikus infrastruktúra védelmével összefüggő és rejtelzéssel védeni rendelt, minősített információk megosztására speciális terület áll rendelkezésre azok számára, akik a „muszáj tudni" elv alapján azokhoz jogosultak hozzáférni.

A CIWIN rendszer (MS SharePoint 2007), piaci alkalmazásra épül és beépített, minden nyelvre automatikus fordítóprogramot, illetve „off the shelf" tartalomkezelőt használ. Funkcióit illetően megtalálhatóak benne a vitafórum, kalendárium, és a személyes belső levelező funkciók is.

A TESTA rendszeren történő elérést megelőzően, minősített információk továbbítására nem alkalmas. Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de középtávon - sTESTA hálózaton - Bizalmas minősítésű információk megosztására lesz alkalmas.

A TESTA (Trans European Services for Telematics between Administrations) egy független zártcélú (publikus hálózatoktól független) gerinchálózat, amely az Európai Unió adminisztrációja és a tagállamok közötti kommunikációs hálózat. A TESTA rendszer, információvédelmi szempontból továbbfejlesztett változata az sTESTA, amely már megfelelő egyenszilárdságú rejtjelző eszközöket és algoritmusokat használ. A tagállamok részére a CIWIN rendszerre történő csatlakozás opcionális, azonban a rendszerhez csatlakozó tagállamoknak a minősített adatkezeléssel összefüggő kötelezettség alapján az elektronikai, dokumentum, személyi és fizikai védelmi követelményeknek meg kell felelni. Az előzőekben már kifejtett EU minősített adatvédelmi követelményekkel koherens szabályozási rendszer, különösen ezen a területen nyit új távlatokat, melyeket az Európai Bizottság, a tagállamokkal kötött többoldalú szerződésekkel is megalapozott.

Az elérést követően korlátozott terjesztésű minősített adatok továbbítására alkalmas, de középtávon Bizalmas minősítésű információk megosztására lesz alkalmas.

Információvédelmi kérdések

Az Európai Bizottság által kiadott irányelv 9. cikkelyében megfogalmazottaknak megfelelően., a minősített információt kezelő személyeknek, személyi biztonsági tanúsítvánnyal kell rendelkezniük. Ennek előfeltétele a megfelelő szintű nemzetbiztonsági átvizsgálást követő kockázatmentesség megállapítása. A tagállamoknak, a Bizottságnak és az illetékes felügyeleti szerveknek (ez hazánkban a Nemzeti Biztonsági Felügyelet) biztosítaniuk kell, hogy a minősített információkhoz a létfontosságú infrastruktúrák védelme céljából jussanak hozzá, az arra jogosult személyek. Ezzel összefüggésben elengedhetetlen a nemzeti és nemzetközi jog harmonizációja (ez meg is történt) valamint az egységes jogértelmezésen alapuló jogkövető magatartás érvényesítése. Az egyes tagállamoknak és a bizottságnak egyaránt tiszteletben kell tartania a minősített adat minősítője által megállapított minősítési szintet.

A CIWIN rendszer információs funkciója biztosítja, hogy az adathoz való hozzáférés alapja a már említett"tudnia kell" elv alkalmazása. A rendszeren belül az információ birtokosa dönti el azt, hogy ki és milyen biztonsági szinten férhet hozzá az adathoz. A tagállamok jogosultsága és felelőssége az, hogy tagállamon belül hogyan szabályozzák a hozzáférést az adathoz. Természetesen itt vissza kell utalni a koherens EU és nemzeti szabályokra, melynek

rendelkezéseit maradéktalanul be kell tartani. A tagállamnak minden alkalommal ki kell jelölnie egy arra jogosult vezetőt, aki a jogosultságokat illetően dönteni tud. Ez az egyszemélyi vezető jogosult ezeket a jogokat – korlátozott mértékben- a tagállam más tisztségviselőjére delegálni. A szabályoknak megfelelő szintű személyi biztonsági tanúsítványokkal a kezelőknek és felhasználóknak egyaránt rendelkezniük kell.

Hazai rendszerek együttműködése a CIWIN rendszerrel

A nemzeti KIV hatókörében, az irányadó szakemberek szerint nem szükséges külön riasztási és értesítési rendszereket létrehozni. Azt azonban célszerű elemezni, hogy a jelenleg működő riasztási és értesítési rendszerek, hogyan tudják támogatni a nemzeti KIV-ben érintett szektorok és az állami szektor döntésképes vezetőit. Ha a vizsgálat eredménye ként erre a jelenlegi rendszerek nem alkalmasak, akkor (és csak is akkor) szükséges új, különálló rendszerek fejlesztésében gondolkodni. Ugyanakkor védelmi vezetéstechnikai rendszerszervezési szempontokat figyelembe véve, nem indokolt sok sziget rendszerű riasztási rendszert üzemeltetni. Célszerű a jövőben megvizsgálni annak a lehetőségét is, hogy a meglévő nemzeti rendszereket (Marathon Terra; K-600/KTIR) illetve azok bizonyos adatbázisait (amelyek nem sértenek nemzeti érdekeket) egy funkcionális interfészen keresztül, hogyan lehet elérhetővé tenni a CIWIN számára, egységes és redundáns platformra helyezve ezzel a nemzeti és európai KIV figyelmeztető és információs rendszereit.

ÖSSZEFOGLALÁS

A biztonság újkori értelmezéséből kiindulva - elfogadva azt, hogy a dimenziók átalakultak és némely dimenziók felértékelődtek – megállapítható, hogy az információs társadalom kritikus infrastruktúrának és ezen belül a kritikus információs infrastruktúra védelmével összefüggő kérdések a biztonsági stratégiába épülő és annak szerves részét képező elemei. Megállapítható, hogy a társadalom zavartalan működésén túl, a katasztrófa helyzetben és a különböző minősített időszaki helyzetekben súlyponti kérdés a kritikus információs infrastruktúrák rendelkezésre állása. Az mára bizonyított tény, hogy az információk gyors, hiteles és változatlan formában történő áramlása alapvetően befolyásolja a védelmi intézkedések hatékonyságát. A fentiekből azt a végkövetkeztetést lehet levonni, hogy ezen a területen is fontos az információs fölény elérése.

A külföldi és hazai jogi és technológiai környezetet elemezve az a végkövetkeztetés vonható le, hogy a hazai szabályozás – a hazai doktrínák rendszerét vizsgálva – ugyan igyekszik követni az európai folyamatokat, de különösen technológiai területen az útkeresés fázisában lévő folyamat érzékelhető. A felhasználók igénye az információs rendszerek használatával kapcsolatban nagyon határozott és jól érzékelhető, de különösen az érzékeny, vagy minősített adatok gyors, hiteles és változatlan továbbítására alkalmas hazai rendszerek kialakítása még várat magára. Ezen a területen több párhuzamos fejlesztési folyamat érzékelhető. Ezért is különösen fontos annak a problémának a feloldása, hogy a hazai és nemzetközi értesítési rendszerek egységes platformon és egységes elvek alapján képesek legyenek a hatékony együttműködésre. A fentieket összefoglalva, irányadó szakemberek szerint az információs társadalom zavartalan működését veszélyeztető fenyegetésekkel szembeni védelmi intézkedések foganatosítása az információs dimenzióban, meghatározó szerepet töltenek be.

FELHASZNÁLT IRODALOM

[1] Egyesült Nemzetek Nevelésügyi és Kulturális Szervezete (UNESCO) társadalomtudományi szótár

[2] Amerikai nemzetbiztonság c. könyv (1981)

[3] A Magyar Köztársaság nemzeti Biztonsági Stratégiájáról szóló 2073/2004.(IV.15) korm. határozat.

[4] Kőszegvári Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány, Magyar

Hadtudományi Társaság, Budapest XVII. évfolyam 2007/1. szám) 13. oldal

[5] Farkasné dr. Zádeczky Ibolya: A biztonságot veszélyeztető globális kihívások (Hadtudomány, MHTT. Budapest XVI. évfolyam 3. szám, 2006. szeptember) 41. oldal.

[6] Wörterbch zur sicherheitspolitik, Mitter Kiadó, 1985. 113. o.

[7] Szabó József::Hadtudományi Lexikon, Magyar Hadtudományi Társaság, 1995. 144. o.

[8] Muha Lajos A Magyar Köztársaság Kritikus Információs Infrastruktúráinak védelme doktori (Phd) értekezés 2007.

[9] a minősített adat védelméről szóló 2009. évi CLV. Törvény

[10] a Nemzeti Biztonsági felügyelet működésének, valamint a minősítet adat kezelésének rendjéről szóló 90/2010.(III.26.) Kormányrendelet

[11] a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Kormányrendelet

[12] Az elektronikus hírközlésről szóló 2003. évi C. törvény

[13] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf 4. (210. 09.10) 4.oldal

[14] MOTEFF, JOHN– COPELAND, CLAUDIA– FISCHER, JOHN: Report for Congress, Received through the CRS Web, Critical Infrastructures: What Makes an Infrastructure Critical?, January 29, 2003.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Varga Péter
varga.peter@kvk.uni-obuda.hu

A POLGÁRI MŰSORSZÓRÁS, MINT KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA ELEMZÉSE

Absztrakt

A cikk bemutatja a polgári műsorszórás szereplőit, a földfelszíni és a műholdas rendszereket és az IPTV-t. Megvizsgálja annak a lehetőségét, hogy egy-egy műsorszóró működésképtelenné válása esetén az információ továbbítása biztosítható-e a felhasználók számára, ami lehet hang, kép vagy egyéb természetű jel.

The author of this paper introduces the key actors of civil broadcasting, terrestrial transmission systems, satellite systems and IPTV. The paper examines the possibilities information transfer – which can be audio, video or other signals – to the users in case of the failure of individual broadcasters.

Kulcsszavak: *műsorszórás, kritikus infrastruktúra, DVB, IPTV ~ broadcasting, critical infrastructure, DVB, IPTV*

Bevezetés

A kritikus infrastruktúrák védelmére már nem csak a védelmi szektor, hanem a jogalkotók is különös figyelmet fordítanak. 2008. június 30-án a kormány határozott a kritikus infrastruktúra-védelem nemzeti programjának megalkotásáról. A program a következő főbb pontokat tartalmazza:

- Elrendeli a Zöld Könyvben foglaltak alapján ágazati konzultációk lefolytatását a hazai infrastruktúra elemeinek üzemeltetőivel és tulajdonosaival
- Elrendeli a hazai infrastruktúra létfontosságú elemeinek védelméről szóló szabályozási koncepció összeállítását
- Az összeállított szabályozási koncepcióban figyelni kell az infrastruktúra honvédelmi célú felkészítésének és fejlesztésének állami feladataira, valamint a honvédelem szempontjából fontos, kritikus infrastruktúra védelmére vonatkozó követelményeire
- Elrendeli az Európai Unió létfontosságú infrastruktúrák figyelmeztető és információs hálózatához való kapcsolódás lehetőségének vizsgálatról szóló jelentés összeállítását.[1]

A határozat megfogalmazza azokat a főbb ágazatokat és alágazatokat, amelyeket a kormány kritikusnak ítélt a működés szempontjából. A jogszabályban nevesített főbb ágazatok a következők:

- Energia
- Infokommunikációs technológiák
- Közlekedési
- Víz
- Élelmiszer
- Egészségügy
- Pénzügy
- Ipar
- Jogrend – Kormányzat
- Közbiztonság – Védelem.

Ezen ágazatok infrastruktúráinak védelme nem minden esetben egyértelmű. A privatizációs folyamat részeként a szolgáltatói szektor, amely ezen infrastruktúrák nagy részét használja, hetven százalékban a magánszféra tulajdonában van, így kikerült az állami kontroll alól. Ahhoz, hogy a megfelelő védelmi rendszert ki lehessen alakítani fontos az állam és a szolgáltatók közös együttműködése. A szolgáltatók nem várhatják el az államtól saját infrastruktúráik védelmének finanszírozását, viszont az állam sem várhatja el, hogy a szolgáltatók a nyereségüket állami feladatok ellátására fordítsák. Az állam abban partner, amit a határozatban is megfogalmazott, hogy konzultációt hoz össze az infrastruktúrák tulajdonosaival, majd megfogalmazza a védelemről szóló szabályozási koncepciót, és megvizsgálja, hogyan lehet az európai figyelmeztető és információs hálózatához kapcsolni a hazai kritikus infrastruktúrákat.

A polgári műsorszórás a fent említett kormányhatározat infokommunikációs technológiák ágazat egyik eleme. A műsorszórás a társadalom kommunikációs rendszerében különleges és egyre fontosabb szerepet játszik. Ez a típusú szolgáltatás a kommunikációnak az a formája, amely nagyszámú emberhez, tömeghez jut el. Olyan információ közlésére is alkalmas, amely nem csak a hétköznapi „megszokott” adásokra korlátozódik, hanem fontos előrejelző, figyelmeztető funkciót is ellát. Ezért joggal állíthatjuk, hogy a védelem és előrejelzés egyik nagyon fontos eleme.

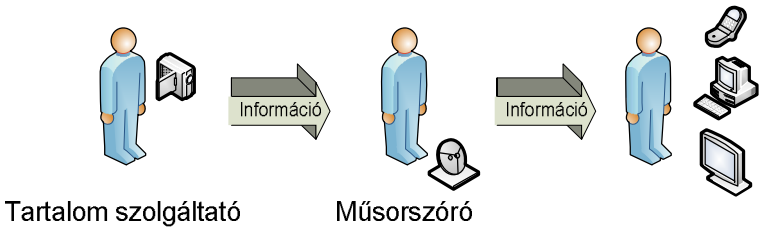
Ez a típusú kommunikáció a következő jegyeket viseli magán:

- a közlemények áramlása egyirányú, a közlő és a befogadó a közlés során sohasem cserél szerepet;
- a közlemények továbbítása a modern hírközlő eszközök útján történik;
- a közlő és a befogadó között térbeli és/vagy időbeli távolság van;
- valamely adott információ sugárzása viszonylag egységesen történik;
- a szétsugárzott közlemények elsősorban társadalmi jelentőségű eseményeket tartalmaznak;
- jellemző a tömeges jelleg, a szó mindkét fentebb említett értelmében. [2]

A cikkben bemutatom a polgári műsorszórás szereplőit - elsősorban a képi műsorszórást -, és megvizsgálom annak a lehetőségét, hogy egy-egy műsorszóró működésképtelenné válása esetén az információ továbbítás biztosítható-e.

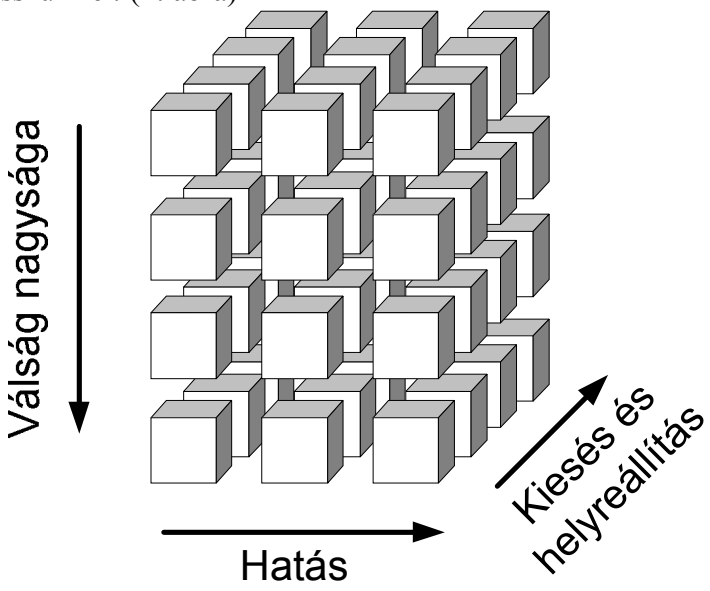
A polgári műsorszórás szereplői

A polgári műsorszóráshoz szervesen kapcsolódik két nagy csoport. Az egyik a tartalom szolgáltatók csoportja – műsorkészítők –, a másik a nézők csoportja. A következő ábra a szereplőket és az információ áramlását mutatja be. (1. ábra)



1. ábra: A műsorszórás szereplői és az információ áramlása (saját szerkesztés)

Ahhoz, hogy a megfelelő információ a megfelelő helyre a megfelelő időben eljusson a tartalomszolgáltatók és a műsorszórók közös együttműködése szükséges. Azt, hogy milyen kockázattal járhat egy esetleges tartalomszolgáltató vagy műsorszóró kiesése azt kockázatelemző modell segítségével lehet meghatározni. A modellalkotásban fel kell sorolni a meglévő erőforrásokat, a fenyegetés lehetőségeit és a kockázati tényezőket. Ahhoz, hogy az elemeket kockázati szempontból tudjuk vizsgálni egy háromdimenziós mátrixot kell alkotni. A mátrix tengelyein a hatást, a kiesés okozta válság nagyságát, és a kiesés és helyreállítás között eltelt időt vesszük fel. (2. ábra)



2. ábra : Kockázati mátrix (saját szerkesztés)

Kategorizálni például a következőképpen lehet a mátrix elemeit:

- *Hatás:* kis, közepes, nagy;
- *Válság nagysága:* kis, közepes, nagy, kritikus;
- *Kiesés és helyreállítás között eltelt idő:* 1 óra, 2 óra, 5 óra…1 nap, 2 nap…x nap

Minden erőforráshoz hozzá lehet rendelni egy-egy kockázati elemet, és el lehet helyezni a mátrixban. Ugyanígy a fenyegetések is paraméterezhetők.

A tartalomszolgáltatók

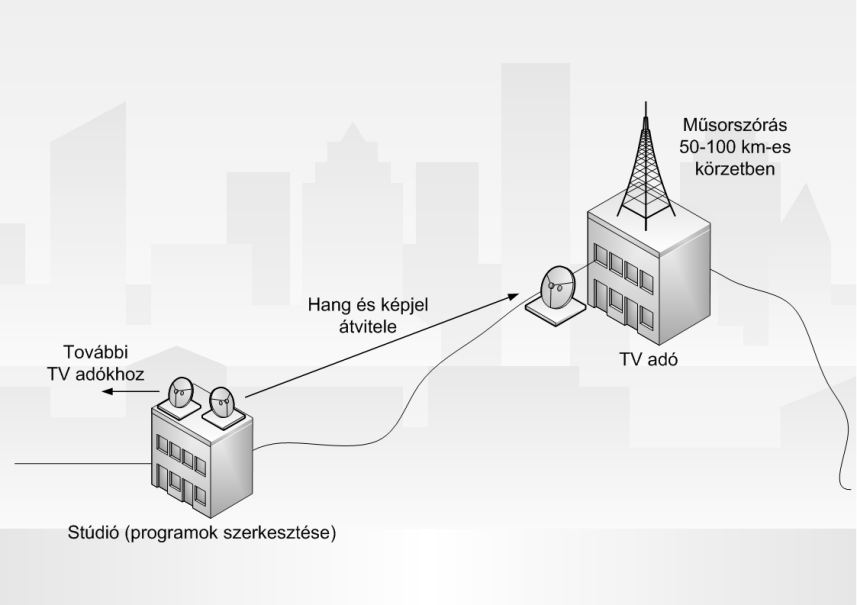
Ma Magyarországon számos tartalomszolgáltató működik. Ezek közül 5 számottevő, és országosan is többnyire elérhető, melyet négy televíziós társaság működtet. Magyarország két közszolgálati csatornája, az m1 és az m2, a Magyar Televízió működtetésében, a Duna Televízió, amely elsősorban a határon túli magyarságnak készíti műsorát, illetve a két országos kereskedelmi televízió, az RTL Klub, és a TV2. Ezen kívül több olyan szolgáltató is működik, amely a műsorszórás egy szűkített keresztmetszetét veszi igénybe. Ezek a

társaságok élő és konzerv anyagok segítségével szerkesztik műsoraikat. Egy esetleges vészhelyzeti információközlés szempontjából megállapítható tehát, hogy egy vagy esetleg több társaság kiesése nem okozna nagy fennakadást a lakosság informálásában.

Műsorszórás

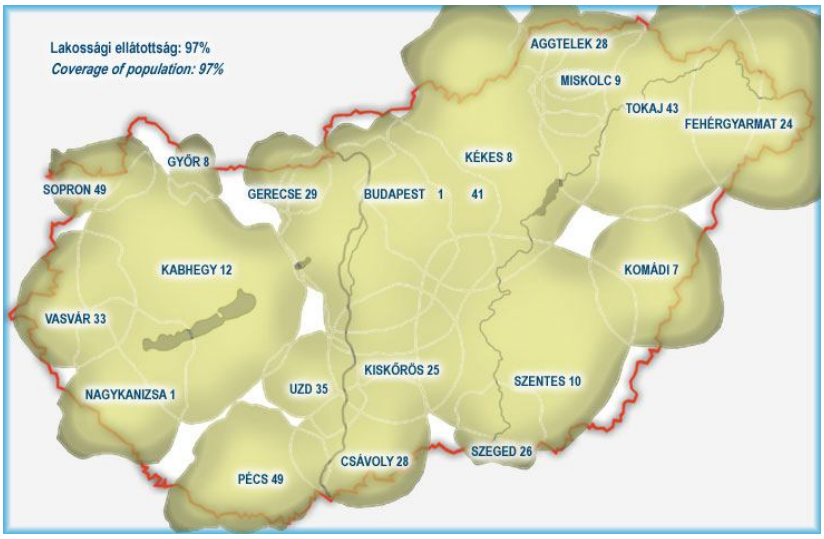
Jelenleg Magyarországon a műsorszórást kizárólagosan az Antenna Hungária Zrt. végzi. A televízióműsor-terjesztéssel kapcsolatos szolgáltatások lényege, hogy a televíziós jeleket a televízióműsor-szolgáltatók stúdióitól eljuttatja a nézőkig. A televízióműsor-szolgáltatók által készített műsorokat földfelszíni, illetve műholdas műsorszóró rendszereken keresztül terjeszti. Ezen kívül analóg, illetve digitális műholdas feladó-szolgáltatásokat is ellát, amellyel kapcsolat hozható létre tévéstúdiók, valamint mobil berendezések, körzeti stúdiók és nemzetközi programforrások között.

A földfelszíni, illetve műholdas műsorszórás között alapvető különbségek vannak. A földfelszíni műsorszórásnál a stúdióból induló program a földi közvetítő állomásokon keresztül (mikrohullámú, pont-pont közötti átjátszók) jut el az adóállomásokhoz. Innen sugározzák az adást 50-100 km-es körzetben és küldik tovább a műsort a többi átjátszóállomásnak. (3. ábra)

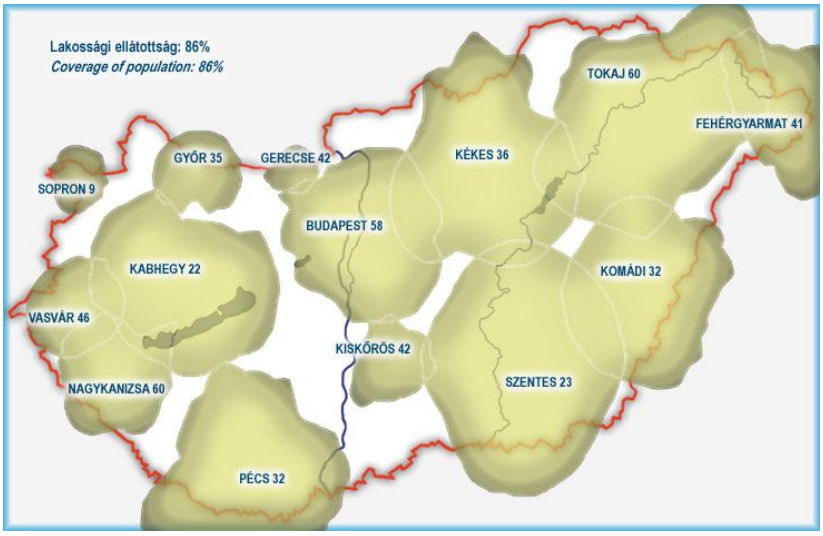


3. ábra: A földfelszíni műsorszórás elvi felépítése (saját szerkesztés)

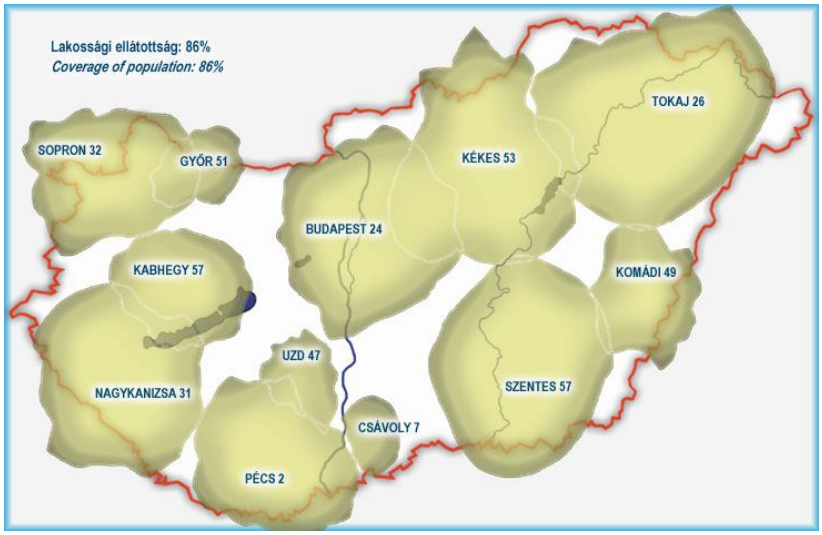
Az adóállomások különböző jelerősséggel sugározzák az adást. A földfelszínen 3 analóg műsor fogható a regionális adókon kívül. Az m1, TV2 és az RTL Klub. Ezen műsorok adási teljesítménye adókörzetenként eltérő, de kijelenthető, hogy nincs olyan lakott terület most Magyarországon, ahol e három adó valamelyikét nem lehet fogni. A következő ábrákon az analóg adások lakossági ellátottsága látható. (4., 5., 6.ábra)



4. ábra: Az m1 műsor országos televízió-ellátottsága [3]



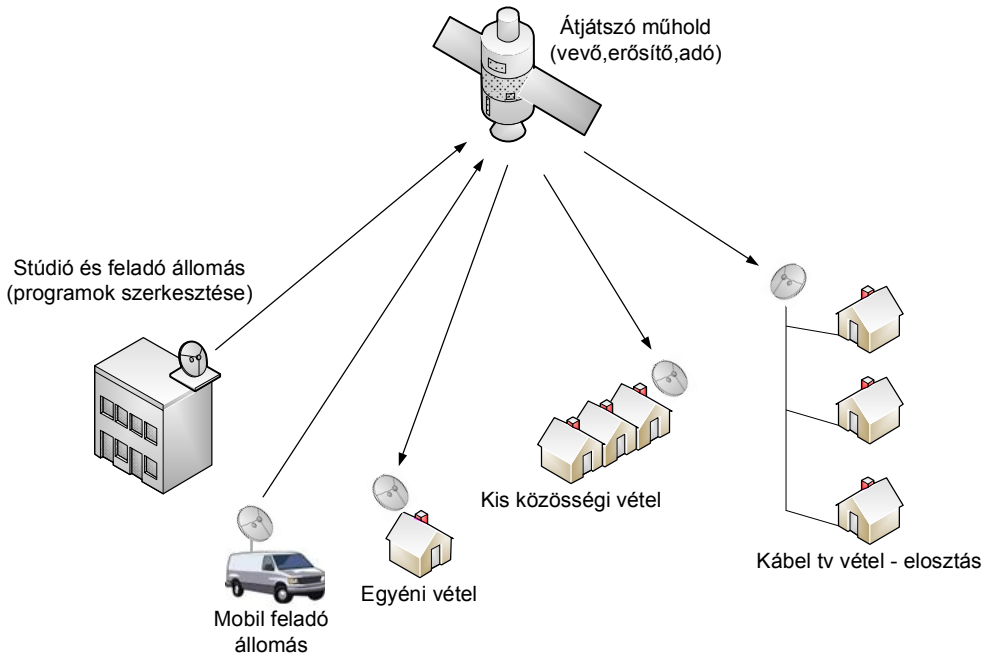
5. ábra: A TV2 műsor országos televízió-ellátottsága [4]



6. ábra: Az RTL Klub műsor országos televízió-ellátottsága[5]

Abban az esetben, ha valamelyik adótorony nem üzemelne, átmeneti fennakadást okozhat az információ továbbításában. Nem szabad azonban megfeledkezni arról, hogy ez csak egy a műsorszórási lehetőségek közül.

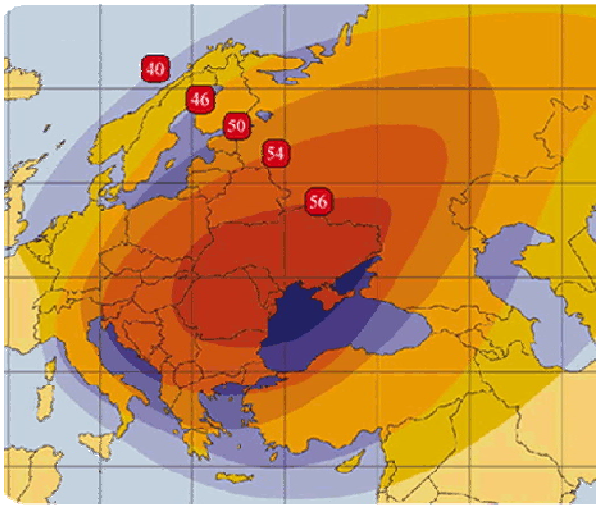
A műholdas műsorszórás jellemzője az egy adó több vevő elrendezés. A videó- és hangjel a földi feladóállomás adójából kerül a műholdra, és a műsorszóró műhold fedélzetén csak egyszerű, ismétlő funkciót ellátó átjátszóállomások működnek. A műsorszórás számára meghatározó fontosságú a geostacionárius műholdpálya és a pályán elhelyezkedő műholdak. A műholdas műsorszórás elvi felépítése a következő ábrán látható. (7. ábra)



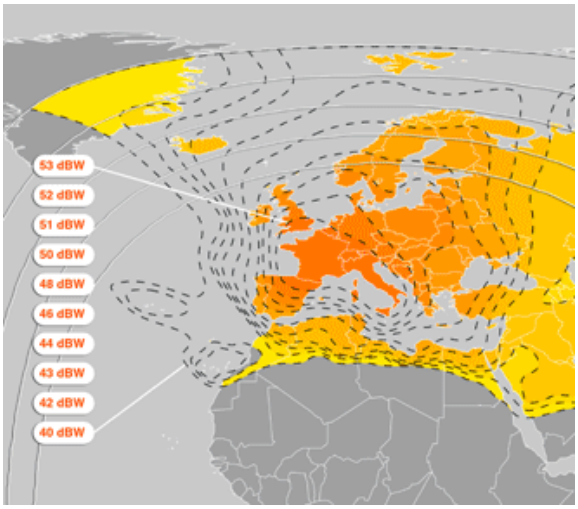
7. ábra: A műholdas műsorszórás elvi felépítése (saját szerkesztés)

Az ábrán jól látható, hogy az adás a műholdra több forrásból is jöhet. Ez az információközlés lehetőségeit még jobban kiszélesíti.

Az Antenna Hungária Zrt. azokat az adókat, amelyek földfelszíni sugárzásra nem jogosultak két műholdon keresztül közvetíti a nézők felé. Az egyik az Amos-3, melynek lefedettsége a 8. ábrán látható, és a Hot Bird-8 melynek lefedettsége a 9. ábrán látható.



8. ábra: Amos-3 műhold európai lefedettsége [6]



9. ábra: Hot Bird-8 műhold európai lefedettsége [7]

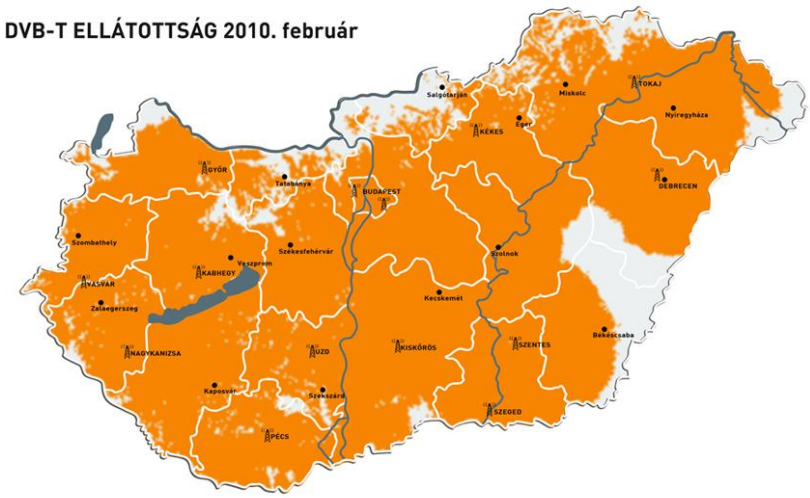
Mindkét műhold európai, illetve hazai lefedettsége jó. Azokat az adókat, amelyeket a műholdak közvetítenek Magyarország bármely pontján egy egyszerű parabolaantennával és egy beltéri egységgel már fogni lehet. Ez lehetővé teszi azt, hogy olyan adókkal bővüljön a kínálat, amelyeket földfelszínen nem tudunk elérni. Ha földfelszíni és a műholdas lefedettség térképeket egymásra helyezzük jól látszik, hogy az ország több mint 95%-ában már van biztosíték az információ biztos célba juttatásához.

Az analóg műsorszórás mellett egyre nagyobb teret kap a digitális műsorszórás. E rendszer kiépítésére jött létre 1993-ban a DVB (Digital Video Broadcasting) néven ismertté vált páneurópai platform. A szervezet feladata, hogy koordinálja a szabványos digitális televíziós sugárzás összehangolt bevezetését a különböző országokban.

A DVB ajánlásai alapján az alábbi szabványok kerültek kidolgozásra:

- DVB-T digitális földfelszíni műsorszórás a VHF-UHF sávban;
- DVB-H digitális műsorszórás mobilkészülékekre;
- DVB-S digitális műsorszórás műholdon keresztül;
- DVB-C digitális műsorelosztás kábelhálózatokon. [8]

Ezen DVB műsorszórások közül hazánkban a DVB-S, DVB-C, DVB-T és DVB-H működik. A földfelszíni analóg adásokat 2011-ben szüntetik majd be. A DVB-T, a földfelszíni digitális sugárzás megoldásainak köszönhetően nagyobb műsorválasztékot, jó minőséget és megbízható vételt biztosít a nézőknek. A DVB-T földfelszíni adásának lefedettsége a 10. ábrán látható.



10. ábra: DVB-T földfelszíni adásainak lefedettsége [9]

Az ábra alapján jól látható, hogy nem teljes a földfelszíni DVB-T lefedettség. Ebben a rendszerben ingyenesen fogható csatornák: m1 HD, m2 HD, TV2, RTL Klub, Euronews, Duna TV HD és a Duna II Autonómia.

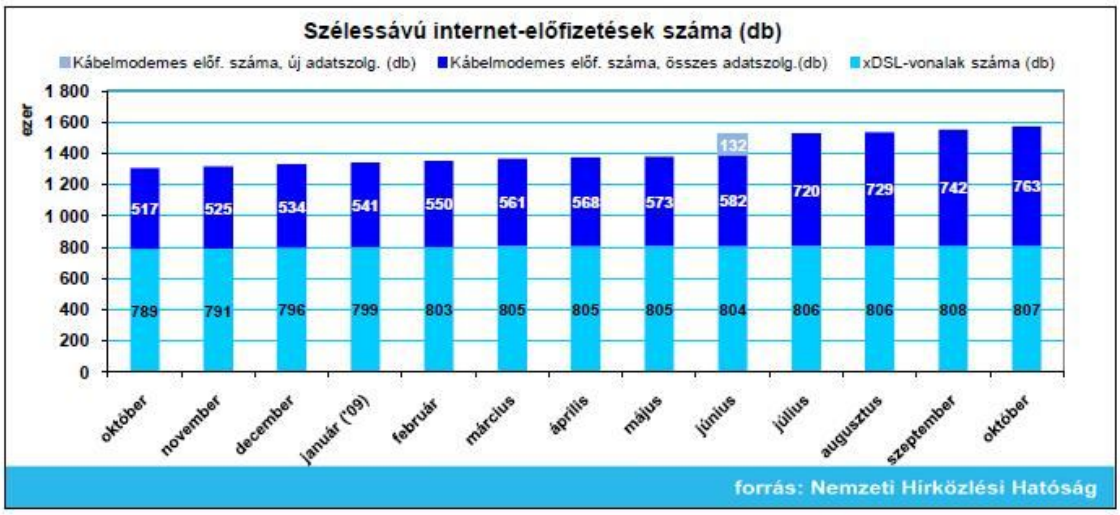
Műsorszórás az IPTV hálózaton

IPTV (Internet Protocol Television) olyan digitális tv-szolgáltatás, melyet IP (Internet Protokoll) használatának segítségével nyújtanak. A szolgáltatás nyújtásának feltétele a szélessávú internet megléte. [10] Ma Magyarországon a szélessávú internet átlagos otthoni felhasználóként háromféle módon érhető el:

- xDSL (különböző DSL technológia) vonalon keresztül;
- kábelmodemmel kábeltv hálózaton;

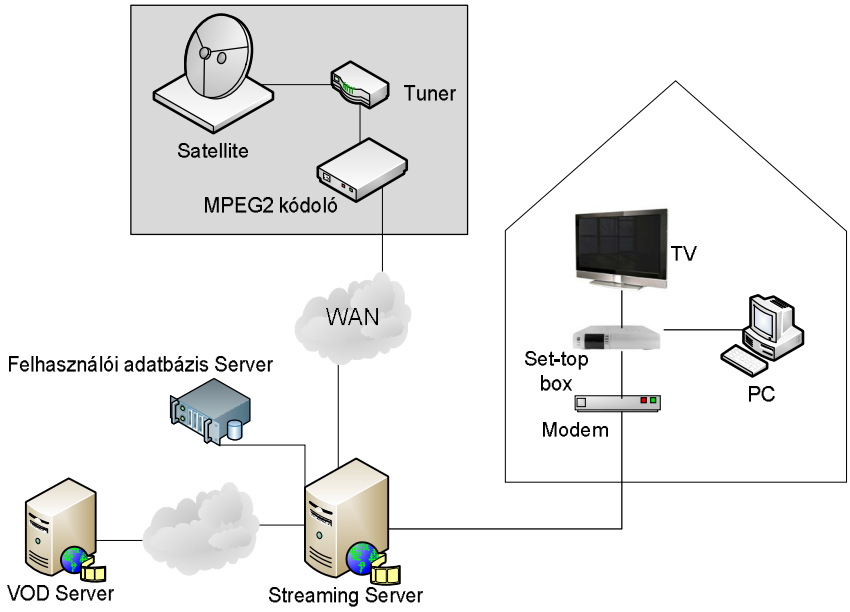
- mobil szélessávon.

Az xDSL és a kábelmodemes szélessávú internet előfizetők száma 2009. októberéig a következőképpen alakult. (11. ábra)



11. ábra: Szélessávú internet-előfizetések száma [11]

Az ábrából jól látszik, hogy a vezetékes szélessávú internet előfizetések száma a 2009. év végére elérte az 1,5 milliót. Ez a típusú szolgáltatás alkalmas IPTV kiépítésére. Az IPTV elvi felépítését a 12. ábra mutatja.

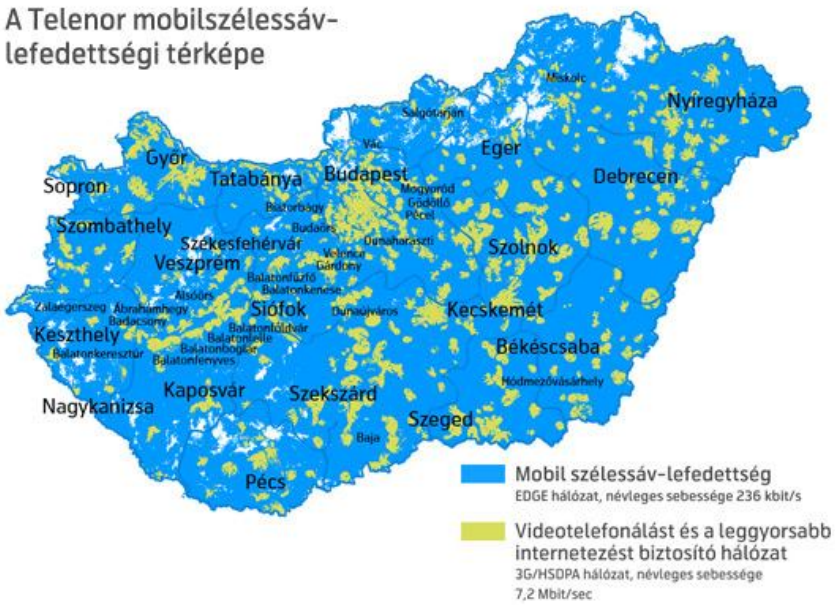


12. ábra: IPTV elvi felépítése (saját szerkesztés)

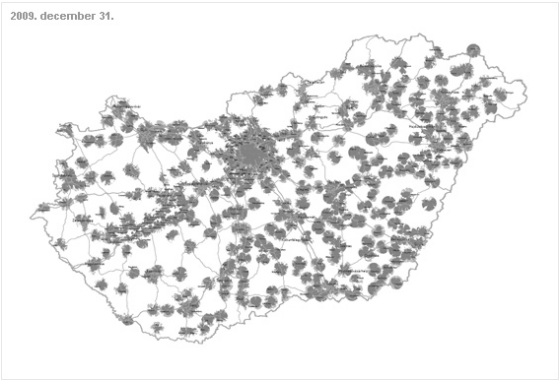
Az IPTV-t gyakran hozzák összefüggésbe az Internet TV szolgáltatással, amely a szokásos interneten keresztül igénybe vehető tv szolgáltatás, egyszerűbben WebTV szolgáltatás – ellentétben az IPTV-vel, amely olyan adattartalom, mely helyi számítógép-hálózatokon keresztül érhető el. [12]

A WebTV szolgáltatás leggyakrabban archív TV műsorokat kínál a felhasználóknak. Ez alól kivétel az m1, m2 és a Duna Tv műsora. Ezen csatornák webes felületén online nézhető a TV adás minden megkötés nélkül.

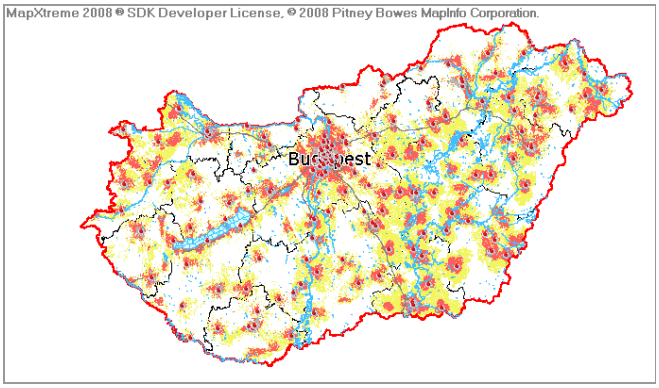
A mobil szélessávú internet elérés segítségével mobiltelefonon is nézhetjük TV adásainkat. Mind a három mobilszolgáltató biztosítja a nagyvárosokban a gyors 7,2 Mbit/s-os internet elérését. A mobilszolgáltatók szélessávú internet-lefedettsége a 13., 14. és 15. ábrán látható.



13. ábra: Telenor mobil szélessávú internet-lefedettség térképe [13]



14. ábra: T-mobile mobil szélessáv lefedettsége [14]



15. ábra: Vodafone mobil szélessáv lefedettsége [15]

Összefoglalás

A polgári műsorszórás, mint kritikus információs infrastruktúra elemzése kapcsán kijelenthetjük, hogy a műsorszórásnak olyan sok és nagykapacitású csatornái vannak, hogy egy-egy műsorszóró médium átmeneti kiesése nem gátolja az embereket az információ megszerzésében a kellő időben a kellő helyen. A mobilitás lehetővé teszi, hogy mobiltelefonnal, vagy a nyaralóban a folyóparton megfelelő eszközzel foghassunk olyan adásokat, amelyek fontos információhoz juttatnak minket.

Felhasznált irodalom

[1] 2080/2008. (VI. 30.) Korm. határozata Kritikus Infrastruktúra Védelem Nemzeti Programjáról
http://www.otm.gov.hu/web/jog_terv.nsf/0/19659F03FD726909C12574C20034751C/$FILE/2080_2008_Korm-hat.pdf
(2010.08.28)

[2] Pete Krisztián:*Társadalmi kommunikáció*
http://ktnye.akti.hu/index.php/T%C3%A1rsadalmi_kommunik%C3%A1ci%C3%B3
(2010.08.28)

[3] Országos televízió-ellátottság, m1 műsora, (2007)
http://www.nhh.hu/hirk_stat/egyedi_grafikon.nhh?&kep=4036_2007.jpg&fejezet=4&nyelv=0

(2010.08.28)

[4] Országos televízió-ellátottság, TV2 műsora, (2007)
http://www.nhh.hu/hirk_stat/egyedi_grafikon.nhh?&kep=4037_2007.jpg&fejezet=4&nyelv=0
(2010.08.28)

[5] Az RTL Klub műsor országos televízió-ellátottsága (2007)
http://www.nhh.hu/hirk_stat/egyedi_grafikon.nhh?&kep=4038_2007.jpg&fejezet=4&nyelv=0
(2010.08.28)

[6] Amos-3 műhold európai lefedettsége
http://www.amos-spacecom.com/amos1/page.asp?cat=45&type=4&lang=1
(2010.08.28)

[7] Hot Bird-8 műhold európai lefedettsége
http://www.eutelsat.com/satellites/13ehb8.html
(2010.08.28)

[8] Digitális műsorszórás szabványai
http://www.ahrt.hu/Digitalis_atallas/Digitalis%20televiziozas.aspx
(2010.08.28)

[9] DVB-T földfelszíni adásainak lefedettsége
http://dvbvevo.hu/cms/dvb-t_lefedettseg.html
(2010.08.28)

[10] IPTV
http://hu.wikipedia.org/wiki/IPTV
(2010.08.28)

[11] Szélessávú internet-előfizetések száma
http://www.nhh.hu/dokumentum.php?cid=22050
(2010.08.28)

[12] IPTV

http://hu.wikipedia.org/wiki/IPTV

(2010.08.28)

[13] Telenor mobil szélessávú internetlefedettség térképe
http://www.telenor.hu/internet/tudnivalok/lefedettseg/
(2010.08.28)

[14] T-mobile mobil szélessáv lefedettsége
http://mobilarena.hu/teszt/hazai_mobilinternet_korkep/lefedettseg.html
(2010.08.28)

[15] Vodafone mobil szélessáv lefedettsége
http://mapinfo.vodafone.hu/mapxtreme/Content.aspx
(2010.08.28)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Bolgár Judit
bolgar.judit@zmne.hu

Krajnc Zoltán
krajnc.zoltan@zmne.hu

SOME THOUGHTS ABOUT PSYCHOLOGICAL QUESTIONS OF ASYMMETRIC WARFARE

Absztrakt/Abstract

A szerzők átfogó képet adnak az aszimmetrikus hadviselés pszichológiai tényezőiről. Áttekintik a kérdést teljes komplexitásában: a fenyegetéseket, stratégiai aspektusokat és a hadtudományi alapokat egyaránt.

The authors sum up the more capital questions of the asymmetric warfare and its psychological factors. They give overview about the military-scientific basis of the asymmetric warfare and its threats; interpretation of asymmetry in the activities of national security; systematic elements of strategic asymmetry; coherence of strategy reacting to asymmetric threats with other strategies and finally psychological aspects of asymmetric warfare.

Kulcsszavak/keywords: *aszimmetrikus hadviselés, pszichológiai hatások ~ asymmetric warfare, psychological factors*

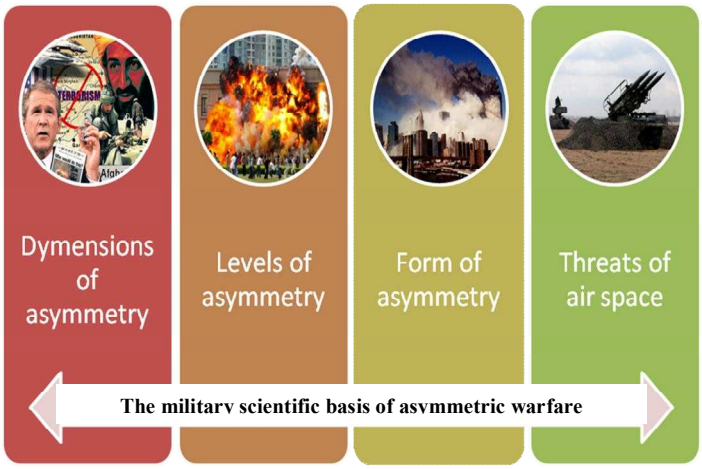
INTRODUCTION

In our article we want to discuss one of the most frequently mentioned topics of today's military science and national security, the so-called *"asymmetric warfare and intimidation"* and its psychological aspects. Our aim is not the explanation of the military scientific aspect of the term, but the sociological and psychological aspect of this phenomenon. But to do this, it is essential to analyse the essence of warfare in a couple of words.
The second part of the research deals with the socio-psychological mass aspect of this term, its influence on today's national security.

THE BASICS OF ASYMMETRIC WARFARE AND ITS THREATS

National security (military) specialists have been using this term as some kind of a paradigm, however, in our domestic literature, it is not possible to find any basic analysis of the main questions of the asymmetric warfare, that would give its main definition, and based on that

would give the answers within the area of national security. If we analyse these scientific papers, we can see that this warfare strategy is considered an axiom, and quite often terrorism and asymmetric warfare are looked upon as one and the same.



We base our findings on relevant research in the USA, on results of operational experience, on the information from our domestic literature, as well as on our analysis of this topic. As a starting point we can consider a simple fact that in wars, in conflicts when weapons are used there are always present differences (asymmetries) between the participants, in the terms of quality, quantity and morale.

It is a historical fact that in certain times, from the point of view of the final result in wars, these differences, called asymmetries, did not play a significant role, though it was different in other conflicts.

This simplifying viewpoint does not take into consideration or shadows the fact that certain warring parties build their strategy on these very asymmetries.

According to the Chinese Sun Tzu, every warfare are based on deception and he suggests to avoid the enemy which bears concentrated force, and to attack the enemy only by means of military deception. As a matter of fact, Sun Tzu built an existing strategy on asymmetry, which is eerily similar to the situation that the USA and its allies have to face today.

The common interpretation of the term requires a complex definition, since only this common platform can provide for future discussion. Almost all relevant experts establish that asymmetric warfare is not a new category, since even in the bible David and Goliath exemplify the difference in the strategy of warriors who possess asymmetric capabilities. However, a common definition and the answers to asymmetric threats have appeared only recently, the reason is that the actual military scientific and national security research started after 9/11 2001 when the fight against terrorism in the USA and its European allies became the central point of the national security.

MAIN ISSUES OF ASYMMETRY IN THE ACTIVITIES OF NATIONAL SECURITY

In 1998 the National defence University of Washington defined asymmetric warfare as an *„unfair"* form of warfare.[1] This definition was based on highly subjective evaluation and quite often it did not represent an easily managed category.

In 1999 the definition presented in the Joint Strategy Review tried to establish a wider definition which would be more acceptable for the military, as well as for the *„decision-makers"*, the introduction of the so- called asymmetric approach (viewpoint). According to this term, *„the strategy of the enemy is aimed at eluding, deceiving or undermining the weaknesses of the USA with methods that significantly differ from the operational ones expected by the USA… usually they focus on psychological elements, like shock effect or disturbance, which influence the American ability to initiate, morale, as well as freedom of action. The asymmetric approach is based on thorough evaluation of the vulnerability of the enemy. It often applies innovative, not traditional procedures, weapons or technologies.*

[1] Strategic Assessment 1998: Engaging Power for Peace (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1998)

Asymmetric warfare can appear in the entire spectrum of military activities, it can be operational, tactical, and strategic."[2]

This definition has tight strings with national security in America, with the challenges and strategic environment, in other words, it is not general or common enough in its character. Moreover, it contains only the „negative asymmetry", which is based on the opinion that the USA is already in great advantage in its technological, military, economic capabilities compared to anybody else, so it does not deal with situations where equal or almost equal partners apply asymmetric procedures against each other, in other words, they base their entire strategy on asymmetry.

Steven Metz and Douglas V Johnson II tried to establish a more general, more complex definition, which can improve the above- mentioned insufficiencies.[3]

"Asymmetry when applied to national security and the military, practically represents different varieties of action, organisations, way of thinking from those of the opponent, which is aimed at maximising their own strength and to use the weaknesses of the enemy, as well as to be able to initiate or to gain more significant freedom of action. So, asymmetry can be politically-strategic or military- strategic or the combination of both."

According to the above-mentioned authors, in practice it means different methods, technologies, organisational framework, it can also be described by several other characteristics, such as the dimensions, levels and forms of asymmetry.

MAIN DEFINITIONS RELATED TO STRATEGIC ASYMMETRY

Dimensions of asymmetry

Strategic asymmetry may be positive or negative in its character. It is usually determined by the opinions or the relative positions of the opposing parties When speaking about positive asymmetry, the United States, for example, emphasises the importance of high level of training, efficient leadership,, and the top technology of the leadership infrastructure, as well as the military arsenal which supports them. This strategy is built on the exploitation of this relevant superiority; on the other hand, negative asymmetry is based not on its own strength, but on the desire to use the weaknesses of the enemy. Consequently, based on these terms, the coalitions led by the USA have to prepare for combat against threats represented by negative asymmetry.

Asymmetry possesses some kind of time aspect; it can have a short- time aspect, as well as a long-time one. There are several examples for both in military science.

There are fewer examples for long-term asymmetry in our days, though certain superpowers, in certain periods of time, held onto their success based on positive asymmetry, but in long term, the balance moved towards equality.

Strategic asymmetry can be brought about intentionally, or there can be asymmetry that appears because of the relative position of the opposing parties. Success is not always

[2] Joint Strategy Review 1999, Washington, DC: The Joint Staff,
1999, p. 2.

[3] Steven Metz és Douglas V. Johnson II. Asymmetry and U.S. military strategy: definition, background, and strategic concepts; (5., 6. oldal), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=223, (2008. 04. 06.)

guaranteed by the superiority in the basic situation, because the analysis of situations shows that the reacting strategies must be flexible and adaptable if a warring opponent whose strategy is based on negative asymmetry needs to be defeated.

The factor of the risk level of asymmetric threat can be low or very high. Forces of excellent training who are operationally well-prepared, the possibility of success or failure represent the high risk category of asymmetry. Having forces that require serious material investment, not to mention their deployment against asymmetric threats is of high risk, to mention, for example, the terrorist attack in Aden of the USS COLE, where terrorists achieved great success without much expenditure. On the other hand, terrorism is characterised by small expenditure, expected success and low risk factors.

Coherence of strategy reacting to asymmetric threats with other strategies

Threats are very complex, consequently, reacting to those needs complex, coordinated and harmonised strategy. Diplomatic, economic, military and other actions need to be coordinated, so that their interference would target strengthening.

Asymmetry can be of cost-effective or psychological nature, although they are interconnected. Materialistic asymmetry can quite often produce a psychological one. Sides who used manipulative techniques, who built their actions on psychological asymmetry, were successful. The most effective is the combination of the two, although psychological advantages need more of intellectual and less of financial investment.

In history there are several examples of asymmetry of operational level. During WW2, for example, the submarine warfare of Germans was aimed at countering the superiority of the traditional colonial one of the British.

In the case of political-strategically asymmetry, military advantages are reached not by military means. This strategy was successful in North Vietnam, where it was possible to portrait their moral superiority against the aggressor, the USA, while neither Milosevic, nor Saddam Hussein succeeded in doing so.

Forms of asymmetry

Asymmetry can be recognised both in methods and procedures, which means different operational and strategic concept (guerrilla warfare vs. traditional operational concept, airborne, airborne mobile operations vs. traditional infantry warfare, etc.)

Technological asymmetry was a regular phenomenon in the past (eg. The Vietnam war, the Afghan talibs vs. The USA, etc.)

Asymmetry is represented in the *„willingness”*, in the moral part of the warfare, as long as a state fights for its existence and its basic interests. In this case this aim can multiply military forces; on the other hand, the combat willingness of an occupying party, whose aims are not of vital importance, can be weaker, due to its moral deficiency.

Organisational asymmetry can also be of great importance in the final result of combat, since the organisational frames, warfare based on teamwork, preparation for decision- making significantly determines the best operational concept and success.

PSYCHOLOGICAL ASPECTS

As we have shown in our short summary above, there is a well-defined system of the notion of asymmetric warfare in special literature, which also deals with the analysis of the psychological aspects of past wars.

If we want to analyse the topic, not to base it only on history, but also in the present and the possible future scenarios of security risk factors, it cannot be avoided to analyse the

psychological aspects that are not of local character, which, in our case, describe those psychological aspects that are more serious than local problems and they can be of interest for the analysis of the phenomenon.

Fragments of the mass psychology of the asymmetric warfare

In case of the notion of asymmetric warfare when it represents the actions of opposing forces that are in confrontation, when the sphere of operation, their targets, arsenals used by one of the sides can significantly differ from those of the opponent – first of all, we need to emphasize that it is not a new phenomenon.

We have already pointed out, asymmetric warfare could have been recognised starting from the ancient times up to modern times, and the fact that it plays such a significant role either in military doctrine research or in publications in the press, has two basic reasons.

As we see, one of the reasons is that something has ended, something that, relatively for a long time, even if not easily but still could handle certain basic security criteria. As a matter of fact, within the historic validity of the Yalta and Potsdam agreements – even though in the meanwhile several military conflicts were marked by the signs of asymmetric warfare- the existence of the bipolar world, the desire to establish balance in the world caused people to think that symmetric arms race is bad but there is nothing it can be substituted by in the upholding of the balance between the two world systems. This system ceased to exist and together with it the unspoken mutual agreement that both poles get a free hand to keep order in their spheres of interest, respectively. There was no fear of the gigantic opposition for the world any more, fears of the past disappeared.

From the point of mass psychology, it could have been the time to feel relieved, but the past fears were immediately substitutes by new ones. It turned out that those prepared for symmetric warfare had no idea whatsoever how to handle asymmetric threats that rapidly became a world problem. Their system of institutions (including military defence structures), proved to be as useless in the fight against terrorism as well as in the fight against other, global kinds of crime, for example, financial, IT, technological, biological, cultural, etc. Those brought up in the symmetric system, soon realised that their sense of defencelessness became acute, nobody and nothing can protect them anymore, that each bite of food, each drop of water, each flight, seaside resort or underground station can be dangerous, and these fears are absolutely irrational, since they are threatened regardless of their behaviour or nationality.

The other reason for the seriousness of the mass psychological effects of the asymmetric warfare can be traced back to the so- called globality, which appeared as a result of a non-organic development. It means that the structure of globality in many regions is not the result of its own organic development, but often imports from developed regions built into given cultures non- organically. Even with only one look into the problem, it brings up a number of questions like the influence of films from Western countries or advertisements, in such remote regions that are far away from the possibilities of this kind of lifestyle. How can people who are destitute use these possibilities, those who never used a telephone, who had never been seen by a doctor, and they are as distant from the lifestyle of a Western billionaire as of that of

a simple shop assistant? Or what about state or religion leaders who fight for peace, who are not able to accept social differences of this magnitude, not to mention those who base their carriers on demagogue anger raising and call for *"sacred wars"*?

Globality can not only diminish, but can also strengthen prejudice, everyday racism, intentional provocation, aggression. Moreover, those used to symmetric behaviour; do not consider the fact that the developed civilisations are much more vulnerable than the less developed ones. With proper military superiority it is easy to paralyse several road junctions, central energy supply points or satellites. But what is the value of the military superiority when there is no electricity and the main means of transport are donkeys? With this example we simply want to emphasize that in case of asymmetric warfare a certain degree of under development can be an advantage and this advantage can be diminished not by applying the most modern means, but by new arms doctrines, moreover, by the establishment of new mass psychology behavioural culture.

„All significant American military failures since 1945 – Vietnam, Lebanon and Somalia – were in the fight against a weaker opponent. Either in the so- called hot or cold wars the USA was successful, let he enemy be the Nazi Germany, the empire of Japan or the Soviet Union, however, the Americans did not always won against weaker opponents… In all cases an American Goliath got into stalemate situation and suffered political defeat from the local Davids. The fact that the weaker defeats the stronger, although it is exceptional happens again and again. Sparta eventually won against Athens. Frederick the Great always punched well above his waist. American rebels stopped the British domination in 13 colonies, Jewish terrorists ruled out the Brits from Palestine, the Vietnamese communists got rid of the French, then the Americans from Indochina and the mudjaheddins presented a „Vietnam„ to the Soviets in Afghanistan. The relative size of the military forces cannot predict effectively the outcome of the war." [4]

It is quite obvious that in an attack against antagonists it is not the most effective if army of massive strength, UAVs or heavy artillery is implied, but rather actions similar to those based on military and police structures, with their help it is possible to diminish the asymmetry of the opposing sides. For the axiomatic practice of such doctrines it is necessary to change old patterns, complicated interest as well as to change the old ways of fighting against global crime.

It is also necessary that those professional – political organisations responsible for the well- being of the mankind would consider their main aim as of the establishment of global security instead of dealing with their local interests. Consequently, asymmetry as an existing reality should not be the tool aimed at the destruction of the *„different"* or *„difference"* but it should be a relative basis that could provide the condition of heterostatic balance to enhance better global cooperation.

CONCLUSION

In our paper we briefly summarised some correlations between the psychological aspects of asymmetric warfare and its threats. Asymmetric warfare, as it is demonstrated in this article, is a complex sociological problem, which, opposed to many simplifying opinions, is not equal with the terrorism.

If we want to understand the important questions about asymmetric warfare and the consequent threats, it is essential to understand the question of the so- called *„choice of target"* method of the antagonist who bases its strategy on asymmetry.

[4] Jeffrey Record : Why the Strong Lose, Parameters, Winter, 2005-06, pp. 16-31., (http://www.carlisle.army.mil/usawc/Parameters/05winter/record.htm)

To simplify this: how, according to what principles, what are the expected effects when targets are chosen? From the point of view of symmetry, as a potential opponent of asymmetric antagonist, we should be able to define, for the benefit of defence, to define the list of objects and the possible forms of the attack. This task is of priority mainly for operational experts (reconnaissance staff) and they can perform this task successfully only in case if they are familiar with the psychological background of the asymmetric warfare.

However, problems described by us point beyond their military aspects: the concepts of mass psychology are in tight correlation with the fact that the process of globalisation has only partially finished and simply from the nature of this process of development comes the proliferation of asymmetries that hinder normal functions. The first task in connection with this – understanding the reasons of their appearance – to accept their existence. The second task, although we are able to explain the proliferation of this phenomenon, is to urge for a global and worldwide action for the establishment of a possible symmetry. The third task is to clarify the fact that this work cannot be considered simply as a military one, but we need to aim to establish an opportunity for a more thorough globalisation than the existing one.

With our article we want to get connected to the process of learning without hiding our aim to help our Hungarian soldiers who work in the operational field, as well as those civilians who participate in research to understand this undoubtedly significant phenomenon.

REFERENCES

[1] Strategic Assessment 1998: Engaging Power for Peace (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1998)

[2] Joint Strategy Review 1999, Washington, DC: The Joint Staff, 1999, p. 2.

[3] Steven Metz és Douglas V. Johnson II. Asymmetry and U.S. military strategy: definition, background, and strategic concepts; (5., 6. pages), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=223, (2008. 04. 06.)

[4] Jeffrey Record : Why the Strong Lose, Parameters, Winter, 2005-06, pp. 16-31., (http://www.carlisle.army.mil/usawc/Parameters/05winter/record.htm)

[5] Krajnc Zoltán: A légierő megváltozott szerepe a XXI. század hadviselésében, Geopolitikai Tanács, Műhelytanulmányok 2006/7.

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Gőcze István
gocze.istvan@zmne.hu

THE WAR OF FUTURE – THE FUTURE OF WAR

THE VIEWS OF THE UNITED STATES ON THE ARMED CONFLICTS OF THE 21ST CENTURY AND THE NEW DEVELOPMENTS OF MILITARY TECHNOLOGY OF THE USA PART 1

Absztrakt/Abstract

A szerző a tanulmányának első részében részletesen megvizsgálja az Amerikai Egyesült nézeteit, elképzeléseit a 21. századi hadviselésről. Továbbá elemzi az USA új technikai-technológiai fejlesztéseit, ennek kapcsán foglalkozik a nagyteljesítményű számítástechnika szerepével, az integrált harctér, a lézerfegyverek létrehozásának lehetőségével, és végül, de nem utolsó sorban az említett szuperhatalom csillagháborús terveivel. A cikk szerzője — többek között — arra keresi a választ, hogy a fent említett amerikai technikai-technológiai fejlesztések valóban csak a terrorizmus elleni küzdelmet szolgálják-e?

In the first part of his study paper the author gives a detailed analysis of the ideas and concepts of the United States of America on 21st century warfare. Furthermore he analyses the new technical-technological developments of the USA, deals with the role of highly powerful information technology, the potentials of creating integrated battlefield and laser weapons, and last but not least with the star wars projects of the above mentioned superpower. The author of the article seeks the answer – among others – to the question whether the above mentioned development projects are aimed at combating terrorism only.

Kulcsszavak/keywords: *háború, hadviselés, jövő ~ war, warfare, future*

Introduction

The end of the bipolar world order – in my opinion – involved much more than the end of the conflict between two superpowers and their alliances (NATO – Warsaw Treaty) since one of them, the Warsaw Treaty, broke up in 1991 and on 31st December the same year the Soviet empire also ceased to exist. However, the end of the Cold War did not mark the beginning of happy peace times. Analysts (Baylis, et.al. /ed./, 2005:10-11.) who anticipated that the Cold War had been a much simpler political and military-political structure than the era which followed and has been on to date proved to be correct. In their analyses these experts stated that the Cold War was a chess game where the two players (the USA and the Soviet Union) were able to keep the rest of the players well in hand. In the first period of time it was reconcilia-

tion which took the foreground and it is highlighted by the fact that defence expenditure fell from USD 1,200 billion per year, the top of the Cold War period, to USD 800 billion per year (see: figure 1.). However, it had to be realised that the new era generated completely new challenges. First of all the significant growth of international terrorism has to be highlighted. In connection with this notion the issue of Islamic terrorism should not be disregarded. After 11th September 2001 the USA and the western world – moreover a significant part of the Eastern countries too – launched significant arms programmes and began elaborating new combat methods under allowing them to fight terrorism. In this particular case the word "significant" means that the defence expenditures of the countries of the world exceeded the Cold War peak (approximately USD 1,350 billion a year). This growth is indicated by the graph below[1].

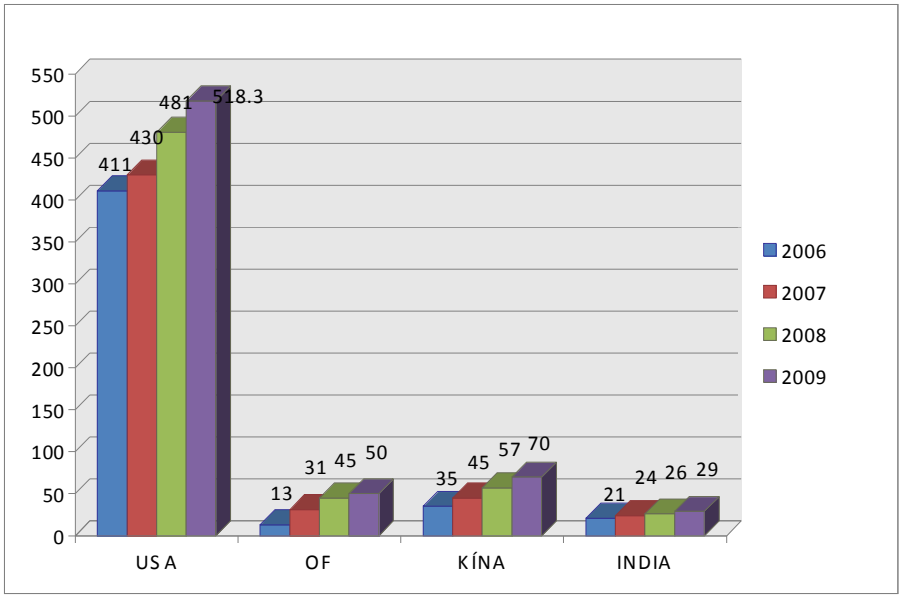


Figure 2[2]. Figure 2 above shows the defence expenditures of the four most significant powers of the world in billions of Euros. It clearly indicates that these expenditures continuously grew in the past period of time.

Let us take a look at some further figures on arms programmes:

[1] www. globalissues.org 2009. 12.11.

[2] www.iiss.org/publications/military-balance 2009. 12.11.

- the defence expenditures of the USA increased from USD 387 billion in 2000 to USD 709 billion out of which a "mere" USD 194 billion was spent on the wars in Afghanistan and Iraq;
- the USA spends 45% of its GDP on arms;
- the combined defence expenditures of states regarded by the Pentagon as potential adversaries (Cuba, Iran, Libya, Sudan, North Korea, and Syria and the two great powers – Russia and China) make up just 29% of the American military budget;
- the combined defence expenditures of the United States and its closest allies (NATO, South-Korea, Australia and Japan) make up 72% of the global military spending. (Hettyei, 2008)

In my opinion, however, it is not uninteresting to take a closer look at the issue and analyse how the USA, currently the only superpower of the world, sees the war of the future. It should be noted that future warfare including the trends in the technological development of conventional branches and services and even the blueprints in the stage of planning are expected to be dominated by the fight against terrorism. In my opinion – and the present study paper may highlight or even prove it – the significance of terrorism may slightly decrease compared with the anticipated global challenges in the near future. These include the lack of drinking water (the United Nations mentions water conflicts in the near future /Kerekes, 2006/[3]); negative impacts generated by the accelerated global warming, such as rising sea levels, migration from coastal megalopolises, decreasing arable lands which may lead up to food wars, easier exploitation of natural resources (see: North Pole conflict /Szerencsi, 2008/), and the list could be continued. However, these challenges go well beyond the issue of terrorism and in my opinion the future will not be an age of fourth generation warfare only – Lind theory (Lind, et. al., 1989:22-26.) – but third and fourth generation conventional conflicts, moreover a mix of warfare at a much higher level, may also get into the foreground. Naturally, the stronger party will force its will on the weaker one in order to achieve its objective. This was established as early as by Clausewitz therefore it can be stated that *revolutionary change of paradigms* labelled after Kuhn (Kuhn, 2000) cannot be fully identified in military science.

Returning to objectives, it is probable that from the fundamental elements possessing drinking water or that of arable lands will be priority and become the main causes of conflicts in the future, besides conflicts erupting due to cultural-religious-civilisation causes as identified by Huntington.

In order to prove my hypothesis, below I examine how the USA military leadership – I wish to repeatedly emphasise under the aegis of combating terrorism – envisages future warfare and what technological-technical developments are conducted at the branches and services in this framework.

A serious analysis helps answer the question: *"ARE THESE WEAPONS TRULY PRODUCED FOR DEFEATING TERRORISM?!"*

The concept of a war of the future

Military people, researchers of military science, and even outsiders often put the question what the war of the future will be like.

From the Hungarian researchers of military science – without striving to completeness – the persons and their study papers listed below must be mentioned as they focus on 21st century warfare and particularly on military theories.

[3] „ForestPress quotes a UN study paper according to which wars may break out for water in regions where rivers and lakes belong to several countries. Allegedly even now a minimum of ten African countries are ready to go to war for the water of the river Nile." (Kerekes, 2006)

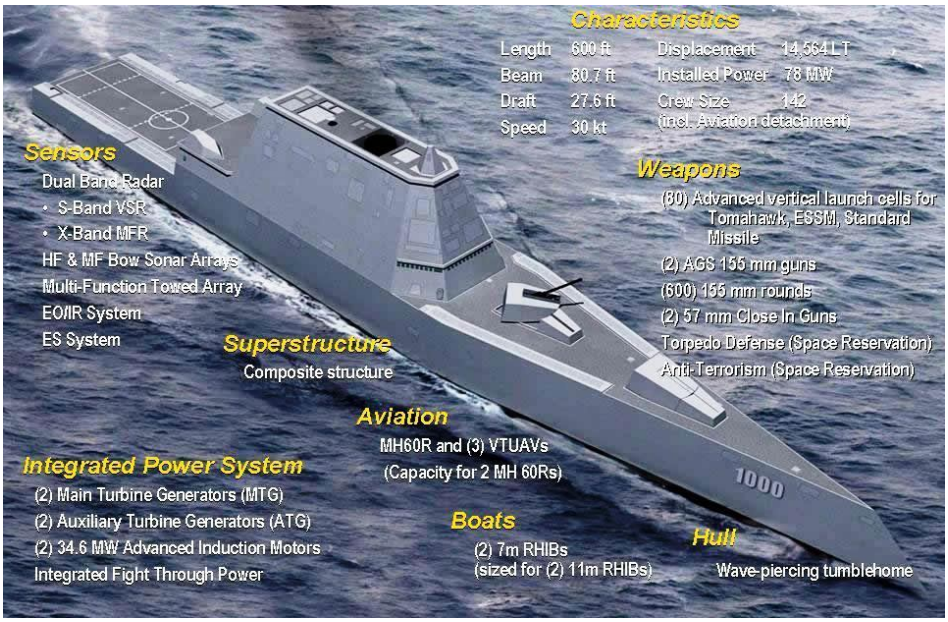
- Braun, László: *A magyar katonai erő újszerű alkalmazása a 21. században* [The New Use of the Hungarian Military in the 21st Century] (Braun, 2005)
- Deák, János: *A katonai műveletek hadászati jellemzői napjainkban* [Some Strategic Characteristics of Modern Military Operations] (Deák, 2005)
- Deák, János: *Napjaink és a jövő háborúja* [War Today and Tomorrow] (Deák, 2005b)
- Makk, László: *A katonai erő alkalmazása a 21. században* [The Use of Military Forces in the 21st Century] (Makk, 2005)
- Molnár, István: *A jövő háborújáról, fegyveres konfliktusáról* [On the War and Armed Conflict of the Future] (Molnár, 2005)
- Nagy, Zoltán: *A 21. század fegyveres küzdelmeinek irányai és kihívásai a NATO szemszögéből* [Some Trends and Challenges of Armed Conflicts in the 21st Century from the Aspects of NATO] (Nagy, 2005)
- Ormos, Mária: *A háborúról és a terrorizmusról* [On War and Terrorism] (Ormos, 2005)
- Szenes, Zoltán: *Katonai kihívások a 21. század elején* [Military Challenges in the Early 21st Century] (Szenes, 2005)
- Resperger, István: *A 21. század fegyveres konfliktusainak hatása a hadtudományra* [The Influence of 21st Century Armed Conflicts on Military Science] (Resperger, 2005)
- Ronkovics, József: *A 21. század hadviselésének néhány főbb jellemzője* [Some Major Characteristics of 21st Century Warfare] (Ronkovics, 2009)
- Szternák, György: *A katonai műveletek megvívásának jellemzői napjainkban, levonható következtetések hatása a hadtudomány fejlődésére* [The Characteristics of Conducting Modern Military Operations and the Influence of Lessons Learned on the Evolution of Military Science] (Szternák, 2010)

Below let us take a look at how the opinions of American experts forecast a future was, *mainly from technological-technical aspects*.

According to the American ideas the countries will fight rebels hiding among civil population and against terrorists possessing bombs, missiles, rockets, or even weapons of mass destruction, with the use of new technology. A number of new (counterterrorist?) assets are in blueprint versions only but a few of them have already been commissioned.

The following situation – presented by American experts in a study paper – describes the near future: an unmanned aerial vehicle (UAV) – for example a Global Hawk – scouts an enemy held area. It forwards the target coordinates to advancing ground troops. The terrain is scouted by robot vehicles and the data are sent to the command centre. Simultaneously the information is also sent to the missile defence system of a DDG-1000 destroyer[4] 80 kilometres off the coast; to other battlefield units; and to the Supreme Command, thousands of kilometres away.

[4] It should be noted here that according to American newspapers the Pentagon may halt the development project of the ship because one single DDG-1000 destroyer has cost USD 5 billion to date. (Eisman, 2008)



Picture 1. DDG-1000 destroyer[5]

An unmanned combat aerial vehicle (UCAV) takes off from a CVN-class[6] aircraft carrier in order to deliver a strike at enemy forces. At the command post the information from several sources is analysed and an operational plan is elaborated.

Picture 2. CVN-79 CG[7]

Then the tasks for the battlefield unit commanders and assets are identified, and the order to open fire is issued. The above mentioned destroyer launches long-range attack missiles. A

[5] www.globalsecurity.org 2010. 06. 23.
[6] Carrier Vessel Nuclear
[7] http://blog.usni.org/2010/01/18/uss-enterprise-cvn-79-petition-update 2010. 03. 21.

Virginia-class submarine launches a cruise missile in order to destroy a distant ground target and F-35 fighter bombers provide air support to ground units.

The military operation is coordinated by the future combat computer system. The fundamental components of future warfare are made up by new technologies, network-based information systems, sensitive sensors, GPS-equipped missiles, piloted stealth aircraft, and UAVs.

According to American experts the high technology systems under development in laboratories will transform our visions on the future warfare. Most probably everything will be different from that envisaged a few years ago. The information superhighway will be the fundament for the future warfare therefore the USA armed forces are building a tremendous communication network.

"The expression 'network-centred' comes from the American navy in the mid 1990s. It reflects the different approach of the navy. The communication with each other and the High Command on the coast has always been a problem for individual ships. In the 1990s the Navy realised that a lot of information can be sent to the ships through satellite links. Data transfer can be established between the High Command and ships; aircraft and ships; satellites and ships. It was realised that navy units can be combined into a network this way and individual ships are allowed to operate as independent systems." (Pike, 2004) The same network, if enlarged, is able to link Ground Forces, Air Force, and Navy, allowing the establishment of a unified command structure. In the future the relevant commander can choose on the basis of the current situation what assets to use from warships, aircraft, missiles, armoured personnel carriers, or UAVs to deliver a strike at enemy targets. The system is based on a technology well known in civil life: silicon-based microchips.

High-power information technology

As it has already been mentioned above, the USA armed forces are working on the development of a gigantic network. To this end high capacity hardware is under development by the army. New methodology should be discovered for linking man and machine. The complex design work and technological development are supported by huge capacity computers.

The key to future warfare is information technology (IT). The USA Armed Forces uses very fast and powerful computers to do calculations on movements, air-flow, structural mechanisms, and simulations.

Such highly powerful computers produce realistic 3D images. Through simulation a designer is able to get a nearly real picture on whether ceramic plates can protect various combat vehicles or weapons systems from a shell or bullet. By now technological development has exceeded imaging and the data from other sensors can also be entered into calculations. USA Army Research Laboratory researcher Jerry Clark claims that high-capacity IT is only part of modern weapons design. Soon high-capacity computers are integrated in military uniforms, unmanned ground vehicles, and UAVs too. They will be omnipresent which will have its impact on data processing. More and more information will be possible to process in less and less time. (ARO, 2009)

A lot of information arrives from a modern battlefield. However, the cluster of data and risks can only be managed if they are transformed into a unified picture: integrated tactics, integrated battlefield.

Integrated battlefield

First of all it should be stated that thanks to the current development level of IT data transfer has achieved the speed of light. IT devices have become increasingly small and powerful. They can be further developed and military forces can be virtually interconnected at a global scale. The USA uses its IT systems for the rapid deployment of its military forces anywhere in the world. This way information can be receives from the battlefield which allows a more efficient planning and execution of actions. On the basis of sensors and precise target data appropriate weapons can deliver a strike at the right time.

The aim of the military and the leadership is to establish an integrated battlefield which provides a picture on the battlefield through various sensors and communication. It is able to identify combat vehicles on land, the air, and water, including their crews and detachments even in adverse weather conditions. The information is forwarded to all of the involved elements from the High Command down to executive levels, from navy to air force and ground forces units. The same battlefield and targets are seen by all players who are aware both of their own positions and those of the enemy. Integrated tactics was used by the Navy both in Afghanistan and Iraq, where sea and air were controlled through AEGIS tracking and combat system[8]. With the computer-guided radar more than 100 targets were tracked simultaneously on the ground, in the air and sea. The commanders can monitor the entire theatre which allows them to give immediate responses. The most important is information superiority that is to be better informed than the enemy. According to HSI[9] Director Trish Hamburger this requires better sensors, better intelligence, better communication, and a better linking of information. (Hamburger, et.al., 2001) In the case of the air force this involves better tracking of enemy in order to intercept, identify, target, follow, and fight anyone, anywhere, anytime. Situation assessment is similarly important on the ground, in the air and sea but the projection of forces including their comprehensive support – another significant factor of victory – can be a theme for another study paper.

Radio controlled war

Enemy forces can be defeated in radio controlled combat quickly and at a lower risk to friendly forces. Most of the long-range combat weapons are robots.

Picture 3.UAV in action[10]

Let us take some examples: Predators fly in a combat formation and mini UAVs support their activities. Military personnel can check the area behind a hill through a model plane.

[8] Aegis Combat System http://en.wikipedia.org/wiki/Aegis_Combat_System 2010. 07. 28.
[9] Human Systems Integration
[10] www.spektrumtv.hu 2009. 02. 19.

With the use of remote controlled vehicles convoys and patrols check suspicious objects then defuse them from a safe distance. The biggest advantage of robots is that their personnel are safe during their actions

Picture 4. TALON military robot[11]

During the Cold War the world was under the surveillance of spy satellites. The intercontinental ballistic missiles targeting big cities were the means of ultimate deterrence. All this is, of course, useless against terrorism. Finding terrorists hiding among civilians is extremely difficult and requires strikes of surgical precision against enemy territories, which is a job for robot warriors.

Picture 5-7. Shot of the UAV[12]

[11] http://abcnews.go.com/Technology/AheadoftheCurve/story?id=7049327&page=1
„In this file photo, A remotely-operated TALON explosives ordinance disposal robot prepares to defuse a roadside bomb during an IED-clearing mission by US soldiers from Fox company, 4th squadron, 2nd Stryker Cavalry Regiment in western Baquba, northeast of Baghdad, on July 20, 2008. Armed robots working for militaries worldwide are not regulated...yet. (Ali Yussef/AFP/Getty Images)" 2010. 09. 01.

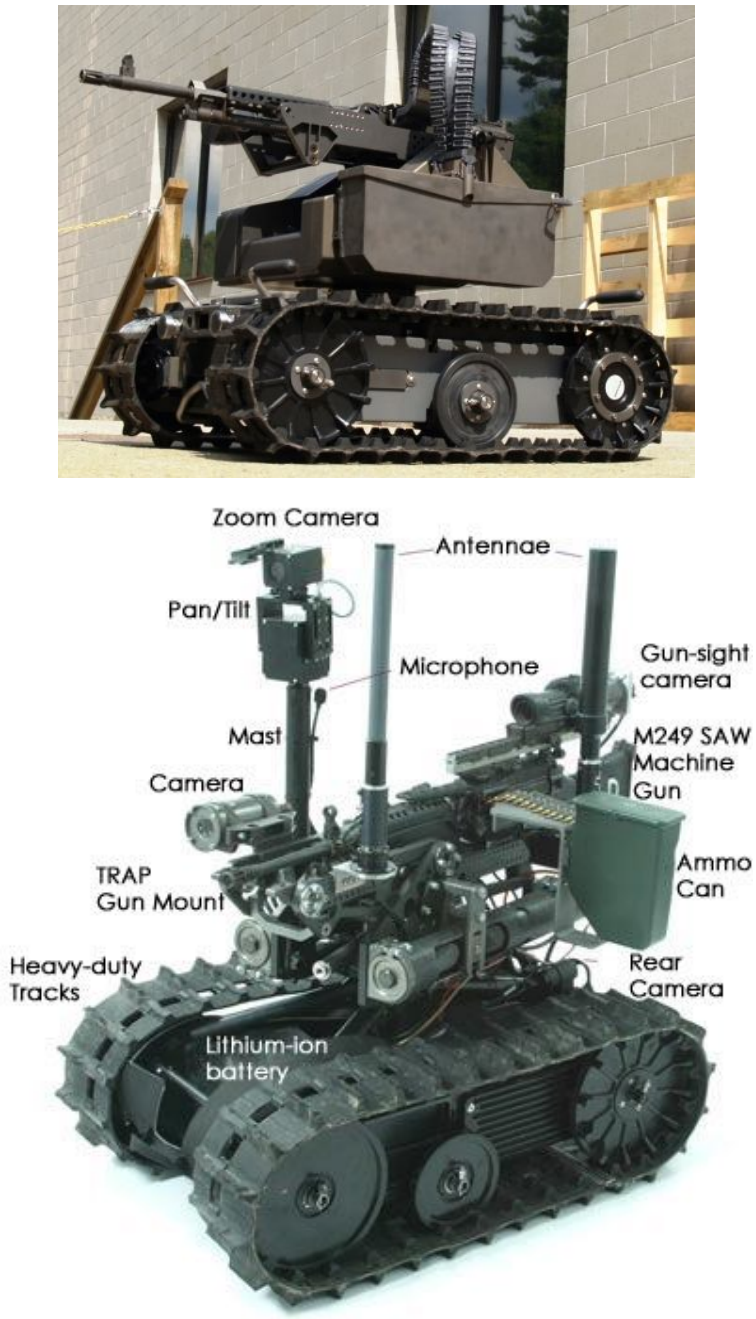
[12] http://www.tacticalwarfightergear.com/tacticalgear/catalog/Military_Robots.php 2010. 09. 01.

When a UAV identifies a target in dozens of kilometres from the battlefield, it sends a video footage to the command post on the other side of the planet, then the CP sends the precise target coordinates to an artillery unit in 30 kilometres from the target via radio. The artillery battery using precision weapons opens fire and with a single shell destroys the target. In the past this job required a lot of rounds as they could not get within the sight of enemy.

Picture 8. F-35[13]

Air force commanders can choose from UAVs, manned or unmanned fighter planes. Then a squadron can include both F-35s and F-22s where each plane participates in a well planned air combat action and it does not matter whether the planes in the formation are piloted or not. This is the battlefield of the future. The assets are tailored to the tasks and missions, regardless of their manned or unmanned feature. The main point is their impact. Not every robot is equipped with wings, like UAVs. Robots provide assistance on the battlefield with simple but dangerous tasks even today. They are telemetric machines guided by people through joysticks. In the future they will be permanent participants in military operations. In the decades to come robots capable of independent decision-making and action will be used. Their role will be more than simple re-supply and they may even play decisive roles however strange it may be. Today there are combat robots and even robots with heavy armament. A device recently used only for mine clearing, tomorrow will be equipped with automatic cannon.

[13] http://www.abc.net.au/news/stories/2008/09/24/2373045.htm?site=news 2010. 09. 01.



Picture 9–10. Robot with weapon[14]

"A robot is more efficient, versatile, and easier to maintain than a human. If it gets damaged in the battlefield it is sent to the repair shop, if it is destroyed no mourning card is to be sent to a family. After war it is taken to the store until its next deployment. In peace time it needs no support. It will fundamentally change warfare. All this may turn reality in a few decades and we are on the right track to have robots fight instead of us. The time may come when no war will have to be waged and if a conflict breaks out robots will be deployed and they will prevent the escalation of war." (Whelan, 2003)

If robot warriors seem too fantastic what opinion could be shaped on the following weapons?

[14] www.spektrumtv.hu 2009. 09. 19.

Laser weapons

Up to now laser weapons only existed in films but soon they appear on battlefields too. A laser is a narrow beam of energy aimed at its target like the death rays in sci-fi movies. High-energy laser can burn a hole through the armour of a tank or into a missile. The navy experiments with free electron laser: with various wavelengths a target can be tracked and destroyed from aerial vehicles or naval vessels.

Picture 11. Laser weapons[15]

Picture 12. Laser weapons[16]

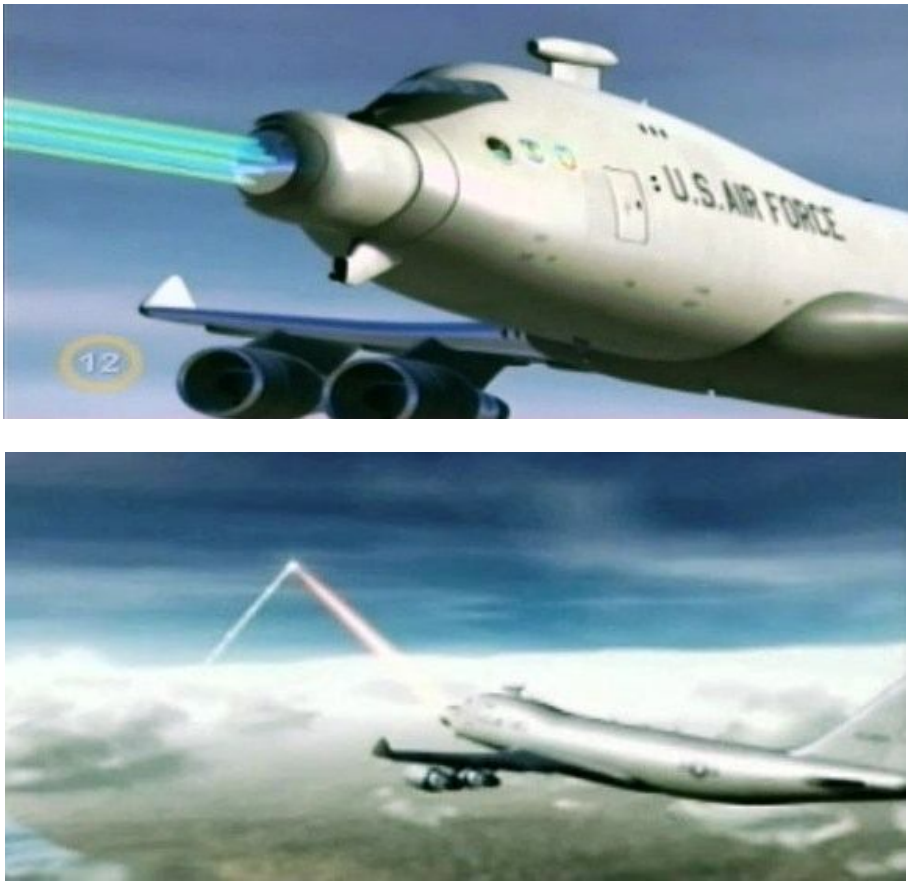
Thanks to its accuracy this laser can become an ideal defence tool of ships against cruise missiles. Since it works at the speed of light the target can be destroyed on time.

The air force entered the laser weapons experiments with an onboard laser mounted on a transformed Boeing 747.

[15] http://www.tacticalwarfightergear.com/tacticalgear/catalog/Military_Robots.php 2010. 09. 01.
[16] www.spektrumtv.hu 2009. 02. 19.

Picture 13. Boeing 747 with laser weapon[17]

The plane at an altitude of 10,000 metres is able to detect and lock on a missile in its initial, acceleration, stage. Then a gas laser beam is emitted from a port in the nose of the aircraft and destroys the missile before it could hit its target.



Picture 14–15. Boeing 747 with laser weapon in action[18]

According to certain American experts in 20 years from now fighter planes will be armed with both attack and defence lasers which will be electric and liquid. The engine will generate

[17] www.spektrumtv.hu 2009. 02. 19.
[18] www.spektrumtv.hu 2009. 02. 19.

electricity which will feed the laser. It will work like a magazine with endless number of rounds. One day it may be laser weapons that will save our World from an attack[19].

Star wars

Below let us examine an interesting imaginary fiction, or maybe a partly existing situation.

An external attack is approaching. A country is willing to deploy ballistic missiles. Can they be stopped? The biggest threat today and in the future is presented by hostile nuclear powers. The USA renewed its contradictory and widely disputed programme. President Reagan's Star Wars programme was aimed at providing the entire country with an umbrella. A smaller version of the missile defence system could be seen in Operation Desert Storm.

Picture 16. Patriot missiles[20]

Patriot missiles[21] were first deployed in 1991 but they did not prove to be as good as it had been expected. The upgraded version was deployed in the second Gulf War and some short range missiles could be destroyed with them[22]. Currently the USA is working on a system capable of destruction of long-range missiles.

The further objective is a global weapons system allowing the destruction of a long-range missile at any points of its trajectory. With a new technology this may be possible. A missile defence system based on kinetic energy can destroy a missile in the acceleration stage of its flight directly after launch when the trajectory of a slowly moving missile is calculable, making its destruction easy if the appropriate weapon is at hand. This has been the first missile defence system of the United States since it terminated the treaty on limiting missiles. The system consists of a mobile launch pad, a command vehicle, and a missile interceptor.

[19] E.g.: Col. Michael Leahy, Director, Air Force Research Laboratory

[20] www.spektrumtv.hu 2009. 02. 19.

[21] http://www.globalsecurity.org/space/systems/patriot.htm 2010. 07. 23.

[22] http://hu.wikipedia.org/wiki/MIM%E2%80%93104_Patriot 2010. 09. 11.

Picture 17. Patriot missile defence system[23]

This system is deployable anywhere in a relatively short period of time, within hours. The initially ground-based system can also operate from ships. After the satellite message on the launch of an enemy missile is received the operator launches a missile interceptor which ascends into the upper atmosphere in the first stage, in the second it takes up its position, in the third phase it approaches the ballistic missile near the point of interception, and finally a small kinetic warhead is activated which exploiting its kinetic energy – through its mass and velocity – hits and destroys the target.

Another element of the defence system – SM3 missile – guards seas[24].

Picture 18. RIM-161 Standard Missile 3[25]

[23] http://www.globalsecurity.org/space/systems/patriot.htm 2010. 09. 11.

[24] GlobalSecurity.org: RIM-161 SM-3 (AEGIS Ballistic Missile Defense) http://www.globalsecurity.org/space/systems/sm3.htm 2010. 09. 11.

The ship-based weapon cooperating with AEGIS system destroys short- and medium-range missiles. The ballistic missile defence system includes a communication and sensing system that did not even exist a few years ago. Today information can be forwarded to ships integrated into major systems and the data in the system comprise crucial elements of the operation of individual ships.

AEGIS calculates the launch time and ascent of hostile missiles then identifies the point of interception. An SM3 missile is launched which is in direct radio contact with the ship. The AEGIS guides the missile into space with radio control, where stage 3 launches the warhead which locks on the ballistic missile and destroys it within minutes.

Picture 19. Guides the missile into space[26]

Does this system work? Of course, this is efficient only if it can detect the ballistic missile in the first phase of its flight. This requires sensitive long-range radars. The prototype of the space-based defence system is already operational: the geostationary satellite network conducts permanent surveillance and early warning. Its task is to detect and monitor the launch of hostile missiles, to forward trajectory data to the ground control in order to allow them a timely response. A Cobra Dane radar is deployed on the Aleutian islands. This radar scans space from the Pacific coast to South-East Asia.

Picture 20. Cobra Dane-radar[27]

[25] http://en.wikipedia.org/wiki/RIM-161_Standard_Missile_3 2010. 09. 11.
[26] www.spektrumtv.hu 2009. 02. 19.
[27] http://www.missiledefenseadvocacy.org/web/page/1043/sectionid/557/pagelevel/3/interior.aspx 2010. 09. 11.

In Great Britain an even more modern radar operates with a 360 degree sight over Europe, the Middle East, and the Atlantic. A radar station, commissioned in the 1980s at a California air base, has recently been renovated thus it is capable of detecting and tracking missiles.

Besides the AEGIS system another new device in being tested: a sea-based X-band radar (SBX-1)[28] (GlobalSecurity.org.na), which is able to send precise sensing and tracking data to the ground based missile defence system.

Picture 21. SBX underway[29]

The SBX is 85 metres tall and more than 120 metres long. It weighs 50 thousand tons that is three times heavier than a DDG-1000. It was tested in the waters of Alaska and in the future it will become an important element of the missile defence system. In principle the system operates well but there are some problems. It is extremely expensive, its deployability is disputed, and the results have been limited so far. "For two decades the USA has spent USD 125 billion on missile defence, which is equal with the amount spent on the Apollo program and the landing on the Moon. And how much more is needed for a spectacular result? The course may be wrong. Some say the USA has no edge in the field of missile defence and if a missile was launched at the United States it would not be certain the missile may be destroyed."[30] (MoD, 2002)

Proper missile defence may be a too hard job to do but there is another, potentially more efficient, strategy: the elimination of satellites.

No modern armed forces are able to operate without high-speed communication, data transfer, and satellite-based air surveillance. Therefore, if these devices are knocked out, the activities of the military are paralysed.

During the Cold War both parties tested anti-satellite missiles but there were many warnings that the debris in space may pose a threat to other satellites too. There was a general fear of the militarization of space therefore the American Congress cancelled the program after the Pentagon destroyed an obsolete research satellite in 1985.

---

[28] http://www.globalsecurity.org/space/systems/sbx.htm; http://en.wikipedia.org/wiki/Sea-based_X-band_Radar 2010. 09. 11.

[29] http://missiledefense.wordpress.com/2009/08/ 2010.01. 28.

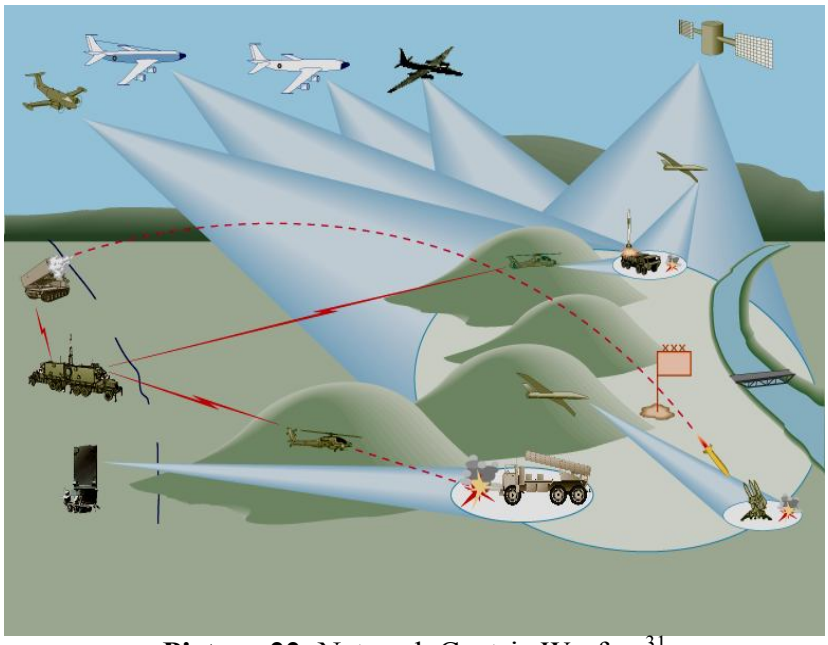
[30] http://www.globalsecurity.org/space/library/report/2002/missiledef.pdf#xml=http://www.globalsecurity.org/cgi-bin/texis.cgi/webinator/search/pdfhi.txt?query=missile+defence+system&pr=default&prox=page&rorder=500&rprox=500&rdfreq=500&rwfreq=500&rlead=500&rdepth=0&sufs=0&order=r&cq=&id=4c8496302a 2010. 09. 11.

Modern anti-satellite weapons use lasers instead of missiles. Satellites are particularly sensitive to laser and there is no need to use a very high-power beam. A medium strength beam is capable of temporarily blinding or permanently damaging optical and infrared sensors. A more powerful laser will destroy the electronics preventing the satellite from exploding and generating a cloud of debris in space.

Smaller lasers can paralyse enemy satellites on the ground or in space. There are serious technical and political barriers but if the international protest fades, these improved weapons may be integrated into the arsenal of future.

Conclusion

One day an enemy attack may be preventable. Combating terrorism requires the development of new weapons, defence systems, and intelligence technologies. This is the only hope for security.



Picture 22. Network Centric Warfare[31]

Is it the new military technologies only that can provide protection in the case of a new conflict?

The present study paper is based on the question whether the above discussed weapons systems are able to combat terrorism and terrorists only. In my opinion these new weapons are perfectly capable of waging a conventional but high-tech armed conflict or even war.

In the following part of the study paper the author will analyse the developments in progress at the services.

[31] www.globalsecurity.org 2010. 04. 05.

BIBLIOGRAPHY

1. Baylis, J. et.al. (szerk.) (2005): A stratégia a modern korban: bevezetés a stratégiai tanulmányokba. -Bp.: Zrínyi Kiadó. (ford.: Meszerics Tamás)

2. Braun László (2005): A magyar katonai erő újszerű alkalmazása a 21. században. =Hadtudomány XV. évf. 2005. 4. szám http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_3.html (2010. 08. 25)

3. Clark, J. (2009): ARO in Review. http://www.arl.army.mil/www/pages/172/aroinreview09_part2.pdf (2010. 05. 29.)

4. Deák János (2005): A katonai műveletek hadászati jellemzői napjainkban. =Hadtudomány XV. évf. 2005. 4. szám http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_6.html (2010. 08. 25)

5. Deák János (2005b): Napjaink és a jövő háborúja =Hadtudomány XV. évf. 2005. 1. szám http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/1/2005_1_3.html (2010. 08. 25)

6. Eisman, D. (2008): Cost and design bugs could sink new destroyer program. The Virginian-Pilot © July 20, 2008 http://hamptonroads.com/2008/07/cost-and-design-bugs-could-sink-new-destroyer-program (2010. 07. 16.)

7. Hamburger, T. et.al. (2001): Human-System Engineering: understanding the process of engineering the human into the system. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA417413&Location=U2&doc=GetTRDoc.pdf (2010. 05. 25.)

8. Hettyey András (2008): Világszerte nőttek a védelmi kiadások. 2008. június 12., csütörtök www.kitekinto.hu http://kitekinto.hu/hatter/2008/06/12/vilagszerte_nttek_a_vedelmi_kiadasok (2009. 09. 11.)

9. Kerekes András (2006): Atombomba, vízháború – miért aggódjunk 2007-ben? 2006.12.28. www.fn.hu http://www.fn.hu/kulfold/20061226/atombomba_vizhaboru_miert_aggodjunk_2007/ (2010. 04. 23.)

10. Kuhn, T. S. (2000): A tudományos forradalmak szerkezete. -Bp.: Osiris Kiadó, -2. bőv. kiad. -ISBN 963 37 93 62 9 (ford.: Bíró Dániel)

11. Lind, W. (et.al.) (1989): A háború változó arculata: a negyedik generáció felé =Military Review, 1989. X. -pp. 22-26.

12. Makk László (2005): A katonai erő alkalmazása a 21. században
=Hadtudomány XV. évf. 2005. 4. szám
http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_9.html (2010. 08. 25)

13. Ministry of Defence (2002): Missile Defence a public discussion
www.globalsecurity.org
http://www.globalsecurity.org/space/library/report/2002/missiledef.pdf#xml=http://www.globalsecurity.org/cgi-bin/texis.cgi/webinator/search/pdfhi.txt?query=missile+defence+system&pr=default&prox=page&rorder=500&rprox=500&rdfreq=500&rwfreq=500&rlead=500&rdepth=0&sufs=0&order=r&cq=&id=4c8496302a (2010. 09. 11.)

14. Molnár István (2005): A jövő háborújáról, fegyveres konfliktusáról
=Hadtudomány XV. évf. 2005. 4. szám
http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_8.html (2010. 08. 25)

15. Nagy Zoltán (2005): A 21. század fegyveres küzdelmeinek irányai és kihívásai a NATO szemszögéből.
=Hadtudomány XV. évf. 2005. 4. szám
http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_4.html (2010. 08. 25)

16. Ormos Mária (2005): A háborúról és a terrorizmusról.
=Hadtudomány XV. évf. 2005. 4. szám
http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_7.html (2010. 08. 25)

17. Pike, J. (2004): Network-Centric Warfare Key to Combat Power in.
http://www.defenselink.mil/news/Jan2004/n01152004_200401151.html (2010. 09.09.)

18. Resperger István (2009): A 21. század fegyveres konfliktusainak hatása a hadtudományra.
=Hadtudomány XIX. évf. 2009. 1-2. szám
http://mhtt.eu/hadtudomany/2009/1_2/003-024.pdf (2010. 08. 25)

19. Ronkovics József (2009): A 21. század hadviselésének néhány főbb jellemzői.
=Hadtudomány XIX. évf. 2009. 1-2. szám
http://mhtt.eu/hadtudomany/2009/1_2/003-024.pdf (2010. 08. 25)

20. Szenes Zoltán (2005): Katonai kihívások a 21. század elején.
=Hadtudomány XV. évf. 2005. 4. szám
http://www.zmne.hu/kulso/mhtt/hadtudomany/2005/4/2005_4_5.html (2010. 08. 25)

21. Szerencsi Ágnes (2008): Háború az Északi-sarkért? 2008. április 8., kedd
www.kitekinto.hu
http://kitekinto.hu/global/2008/04/08/haboru_az_eszaki-sarkert (2009. 12. 01.)

22. Szternák György: A katonai műveletek megvívásának jellemzői napjainkban, levonható következtetések hatása a hadtudomány fejlődésére.
ZMNE Hadtudományi Doktori Iskola Honlapja
http://portal.zmne.hu/portal/page?_pageid=34,17704,34_112973,34_112965&_dad=portal&_schema=PORTAL (2010. 09. 12.)

23. Whelan, D. (2003): Firm envisions high-tech combat. May 01, 2003
http://www.globalsecurity.org/org/news/2003/030501-trans01.htm (2010. 04. 17.)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Réger Béla
reger.bela@zmne.hu

VONALKÓDOS VIZSGAÉRTÉKELÉSI MÓDSZER ALKALMAZÁSÁNAK LEHETŐSÉGEI AZ OKTATÁSBAN

Absztrakt

A szerző a teszt alapú vizsgáztatás vonalkódos újszerű kiértékelési módszerét vizsgálja, tapasztalatai alapján. Az általa kidolgozott megoldás könnyen adaptálható más tantárgyakra is.

The author of the test bar-code-based testing new methods of assessment to examine the basis of experience. It has developed a solution can be easily adapted to other subjects as well.

Kulcsszavak: *vonalkód, vizsga, értékelés ~ bar code, exam, analysis*

Bevezető

Egyetemünk életében nagyon örvendetes, hogy egyre több hallgató választja intézményünket. A korábbi megszokott 10-15-fős osztályok helyett ma már nem ritka a 180-210 fős osztály sem. Ez az új kihívás új módszereket kíván a vizsgáztatás, dolgozatjavítás területén is. Az egyetemi oktató idejét az oktatásra kell fordítani és nem a mechanikus tesztek javítására. Az emberi erőforrás elpazarolása, ha egyetemi tanárok, docensek az alkotó munka helyett a pontok értékelésével és számolásával vannak elfoglalva. Mint Dövényi–Nagy Tamás a feltüntetett forrásirodalomban is megállapítja ez a kihívás nem csak a Zrínyi Miklós Nemzetvédelmi Egyetemet (ZMNE) érinti. Az elektronikus oktatás eszköztárának fokozatos adaptálása az egy vizsgáztatóra jutó hallgatói létszám dinamikus növekedése következtében a hazai felsőoktatás intézményei számára is egyre inkább elkerülhetetlenné válik. Hogy a rendelkezésre álló eszközöknek milyen széles palettáját veszi igénybe egy-egy oktatási egység, az nagyban függ a rendelkezésre álló technikai, személyi feltételektől, valamint az adott tanszékre - főként emberi erőforrás-kihasználtság szempontjából - nehezedő nyomástól. Az utóbbi évek oktatástechnikai, műszaki és számítástechnikai fejlődése mindenesetre megteremtette az egyszerű, olcsó és testreszabott elektronikus oktatás meghonosításának lehetőségét.

A megvalósuló tartalomfejlesztési projektek az e-learning hagyományosan értelmezett oktatási fázisában nyújtanak széles körben elérhető segédeszközöket, ugyanakkor a tanszékek oktatókapacitásának legnagyobb mértékű lekötése éppen a számonkérés fázisában tapasztalható.

1. Az Ötlet

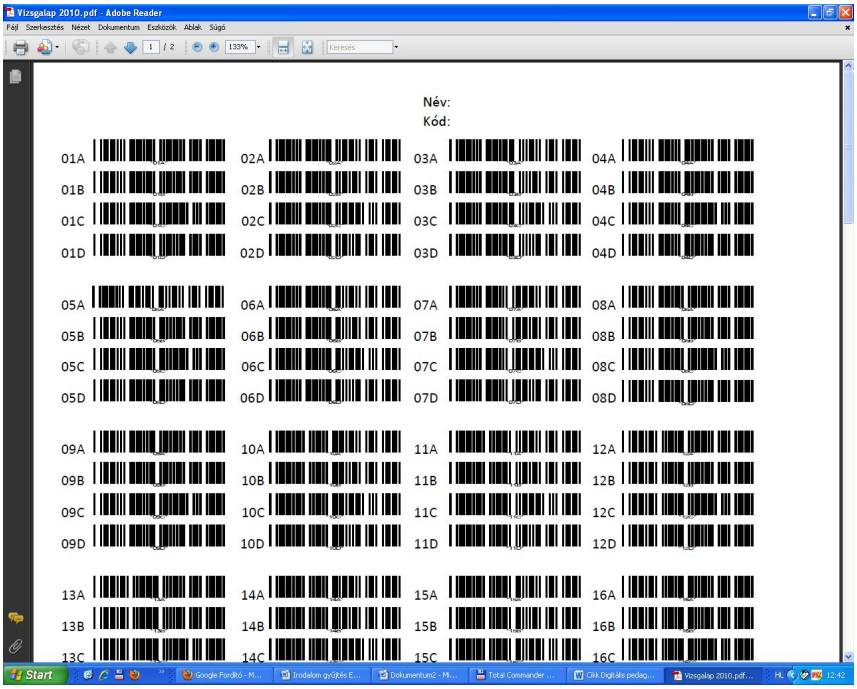
A vizsgáztatás munkacsúcsa a hallgatói létszám dinamikus növekedése következtében egy kritikus vizsgázói létszámon túl elviselhetetlen terheket ró az oktatókra, így egyenesen kikényszeríti, hogy az elektronikus oktatás, vizsgáztatás egyre nagyobb teret nyerjen és akaratlanul is nagyobb figyelmet kapjon. A sokszor kényszer szülte megoldások optimális esetben az oktatás színvonalának és a számonkérés objektivitásának növeléséhez is hozzájárulhatnak.

A hallgató jogos igénye, hogy a dolgozat, vizsga után ne kelljen heteket várni az eredményre. A megoldásnak egy olyan módszer mutatkozott, ami gyors kiválasztós vizsgát tesz lehetővé és vonalkódos programrendszerrel a javítás is gyorsan megoldható.

Nézzük a megoldás menetét:

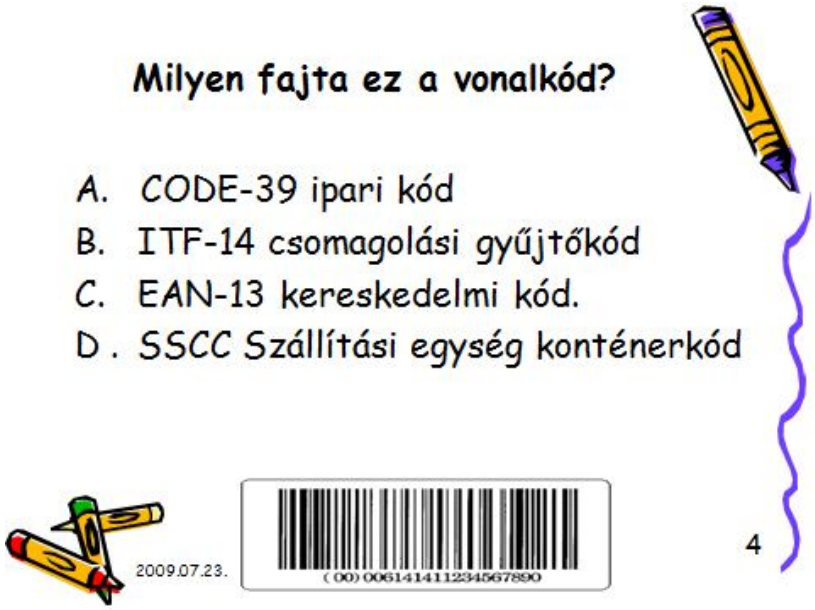
Elkészítettem egy speciális vonalkódos (CODE39) tesztlapot. Az 50 kérdéses lap (elvileg nincs korlát a darabszámra, nekem az 50 kérdés elég egy vizsgánál) egy lap két oldalára került másolásra.

- Egy kérdésre 4 válaszadás lehetséges A-B-C-D. A kiválasztásnál nem csak 1 helyes válasz lehetséges, akár 2-3-4 válasz is jó lehet. Minden találat értékelhető pontot ér. Az úgynevezett TOTO elkerülése érdekében a hibás válasz büntetőponttal kerül értékelésre.



1.sz.ábra. Tesztlap

A vizsgakérdések PowerPoint prezentációval kerül kivetítésre, egy kérdés meghatározott másodpercig. Nálam a 30-50 mp vált be. Ezzel a módszerrel a kinyomtatott akár több oldalas (5-10) tesztlapok megspórólhatók.



2.sz.ábra. Minta vizsgakérdés

A hallgatók kitöltik a tesztet és leadják.

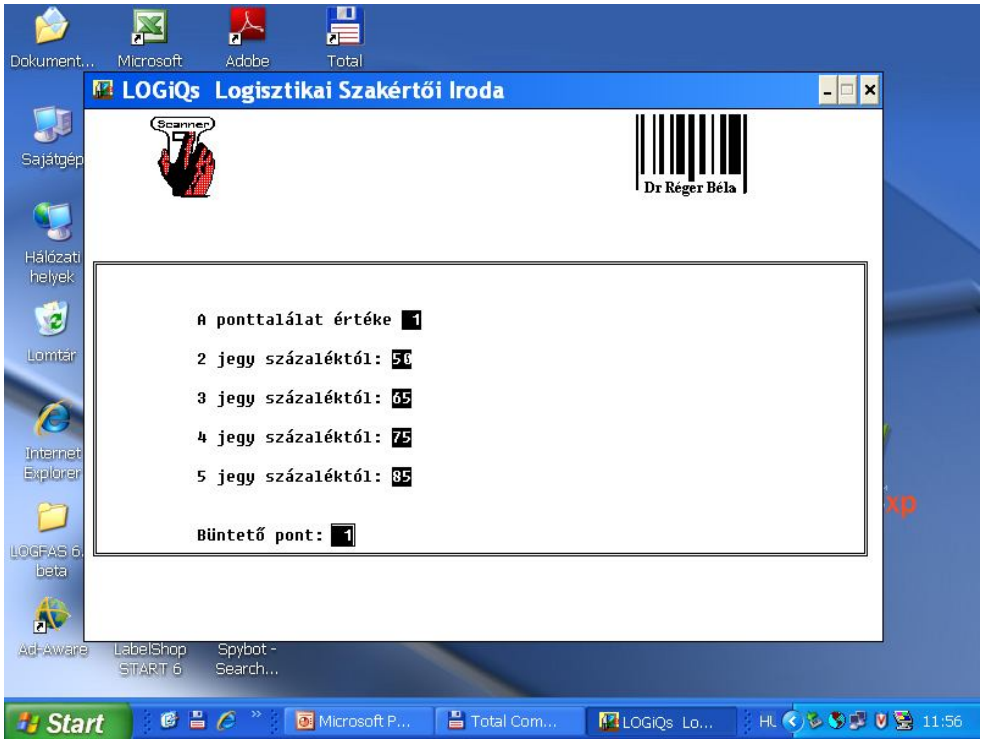
2. A megvalósítás

A kiértékeléshez készítettem egy vizsgakiértékelő programot.

3.sz.ábra. A program nyitóképe

A program 4 főmenüből áll. A harmadik menü „Új tárgy” amikor leürítjük az adatbázist, a negyedik a kilépés ezeket külön nem részletezem.

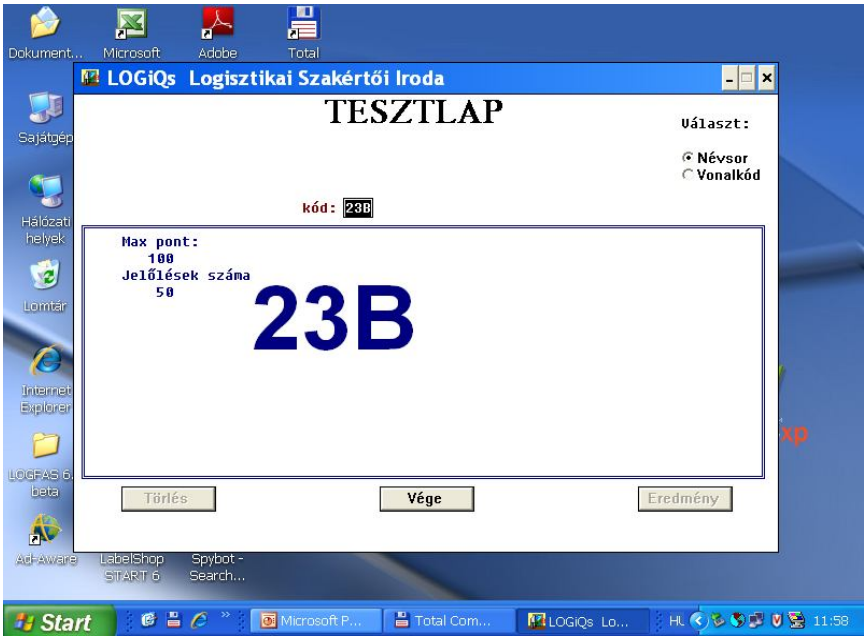
Első lépés a „Tanár” menüpontban a „Tanári változat” rögzítése történik. Először a ponttalálatok értékét állíthatjuk be. Nálam a 2 pont vált be és 1 büntetéspont a helytelen találatért.



4.sz.ábra. Vizsga %-os érték beállítás

A következő lépés az értékelési %-k arányok beállítása történik.

Ezt követi a „Minta tesztlap” rögzítése. A képen látható, hogy ez egy 50 kérdéses, 100 pontos tesztlap. A példánál, a 23. kérdésnél a B válasz az egyik helyes döntés.



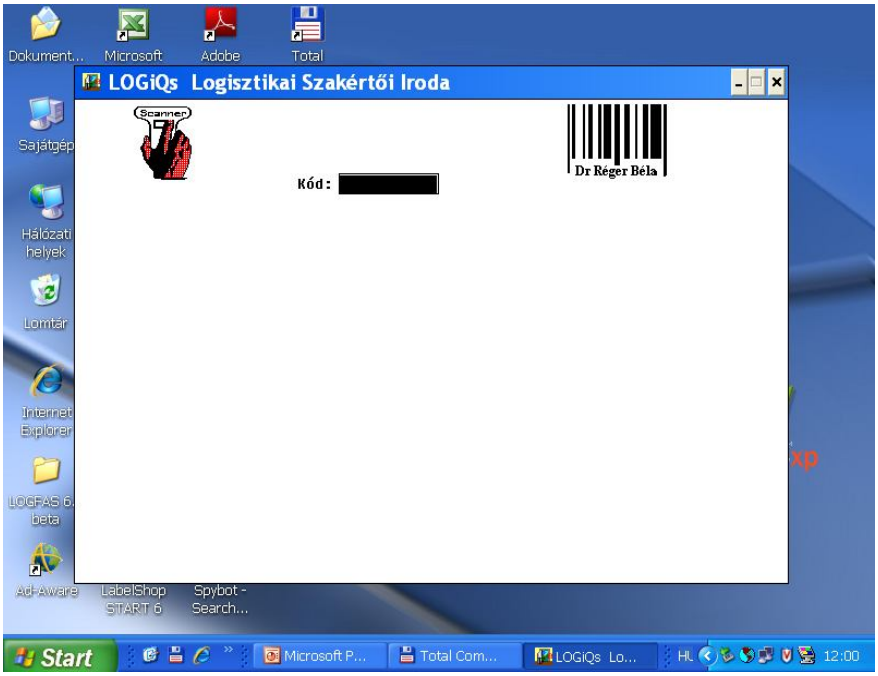
5.sz.ábra. Adatbevitel ellenörzése

Ezek voltak az előkészítés feladatai. Ezek a műveletek már korábban is elvégezhetők. Időszükséglete nálam kb. 5 perc.

Ekkor következik a hallgatói eredménylapok értékelése.

6.sz.ábra. A NEPTUN kód CODE 39 vonalkód képe

A hallgatói azonosításra is bevezettem a Neptun kód vonalkódos változatát. (Nemcsak a Neptun, bármilyen más azonosító is megfelel). Ez az adat kerül az eredménytáblázat tanuló megnevezése oszlopba. Így a hallgatók személyiségi jogai jobban védve vannak, a vizsgáztató elfogultsága kizárt. A logisztika oktatásánál a termékazonosítási vonalkódok a tematikában szerepelnek, így házi feladatként készítik el az azonosítási kártyáikat. Ez nem kötelező más tárgyak esetében, de pl. a ZMNE könyvtári kódkártya vagy a diákigazolvány is tökéletesen megfelel.



7.sz.ábra. NEPTUN kód adatbeviteli képernyő

Ezután történik a tesztlapok feldolgozása. A beolvasott adatok és a pontok változásával a képernyőn folyamatosan látható az eredmény. A vizsgalap beolvasása után az eredmény gomb lenyomásával az Excel által is értelmezhető adatbázis jön létre, ami már szabadon tovább szerkeszthető.

8.sz.ábra. A tesztlap kiértékelés kezdőlapja

Az általam oktatott tantárgynál, 25-30 fő hallgató vizsgáztatása esetén, a vizsga után kb. 1/2 órával megtörténik a kiértékelés. 100 fő fölött ez kb. 2-3 óra.

Az oktatásban általánosan használt technikai eszközökön kívül, a javításhoz egy átlagos CODE-39 kódot olvasni képes vonalkód olvasó szükséges.

9.sz.ábra. Lézeres vonalkód olvasó

A vizsga kiértékelése egyszerre akár több számítógépen is lehetséges, így az idő ennek megfelelően csökkenhet.

Egy másik módszer az alkalmazásra:

A vizsgát egy számítógéppel felszerelt szakkabinetben folytatjuk le. Ebben az esetben a hallgatók a válaszok számkódjait közvetlenül a program alkalmazásával vihetik fel a gépre. Ennek nagy előnye, hogy a hallgató ún. on-line módon látja eredményének alakulását. Az utolsó adatbevitellel a kiértékelés egyből látható.

Felhasznált irodalom

1. Dövényi–Nagy Tamás: Az elektronikus vizsgáztatás tapasztalatai az agrár-felsőoktatásban http://www.agr.unideb.hu/~dovenyi/?c=3 (letöltés 2010. július 8.)
2. Dr. Bernátsky László: Az Elektronikus Vizsgáztatási Rendszer kialakítása, működése az SZTE Egyetemi Könyvtárban http://videotorium.hu/hu/recordings/details/1517,Az_Elektronikus_Vizsgaztatasi_Rendszer_kialakitasa_mukodese_az_SZTE_Egyetemi_Konyvtarban (letöltés 2010. július 8.)

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Szegediné Lengyel Piroska
l.piroska@t-online.hu

ÖTVEN ÉVES A TÁVOKTATÁS?
(PROGRAMOZOTT OKTATÁS ÉS E-LEARNING – PROGRAMOZOTT KÖNYV ÉS E-KÖNYV)

Absztrakt

A tanulmány bemutatja a programozott oktatástól az e-learninghez vezető út fontosabb állomásait, a kétféle oktatás közötti hasonlóságokat, különbözőségeket, párhuzamokat, mindenek előtt a taneszközök, a tankönyvek és a módszertan tükrében. A tanítás és a tanulás munkaeszközeinek fejlődéstörténetét áttekintve, a szerző rámutat arra, hogy az oktatás eszközei egyre többféle pedagógiai tevékenység átvállalására, objektiválására alkalmasak, ugyanakkor a korszerű tanítási-tanulási folyamat nem nélkülözheti a pedagógust. A pedagógus közelibb és emberibb kapcsolatba kerülhet a diákjaival, annak ellenére, hogy a közvetlen „ismeretátadás" helyett a szervezés, az irányítás, a facilitálás, a mentorálás és a megbeszélés feladatait „vállalja magára". Az eszközök sok mindenre képesek, de „megszólítani" nem lehet őket: a tanulók kérdéseire csak a tanár válaszolhat megnyugtatóan.

The study presents the major stations of the road from the programmed instruction to e-learning, the similarities and differences between them, basically in the mirror of the school equipment, the course books and the methodology. Reviewing the phylogeny of teaching and learning equipments, the author points out that the devices of the education are suitable for continually taking over and accomplish more and more kinds of pedagogic activity, however, at the same time the modern teaching-learning process may not miss the educator. The educator can get into a closer and more human contact with his students, it, despite the fact that he takes over the tasks of the organization, the management, the facilitating, the mentoring and the discussion, instead of direct passing over of the knowledge. The devices have got many types of capacities, but they can not be omnipotent, thus the access to the teacher's support will remain a major factor in the learning process.

***Kulcsszavak**: oktatógép, programozott oktatás, számítógép, program, programozott könyv, e-könyv, e-learning, LLL ~ teaching machines, programmed instruction, computer, program, programmed books, e-books, e-learning, LLL*

„Nem sejthetjük meg az emberi agy lehetőségeit kiterjesztő technológia jövőjét, ha nem ismerjük eredetét.”
Howard Rheingold [1]

BEVEZETÉS

Mintegy fél évszázaddal ezelőtt, a hatvanas évek elején jelent meg nálunk az első közlemény, amely hírt adott a programozott oktatásról. A kezdeti hatalmas érdeklődés után azonban szinte egyik napról a másikra, kezdett kimenni a divatból, míg végül teljesen elfelejtettük. De valóban elfelejtettük volna? Vagy „észrevétlenül” újból színre lépett? Az információs társadalom, a „tudástársadalom”, a „LifeLongLearning” életre hívta? Megújult formában – a társadalmi, technikai, technológiai fejlődés szükségszerű velejárójaként – a korszerű oktatás egyik főszereplője lett? A neve távoktatás, e-learning, mobil oktatás…?

A PROGRAMOZOTT OKTATÁS, A TÁVOKTATÁS ÉS AZ E-LEARNING LÉNYEGE

A „programozott oktatás” – a minden bizonnyal sokak számára ismeretlen, vagy szokatlan szókapcsolat – a 60-as években került az érdeklődés középpontjába. A támogatói az oktatás forradalmasíthatóságát látták benne, a kétkedők, pedig negligálni próbálták, arra hivatkozva, hogy felesleges zavar, bizonytalanság keltésével rontja a hagyományos, jól bevált tanítási-, tanulási formák pozícióját, hiszen maga a fogalom is „mondvacsinált”, ezért nem is lehet világosan megfogalmazni, hogy valójában mit takar. A vita igazából nem került ki a szakmai körökön kívülre, így a fogalom sem csapódott le a köztudatban, annak ellenére, hogy az oktatás színterén jelentős változások mentek végbe, ezekben az években.

A szakmai vita során a támogatók ugyanakkor számos definíciót alkottak, illetve pontosították, továbbfejlesztették a korábbiakat. A primer szakmai dialógus mellett, értelemszerűen céljuk volt az oktatáspolitika figyelmét is felkelteni, fokozni a téma iránt. Nem véletlen tehát, hogy a definíciók a piacképesség, a korszerűség, a gyakorlatiasság hangsúlyozása jegyében születtek. Talán sejtették, hogy a programozott oktatás kezdetleges megoldásai a programozottan megírt könyv, az oktatógépes próbálkozások után ölükbe hullik a valódi eszköz, a világháló.

„A programozott oktatás lényege: fogyasztásra előkészített információ. Ez egyszerűen azt jelenti, hogy a tanulásra, ismeretszerzésre szánt könyveket úgy is meg lehet írni, hogy aki olvassa, az megérti, megjegyzi, magában feldolgozza, elsajátítja mindazt, amit a könyv közölni kíván.”.[2]

Ebben az értelmezésben a programozott oktatás azt jelenti, hogy az információt, a tudást egy olyan eszköz (a könyv) segítségével közvetítjük, amely az **önálló ismeretszerzésre,** az **önálló tanulásra** helyezi a hangsúlyt. Az „amit a könyv közölni kíván” kifejezés azt sugallja, hogy a tanulási folyamatban a diák és a tanár közötti kommunikáció a könyvön keresztül zajlik.

Az 1960-as években a pedagógiának ez az új jelensége „programozott” szövegű tankönyvekben öltött testet, amelyek a tananyagot részekre, tanulási egységekre, leckékre bontva adagolták. Minden egység feldolgozása után – esetenként a kitűzött numerikus feladat megoldása után – általában „feleletválasztós” visszacsatolás eredményének függvényében léphetett tovább a tanuló, vagy a lineáris, vagy az elágazásos programozás által kijelölt útvonalon. A programozott tananyagok szinte maguktól követelték meg a gépi feldolgozást. Erre a célra világszerte igen sokféle típusú **oktatógépet** fejlesztettek ki. Magyarországon az első oktatógép a „Magnokorr” (a Budapesti Elektroakusztikai Gyár terméke), amely mágnesszalagra rögzített program alapján álló, majd mozgóképek vetítésével, beszéd kíséretében közvetítette a tananyagot. A látás és hallás utáni kommunikációra épített program a programozott könyv bemutatott funkcióját egyéni és csoportos tanulás esetén is alkalmas volt ellátni.

Az oktatási folyamat tervezésében, irányításában, az ismeretátadás módjában, az ismeretelsajátítás ellenőrzésében is forradalmi változást jelentő programozott oktatás a kezdeti sikerek ellenére sem tudott kibontakozni, tovább fejlődni, aminek szükségszerű velejárója volt a fokozatos háttérbe szorulás, míg végül teljesen kiment a divatból.

Az oktatógépeket felváltó számítógépek megjelenése a 80-as évek elejére tehető, amikor is megjelennek a **számítógéppel támogatott oktatás** csírái, de az igazi áttörésre még további 15 - 20 évet kellett várni. Magyarországon az oktatási kultúra ugrásszerű fejlődését az 1997-ben indult SuliNet program eredményezte, amikor több oktatási intézmény sikeresen pályázott gépparkjának bővítésére és az iskola világhálóra való kapcsolására.

Az Internet megjelenésével és széleskörű felhasználásával merült fel annak lehetősége, hogy a programozott oktatást az Internet útján kellene megvalósítani. Az ötlet kézenfekvő, egyrészt a programozott könyv mintájára, a feldolgozandó konkrét tananyag kerüljön fel az Internetre, legyen elérhető a célközönség, azaz a tanuló számára, másrészt biztosítható virtuális interaktivitás és visszamérés, a feldolgozott tananyag ellenőrzésének eredménye „visszakerülhet” a tanuló számítógépére. Az elképzelésből soha nem látott gyorsasággal bontakozott ki egy újfajta oktatási forma, a **távoktatás,** az **e-learning**, amely mára a számítógépes hálózatok, az Internet térhódítása következtében az egész világon ismert fogalommá vált. „…a huszonegyedik század második évtizedében született meg a számítógép-felhőnek (Cloud Computing) nevezett szolgáltatás. Ennek lényege, hogy az adattárolási és adatmozgatási, valamint a nagy számítástechnikai feladatokat nem a felhasználók saját számítógépe végzi, hanem egy egyszerű internetes böngésző útján ingyenesen, vagy – a saját erőforrások létrehozásánál és üzemeltetésénél lényegesen kisebb – bérleti díjak fejében a számítógépfelhőben működő szolgáltatók biztosítják.” [3]

Az Internet segítségével otthonunkban, saját megszokott környezetünkben, saját időbeosztásunk szerint tanulhatunk, a modern technológiának köszönhetően a távolból lehetőségünk van hozzáférni komplex tananyagokhoz, a legújabb tudományos eredményekhez, részt vehetünk szervezett tanfolyamokon, oktatási kurzusokon.

Desmond Keegen a távoktatás sajátos jegyeit a következőkben határozza meg: „a tanár és a tanulók elkülönülése, a hallgatók közötti kommunikációt és együttműködést biztosító műszaki közvetítőeszköz használata, egy oktatási szervezet fennhatósága.” [4]

A tanár és a tanulók közvetlen kapcsolatának hiánya „távolból történő oktatást” eredményez, és éppen emiatt helyeződik a figyelem középpontjába az ismeretanyag, a

tananyag, az önálló tanulás minden igényét kielégítő, a tanárt helyettesítő taneszköz. Ebben a tanulási környezetben a tananyag nem pusztán a szemlélődés tárgya, hanem a tanulói ismeretszerzés aktív eszköze, amit a tanuló alkotó módon használhat. Ez azonban nem jelenti a tanárközpontú oktatási modell háttérbe szorulását. Sőt éppen ellenkezőleg! A tanári szerepkör felértékelődik, megújul, új dimenzióban jelenik meg. A tanár az oktatási folyamat minden szintjén jelen van, az önálló tanulást pedagógiailag, didaktikailag jól felépített tananyaggal irányítja, olyan tanulási környezetet alakít ki, amely felkelti az érdeklődést, motivál, amely a tanulói aktivitásra épül. A tananyagkészítés kihívás a pedagógus számára: vizsgázik szakmai ismeretből, módszertanból, kreativitásból, pedagógiából. A távoktatásra szánt tananyag motiváló ereje attól függ, hogy a tananyagkészítőnek sikerül-e szakmailag kifogástalan, kivitelezésében ötletes, látványos innovatív technológiai megoldásokat találnia, hogy a multimédia eszköztára segítségével a sorok között rejlő fontos információkat, összefüggéseket közvetíteni tudja-e a tanuló felé.

A távoktatás, a távolból nyújtott oktatási és képzési szolgáltatás, megvalósulhat a világháló segítségével is, ami az e-tanítást és tanulást jelenti. Az e-learning lényege tehát: egyfajta, az Internet támogatta távoktatás, a világhálón nyújtott oktatási és képzési szolgáltatás, amely az önálló tanulásra, az önálló információfeldolgozásra gondosan előkészített kurzusanyag alapján folyik.

Programozott oktatás vagy távoktatás, e-learning? A cél ugyanaz: a tanulók önálló ismeretszerzésének irányítása, egy tanulásra előkészített, szakmailag és módszertanilag átgondolt, lépésről-lépésre megtervezett programmal. A program olyan tankönyv, amelyből önállóan, tanári irányítás nélkül is, hatékonyan lehet tanulni. A programozott könyveket nem olvassuk, hanem feldolgozzuk, ami már tanulást jelent. A program tehát feldolgozásra előkészített tananyag, olyan tananyag, amely kisebb egységekre van tagolva, mindegyik egység feladatot ad, kérdést tesz fel a tanulónak, és gondoskodik arról, hogy a tanuló a megoldása eredményéről azonnal visszajelzést kapjon.

A HAGYOMÁNYOS TANKÖNYVTŐL A PROGRAMIG, AZ E-KÖNYVIG VEZETŐ ÚT

A tankönyvek csoportosítása, tipizálása, a tankönyvmodellek leírása többféle szempontrendszer, nézőpont szerint történhet. Jelen tanulmányban a tankönyvtípusokat a tankönyvi szerepvállalás, a funkciódominancia [4] alapján különböztetem meg.

Az ismeretek (információk) tárolását és közlését szolgáló **hagyományos vagy leíró jellegű tankönyvek** alapvető funkciója az információáramoltatás, amelyben a tankönyv jelenti az informátort, a közlőt, a tudás birtokosát és átadóját, a tanuló, pedig a „felvevőt”, az ismereteket átvevő, passzív befogadót. Az ilyen tankönyv készítőinek az a céljuk, hogy könyvük megbízható, sokrétű, érthető és megtanulható ismeretanyagot nyújtson. Ezt a tankönyvtípust képviselik a tanári közreműködést igénylő **információtároló, vagy leíró jellegű tankönyvek**, amelyekben az ismeretek összegyűjtése és rendszerezett tárolása dominál, viszonylag kevés a magyarázat, a magyarázó szemléltetés, vagy az **információátadó, vagy közlő típusú tankönyvek**, amelyekben dominál a képes (szemléltető) vagy a verbális magyarázat, illetve a kettő kombinációja. Az ilyen típusú tankönyvekben az információáramoltatás egyirányú, a tanulási folyamatban a tankönyv jelenti a tudást, a tanuló feladata, hogy megértse és megtanulja annak tartalmát.

A tananyagot feldolgoztató, munkáltató tankönyvtípus kategóriába a készségfejlesztésre törekvő tankönyvek tartoznak, amelyekben a transzformációs szerepek, a gyakorlati alkalmazás, a gyakorlás dominálnak. Az ismeretek tárolása és puszta közlése helyett az ilyen tankönyvek fokozott tanulói aktivitásra építenek, az ismeretek „betanulásán" túl azok aktív, kreatív elsajátítására, gyakorlati alkalmazására, a készségek, képességek fejlesztésére. Ezek a könyvek a tanulót kérdések feltevésére, megválaszolására, feladatmegoldásra, kísérletezésre stb. késztetik. Alapvető cél, hogy a tanulók a mérhetetlen tudásanyag forrásait, azok kiaknázásának készségeit, illetve bizonyos alapkészségek biztonságos gyakorlatát sajátítsák el. Ebben a csoportban főleg **munkáltató elemeket tartalmazó hagyományos tankönyveket** (közlő, leíró jellegű tankönyvek, kérdésekkel, feladatokkal, kísérlet-leírásokkal, de a tankönyv egészének leíró, közlő, hagyományos jellege nem kérdőjelezhető meg), illetve **munkáltató modulokat** (munkafüzetek, feladatlapok stb.) **tartalmazó tankönyveket** találunk.

A munkáltató tankönyvek elterjedése a 70-es években következett be, amikor szinte „kötelező" volt a tankönyvekben munkáltatni. Bár a „munkáltatási láz" az idők folyamán visszaszorult, de jól bevált elemei, előnyei az ezredforduló tankönyveiben is fennmaradtak, együtt élnek más, különböző módszertani elemekkel, s így egymást célszerűen kiegészítve számos didaktikai funkciót töltenek be. Ráirányítják a figyelmet a mondanivalóra, a „megtanulandóra", megfigyelésre késztetnek, koncentrációt teremtenek az egyes tananyagrészek között, illetve más tantárgyak anyagával, összefüggésbe hozzák az elméleti ismereteket a gyakorlattal, az ismeretek felújítására késztetnek; segítik a rendszerezést, az ismétlést, gyakoroltatnak, további ismeretszerzési lehetőségek forrásaira utalnak.

Ha a munkáltatás magában a tankönyvben, és nem annak kiegészítő mellékleteiben valósul meg, akkor **munkatankönyvről** beszélhetünk. A módszer szükségszerűen megkívánja, hogy a tankönyvbe írjanak, rajzoljanak a tanulók, ami a tankönyvek többszöri használatát, gazdaságos megjelentetését korlátozza. Bár jelenleg az oktatásnak csak néhány szegmensében (pl. gyógypedagógia) használják sikeresen ezt a módszert, prognosztizálható, hogy a munkatankönyvek kora nem járt le, éppen ellenkezőleg, a közeljövőben kezdődik. Mindez arra alapozható, hogy a számítógépek térhódításával egyre inkább gyarapodó **„elektronikus" tankönyvek** a tanulók aktív közreműködésére építenek: a beleírása, a belerajzolása, különféle kiemelési, formázási lehetőségekre

Programozott tankönyvek sajátos típust képviselnek a tankönyvek családjában. Erőteljes bennük a tankönyvkészítő általi vezérlés és a tanulók önálló munkája. A programozás zárt rendszerekbe, kötött utakra készteti a tanulókat, mégis épít aktivitásukra, tevékeny, önálló munkájukra. A programozott tankönyveket alapvetően az különbözteti meg a hagyományos tankönyvektől, hogy míg a hagyományos tankönyv csak lehetővé teszi a tanulónak a tanulást, addig a programozott könyv irányítja az önálló ismeretszerzést, miközben megtanítja a tanulóval a hatékony tanulás metodikáját is, megtanítja a tanulót helyesen tanulni. A programozott oktatás előnye, hogy erőteljes egyéni munkára épít, aktivizál, így valószínűleg tartósabb ismereteket és készségeket alakíthat ki, hátránya az emberi, pedagógusi közreműködés minimalizálása, az egyirányúság, a gondolati merevség.

A programozott tankönyv legújabb definíciója a Pedagógiai lexikonban, Tóthné Köröspataki Kiss Ágnes megfogalmazásában: „A programozott tankönyv a tananyagot önálló tanulásra alkalmas formában tartalmazza. A tananyag megtanulása az előre megtervezett programlépések feldolgozása útján valósul meg. A programozott tankönyvben az előrehaladás nem folyamatos lapszámozást követ, mert a lépések egymásutánja a

kérdésekre várható egyéni válaszadástól függ. A program megtervezésének első mozzanata a tanulók kezdeti tudásszintjének tisztázása és a tanulási cél meghatározása. Ezután a tanulási célnak megfelelően kiválasztott és elrendezett tananyag elemzése következik. A tananyagelemekből felépített algoritmus a programlépések menetét írja le. A program algoritmusa már a kívánt pedagógiai feladatok (kikötések, sorrendi variációk stb.) alapján nyújt a programozáshoz kiindulást. A pedagógiai céloktól függően a tananyag ismereteket feldolgozó lépéseihez problémafölvető, gyakorló, ellenőrző stb. kérdések, feladatok kapcsolódhatnak." [6]

A programozott tankönyvek különböző típusai pedagógiai szempontból alapvetően az alkalmazott programozási eljárás tekintetében különböznek egymástól. A **lineáris programozási eljárással –** Skinner módszer **–** készített tankönyvek ésszerűen irányítják a tanulók tanulási folyamatát igenlő válaszaik megerősítésével, míg az **elágazásos programozási szisztéma –** Crowder módszer **–** a helyes felelet után továbbvezeti, hibás válasz esetén viszont különböző feladatokkal, gyakorlatokkal, szemléltető ábrákkal stb. segíti a tanulót. Egyes programok az elkövetett hibák elhárításához kiegészítő magyarázatokat, útmutatásokat, kérdéseket adnak a tanulóknak. [2]

A program szigorúan szabályozza a tanulási folyamatot, annak műveleteit, de csak akkor lesz hatékonyabb a hagyományos tanulásnál, ha a műveleteket a legcélravezetőbb módon választották meg és végzik el a tanulók. A programozott oktatással szemben igen gyakran megfogalmazott kritika, **–** hogy elnyomja a tanulók intellektuális aktivitását, leszoktatja őket a kreatív gondolkodásról, cselekvésről, mivel folyton csak a feladatsor kérdéseire kell válaszolniuk **–** reálisnak tűnhet. Ezt a gyengeséget próbálják kiküszöbölni a **panorámatankönyvek,** amelyek sajátos jellemzője az eltérő megoldási útvonalak felsorakoztatása. A tankönyvek a választható forrásokat, szemelvényeket, az ellentétes nézeteket tényszerűen ismertetik, a tanuló dönt a haladási irányról. Az alapelv, miszerint az önállóan, fáradságos mérlegeléssel kialakított meggyőződés értékesebb, tartósabb, mint a „betanult", igazolódva látszott, az ilyen típusú könyvek fejlesztése a kezdeti kísérleti fázison mégsem jutott túl.

A programozott tankönyvek a program közvetítésének csak egyik lehetséges változatai, hiszen a programot, a tanulmányi anyag feldolgozását többféle technikával is lehet közvetíteni: oktatógépekkel, filmszalagon, diavetítővel, modern korunkban, pedig audiovizuális eszközökkel, számítógépekkel, számítógépes hálózatokkal.

Mai korunk modern tankönyvei az **audiovizuális elemekkel kiegészített tankönyvek**, illetve az **elektronikus tankönyvek** vagy a **számítógépes kiegészítésekkel élő tankönyvek.** Ma már egyes tudományterületeken – nyelvészet, építészet, hadtudományok… – igazán modern könyvek alig képzelhetők el audiovizuális elemek, hangkazetták, CD-ROM-ok, videoklipek, számítógépes programok szatellitjei nélkül. Az elektronikus, a számítógépes kiegészítésekkel élő tankönyvek számítógépes úton, például Interneten válnak hozzáférhetővé. A számítógépes program nemcsak kiegészíti, élőbbé teszi a könyv szövegét, hanem könnyen és tartósan érthetővé, jól tanulhatóvá is varázsolja a tananyagot.

Természetesen mindenfajta könyv elindíthat egyfajta gondolatcserét az olvasó és a tartalom között, de a programozott könyvekben ez a lehetőség szerkesztési elvként jelenik meg: a tartalom, a mondanivaló elvárja az olvasó válaszát és a válaszra reagálva halad tovább. A program tehát a „párbeszédes tanulás" eszköze, amely **–** tanuló és könyv közötti **–** párbeszéd szigorú rendet követ, lépésről lépésre halad az egyszerűtől a bonyolultabb

ismeretek felé. Ez a párbeszéd „barátságos” hangvételű, világos, minden mozzanata érthető, felkelti, éleszti, ébren tartja a figyelmet, úgy képes vezetni a tanulót, hogy ő saját maga, tapasztalati úton találja meg a probléma megoldását, hogy örömforrásként élje meg a tanulás folyamatát.

Összegezve elmondhatjuk, hogy a technikai fejlődés, megújítás szempontjából a programozott tankönyvek sikeresek és eredményesek, de a könyvet megújító találmány mégsem az egyik, vagy másik technika, hanem a technikában érvényesülő elv: a befogadás számára előkészített tartalom és annak állandó kísérője, a módszertan. Amennyiben az audiovizuális elemekkel kiegészített tankönyvek, az elektronikus tankönyvek megfelelnek az említett követelményeknek, akkor azokat a mai kor programozott könyveinek tekinthetjük.

A PROGRAMOZOTT OKTATÁS PEDAGÓGIAI ÉS DIDAKTIKAI ELVEI

Burrhus Frederic Skinner a Harward Egyetem pszichológia tanára, a programozott oktatás „úttörője” „A tanulás tudománya és a tanulás művészete” című munkájában a sikeres tanulásról így vélekedik: „Valószínűnek látszik, hogy a tudomány technológiai alkalmazásának éppen a pedagógia a legfontosabb területe, hiszen az oktatásnak minden ember életében igen nagy jelentősége van. Az oktatás követelményeinek ma már nem tehetünk eleget anélkül, hogy fel ne használnánk azokat az óriási lehetőségeket, amelyeket a tudományosan megalapozott technika kínál.” [7]

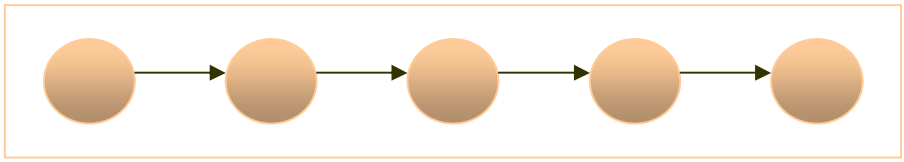
Bár a „tudományosan megalapozott technika” óriási lehetőségeinek csak a kezdetét képviseli a Skinner által kifejlesztett és a tanulmányában bemutatott oktatógép, igazi érdeme, hogy alkalmat ad azoknak a tanulási elveknek a megvalósítására, amelyek véleményem szerint, a mai pedagógiai gyakorlatban is meghatározó erőt képviselnek. Ezek az elvek a következők: a géppel dolgozó tanuló saját tanulási ütemében, lassabban vagy gyorsabban haladhat előre, lépésről-lépésre feladatokat old meg, a helyes választ azonnal megerősítés követi, a tanulók hibáinak tapasztalataiból okulva többször is módosítani lehet a feladatokat, annak érdekében, hogy az átlagos képességű tanuló is a feladatok többségére hibátlanul válaszoljon.

Skinner a legfontosabb elvet így fogalmazza meg: „Ez az eszköz lehetővé teszi, hogy a tanulóknak gondosan megtervezett tanulmányi anyagot adjunk, amelyben minden egyes probléma az előző kérdés helyes megfogalmazására épül, tehát eredményes haladást biztosíthatunk az egyszerűtől a bonyolult felé vezető úton.”[7]

A Skinner-féle tanuláselméletből még egy nagyon fontos, az önálló tanulási folyamat sikerességét döntően meghatározó nézetet kell kiemelnünk, a „viselkedés-kondicionálást”, amelynek értelmében azok a mozdulatok, cselekvések, viselkedésmódok ismétlődnek meg és válnak tartósan elsajátított, megtanult viselkedésformává, amelyet valamilyen jutalom, elismerés, siker megerősít.

Skinner elmélete és programkészítési gyakorlata heves vitát indított el a pedagógia történetében, olyan éles kritikák is fogalmazódtak meg, hogy a program nem gondolkoztat, figyelmen kívül hagyja a tanuló szellemi képességeit, kizárólag a mechanikus tanulást, a tények emlékezetbe vésését segíti elő, megakadályozza a tanulót abban, hogy felfedezze az alapvető elveket. Sokan úgy vélekedtek, hogy a programozott oktatás gépies és egyhangú,

örömtelen és lélektelen módja a tanulásnak, míg mások egyenesen idomításnak nevezték, aminek semmi köze az igazi aktív tanuláshoz.



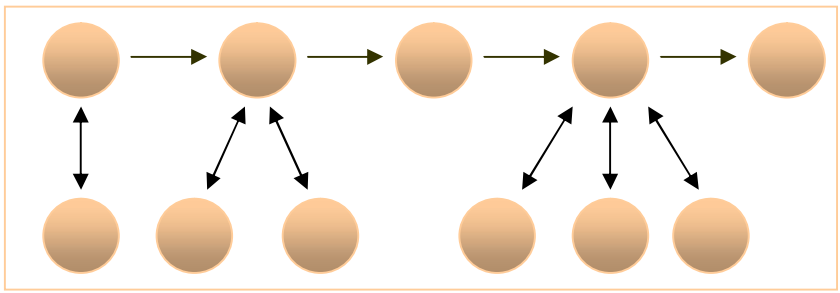
1. ábra. A Skinner–féle lineáris program vázlata [2] (Saját szerkesztés)

Élesen bírálta Skinner lineáris programját Norman A. Crowder, a U.S. Industries oktatási osztályának akkori vezetője, s érvként, „válaszként" bemutatta a „Tutor" típusú oktatógéppel közvetített, Tutor text-nek nevezett, tankönyvek formájában kidolgozott **elágazó programját**.[2]

De vajon miben tér el egymástól a lineáris és az elágazásos program elméleti megalapozása és pedagógiai elvei?

Az elágazásos program lényege, hogy a tananyag egy-egy kisebb szakasza, leckéje után egy kérdést intéz a tanulóhoz, amelyre feleletválasztással válaszolhat, tehát több felkínált válasz közül választja ki a szerinte helyeset. Amennyiben a válasz helyes, a program a következő, új ismereteket közlő leckéhez irányítja a tanulót, míg hibás válasz esetén a tévedés okára rámutató magyarázathoz vezérli, és addig nem engedi a továbblépést, amíg a meghatározott követelményszintet nem teljesíti.

Az elágazásos program tekintetbe veszi a tanulók közötti különbségeket, motivál, „jutalmaz" és „orvosol", hiszen egy-egy lecke egy-egy mérföldkövet jelent a tanulási folyamatban, amelynek a teljesítése a továbbhaladást, a fejlődést jelenti, nem teljesítés esetén viszont csak a hibákkal való szembesülés és a korrigálás után van lehetőség a továbblépésre. A program érdeme tehát a diagnózisban rejlik: a tanuló hiányosságaira rámutat, majd azokat a hiányosságokat használja fel a következő lépésben az orvoslásra.



2. ábra.A Crowder-féle elágazásos program egy lehetséges változata [2] (saját szerkesztés)

Hogy a lineáris és elágazó programok közötti különbségeket a tanuló szempontjából is megítélhessük, nézzük meg, hogy „nézne/nézhetne ki" egy programozott tankönyvben egy igen egyszerű **számviteli ismeretek lecke** a kétféle program nyelvén.

Számviteli ismeretek lecke bemutatása lineáris programozással programozott tankönyvben

Programozott tankönyv 1. lecke A számviteli mérleg	1. A számviteli mérleg kétoldalú kimutatás, amelynek (**a bal / a jobb** oldalán találhatók az eszközök. a bal	2. A mérlegben a tartós eszközök neve **(befektetett eszközök/forgóeszközök)** befektetett eszközök
3. A saját tőke egyik csoportja **(a jegyzett tőke/ a pénzeszközök**) a jegyzett tőke	4. A készletek a vállalkozás **(befektetett eszközei / forgóeszközei**) forgó-eszközei	5. A mérleg szerinti eredmény **(adózott eredmény / adózatlan eredmény)** adózott eredmény

3. ábra. Számvitel lecke a lineáris program elve alapján [8] (saját szerkesztés)

A helyes válaszok „elrejtését” a könyvhöz mellékelt takaró lap biztosította, s miután a tanuló beírta a válaszát, a takarólap felemelésével láthatóvá vált a helyes válasz.

Számviteli ismeretek lecke bemutatása a legegyszerűbb elágazásos programozással programozott tankönyvben

Programozott tankönyv **1. lecke** A számviteli mérleg	**1/A** Számviteli mérleg kétoldalú kimutatás, amelynek **a bal** oldalán találhatók az eszközök. **IGEN 2/A** **NEM 1/B**	1/**B** **Válasza hibás!** Az eszközök a vállalkozás vagyonát jelentik megjelenési forma szerint. Az eszközöket aktíváknak is nevezzük. Az aktívák a mérleg bal oldalán találhatók. **Térjen vissza az 1/A oldalra és válaszoljon újra**	**2/A** **Válasza helyes!** Következő állítás. A mérlegben a tartós eszközök neve **befektetett eszközök** **IGEN 3/A** **NEM 2/B**
2/B **Válasza hibás!** A befektetett eszközök neve arra utal, hogy tartósan, egy éven túl szolgálják a vállalkozási tevékenységet **Térjen vissza a 2/A oldalra és válaszoljon újra!**	**3/A** **Válasza helyes**! Következő állítás: A saját tőke egyik csoportja a jegyzett tőke **IGEN 4/A** **NEM 4/B**	**3/B** **Válasza hibás!** A készleteket – például árukat, késztermékeket – a vállalkozás, értékesítési céllal szerzi be, illetve állítja elő. . **Térjen vissza a 4/A oldalra és válaszoljon újra!**	**4/A** **Válasza helyes!** Következő állítás: A készletek a vállalkozás forgóeszközei **IGEN 5/A** **NEM 3/B**
4/B **Válasza hibás!** A jegyzett tőke a vállalkozás cégbíróságon bejegyzett tőkéje, megalakuláskor összege a saját tőkét jelenti. **Térjen vissza a 3/A oldalra és válaszoljon újra!**	**5/A** **Válasza helyes!** Következő kérdés: A mérleg szerinti eredmény adózott eredmény **IGEN 6/B** **NEM 5/B**	**5/B** **Válasza hibás!** A mérleg szerinti eredmény a vállalkozás tiszta eredménye, amelyet az adózott eredményből az osztalék kifizetése után kapott meg. **Térjen vissza az 5/A oldalra és válaszoljon újra!**	**6/A**

4. ábra. Számvitel lecke az elágazásos program elve alapján [8] (Saját szerkesztés)

Skinner pedagógiai felfogása szerint, a lineáris programokat úgy kell szerkeszteni, hogy a tanulók többsége általában helyesen válaszoljon, sikerélményhez jusson. Mindenkinek minden lépésen végig kell haladnia, egyéni üteme szerint. Bírálói szerint a lineáris program mechanikus, a gondolkodást nem fejleszti, csak az emlékezetre épít.

Crowder feltételezte, hogy a hibás válaszok (negatív megerősítéssel is) aktivizálják a tanulót. Nagyobb egységekre bontotta a tananyagot, a feltett kérdésre több megadott felelet közül kellett a tanulónak választania. A helyes feleletet választó a főágon (rövidebb úton) haladhatott végig, a hibásan válaszoló kiegészítő információt (magyarázat, kiegészítés) kapott, tehát mellékágon, hosszabb idő alatt jutott célba. Technikailag ezt ún. „kevert lapú" programozott tankönyvekkel oldották meg, később erre épültek a feleletválasztásos oktatógépek. Bírálói szerint az elágazásos oktatóprogram hibája, hogy a helytelen válaszok is rögzülhetnek a tanulóban, a helyes feleletválasztás véletlen is lehet, a választható feleletek számától függően 25-50 %-os a „találati valószínűség".

A számítástechnika rohamos fejlődése életre hívta a **taneszközök legújabb generációját,** amelyek interaktív kapcsolatot tudnak megvalósítani a tanuló és a számítógép között. Ebben a kapcsolatban a számítógép programjaival és kiterjedt hálózati struktúrájával olyan interaktív tanulási környezetet teremt, amely egyidejűleg több emberi érzékszervre irányul, és műveletvégzésre késztet Ebben a tanulási környezetnek a „főszereplői" a korszerű oktatástechnikai- és információhordozó eszközök, mindenekelőtt az **Internet.** Az Internet ugyanis egyedülálló módon teszi lehetővé az ún. many to many kommunikációt, ráadásul időben és térben aszinkron módon, ami elsőrendű lehetőség a nyilvánosság és a közösségépítés számára. [9]

AZ E-LEARNING PEDAGÓGIAI ÉS DIDAKTIKAI ELVEI

Az elektronikus tanulást „**új irányzat"-**nak nevezhetjük az oktatás palettáján, annak ellenére, hogy egyes elemeiben a hagyományos tanulást viszi tovább (bár radikálisan más felfogás szerint), illetve annak ellenére, hogy a programozott oktatás meghatározó jegyeit hordozza.

Az új irányzat újfajta tanulási helyzetet, újfajta tanulási környezetet teremt, a tananyagok előállításának újfajta szempontjait és módszereit hívja életre, olyan modern oktatástechnológiai és pedagógiai módszertanra épül, amelynek életfeltételét jelentik az informatika és a telekommunikáció vívmányai.

Az e-learning fejlesztéseket, programokat, tananyagokat jelent a tanulás szervezésére, irányítására és támogatására. Komplex rendszer, amelynek célja, hogy a technika fejlettsége folytán hatékonyabb, célirányosabb legyen a tanulás, gyorsabb az információszerzés és az információcsere és a folyamatok könnyen ellenőrizhetőek legyenek. A virtuális környezet megteremtésére szolgáló keretrendszerek számos változata jelent meg az utóbbi években, (Moodle, ILIAS, Oracle-iLearning, stb.), amelyek között a legnépszerűbbek, legelterjedtebbek azok, amelyek leginkább képesek támogatni a pedagógiai elvek érvényesülését, illetve amelyik „az összes adminisztráció, tananyag-elhelyezési és -hozzáférési, levelezési, feladatbeküldési és értékelési, hirdetőtábla stb. funkciót biztosítja." [10]

A Moodle dinamikus fejlődésének, elterjedésének magyarázata a könnyű használhatóság a telepítéstől a közösségi életig. [11] Az utóbbi években a legkülönbözőbb kurzusok – informatika, számviteli ismeretek, adózási ismeretek – jelentek meg a Moodle közvetítésével

felsőoktatásban résztvevő hallgatók számára, amelyek a hallgatói elégedettség mérése alapján jelesre vizsgáztak.

http://www.lengyelpiroska.hu/Oktatas.html [12]

http://forika.hu/moodle/ [13]

http://miskolczi.net/moodle/[14]

Az e-learning alkalmazások során egyre gyakrabban kerül előtérbe a pedagógiailag helyes tananyag kérdése, illetve az e-learning eszközrendszerének pedagógiailag releváns alkalmazása. A keretrendszertől való függés miatt az e-learninges tananyagok készítése sokkal összetettebb, mint a programozott tananyagoké. Nem elég csak digitalizálni a tananyagot és valamilyen formában a tanulókhoz juttatni, nem elég csak megteremteni „a kis lépések, az aktív válaszadás, az azonnali megerősítés, az egyéni ütem, a teljesítmények kiszolgálása elvek" [7] feltételeinek érvényesülését. Meg kell teremteni a folyamatos rendelkezésre állást, a megfelelő interaktivitást, amely elég rugalmas, hogy szinte minden tanulónak megfelelő választ és világos, egyértelmű anyagokat adjon, és meg kell teremteni a megfelelő hátteret és terveket a működéséhez. A legfontosabb kérdés, hogy milyen eszközrendszert biztosít egy-egy keretrendszer a tanár számára, hogy milyen formátumban képes megjeleníteni a tananyagot, hogyan támogatja a tananyag feldolgozását, milyen kollaborációs eszközöket biztosít ehhez.

A rendszerek meghatározó komponensei az oktatást lebonyolító rendszer és a tartalommenedzsment rendszer, amelyek a képzés, a kurzus és a tananyagok hármas egységében működnek, ellátva speciális adminisztratív, kommunikációs, csoportmunka és vizsgáztatási funkciókat. A rendszer két komponense között a kapcsolatot a **tananyag** teremti meg, amely a képzés legfontosabb kommunikációs eszköze, a tanuló iránytűje, motivátora, motorja a tanulási folyamatban, az ismeret, a tudás megtestesítője, a tanárt képviselő, a tanárt „helyettesítő" taneszköz.

A továbbiakban az e-learning pedagógiai és didaktikai módszertanát a tananyag szemszögéből próbálom meg értelmezni, összevetve azt a programozott oktatás módszertani

gyakorlatával, illetve utalva azokra a módszertani megoldásokra, amelyeket e-tanulásra fejlesztett számviteli ismeretek elektronikus könyveimben is alkalmazok.

Az e-learninges tananyagok legfontosabb ismérve és érdeme a moduláris rendszerű felépítés, amely a programozott tananyagban alkalmazott „kis lépések elvnek" a korszerűbb változata**.** A **modulrendszerű tananyag** azt jelenti, hogy az elsajátítandó tananyag önálló egységekre van bontva, ami jellemzően egy-egy tanulási alkalomra elegendő tananyag-mennyiség, amelyet a tanulók, a saját lehetőségeik és igényeik alapján megfelelő időben sajátíthatnak el. A rendszer nemcsak egy-egy modulon belül ad nagyobb szabadságot a tanulónak – természetesen a szabadságot az ismeretanyag specifikus jellege időnként korlátozhatja –, hanem az egyes modulok közötti választásban, kombinálásban is, azáltal, hogy a modulok közötti kapcsolatot, az átjárhatóságot biztosítja. Az ismeretanyag modulrendszerű felépítése kiküszöböli a felesleges tananyag-ismétlődéseket egy kurzuson belül, szerves egységgé kapcsolja a kurzus tantárgyi elemeit, segíti a globális gondolkodást, a rendszerszemlélet kialakítását.

A szokásostól eltérő tanulási folyamat tananyagaival szemben fontos elvárás, hogy folyamatosan támogassák a tanulót, hogy biztosítsák a folyamatos visszacsatolást és a teljesítményértékelést, hogy „tanulóra szabottak" legyenek. A tanulóközpontú e-learning tananyagai csak akkor képesek megfelelni a tanulói igényeknek, ha figyelembe veszik a tanulói különbözőségeket, az egyes tanulók eltérő tanulási stílusjegyeit. A tananyagoknak olyan tartalommal kell rendelkezniük, olyan – a tanulási stílusokat figyelembe vevő – módszertani megoldásokat kell tartalmizniuk, amelyek sikerélményhez juttatják a tanulót, motiválják a tovább lépésben, az előre haladásban. Az e-tananyagok előnye a hagyományos, illetve programozott tankönyvekkel szemben a mobilitás, hogy a folyamatosan változó/változható tanulói preferenciák – vizuális, auditív, kinesztetikus tanulási stílus – függvényében, módszertani elemei folyamatosan bővíthetők, változtathatók.

Az e-tananyagok korszerű, a tudástársadalom, a LLL elvárásainak megfelelő olyan pedagógiai elvek megvalósítását teszik lehetővé, – mint, például a tapasztalati úton való ismeretszerzés, a problémamegoldás különböző útjainak keresése, az elméleti ismeretek átültetése a gyakorlatba – amelyek a tanulás hatékonyságát sokszorosára képesek növelni.

A kívánt pedagógiai célok elérése kizárólag „tanulócsoportok" aktív munkájára építve valósítható meg. A tanulóknak olyan tantárgy-specifikus ismeretekre épülő, a mindennapi élet egy-egy komplex problémáját felölelő feladatot kell adni, amelynek színvonalas, eredményes feldolgozása igényli a társakkal való együttműködést. A kooperatív munka – a szakmai fejlődésen túl – lehetőséget ad a csoport tanulói számára az önállóság és a felelősségtudat fejlesztésére, a demokratikus közösségi viselkedésmódok gyakorlására.

Az e-learning tehát újszerű pedagógiai gyakorlatot igényel, és újszerűségét azok a módszerek adják, amelyek hagyományos tantermi körülmények között nehezen alkalmazhatók: a munkáltatómódszerek (projekt módszer, kooperatív tanulás, szerepjátékok, szimuláció, játék…)

Az e-tananyagok egy-egy nagyobb egységének lezárásaként célszerű **projekt feladatot** adni a tanulóknak. A projekt tulajdonképpen egy terv, amely egy összetett, komplex feladat elvégzésének feltételeit, folyamatát és eredményeit határozza meg. A projekt sajátossága kétirányú. Egyfelől, középpontjában mindig egy valós életben felmerülő, az emberek többségét érintő kihívás, probléma áll, amelynek megoldásához felelős, együttműködésre

építő magatartás szükséges. Másfelől, a téma feldolgozása – projektválasztás, tervezés (feladatok és végrehajtásuk módja), végrehajtás, értékelés – a hagyományostól eltérő oktatási stratégiát, „projektoktatást" igényel. A projektoktatással megvalósuló tanulási folyamatban döntő szervezési tényező a tanulók önállósága. A **„projekt módszer"** az ismeretátadás, a véleménycsere, az esetleges viták lebonyolításához szükséges eszközök – fórum, e-mail, blog, hirdetőtábla, on-line óra…- kiválasztásának összehangolását is igényli a tanulócsoportokon belüli, valamint a „tanulócsoport – tanár" kommunikációhoz. A „tanulócsoport - tanár" kommunikáció sajátos eleme a tanári megfigyelő szerepkör. A tanár – a virtuális tanteremben tartott on-line foglalkozáson – a háttérből figyeli a tanulók munkáját, szükség esetén egy-egy információval aktivizálja a „kiváró, visszahúzódó" tanulókat, átsegíti őket a nehézségeken akár a munka, akár az együttműködés terén, illetve a frissen szerzett információ gyakorlatba való átültetésének kreatív megoldásait, az együttműködést, a közös munkát „jutalmazza".

Projekt feladat a számviteli alapismeretek e-könyvben [15]

A tanulóközösségekben folyó munka alapvető szemléleti változást követel a tanulótól, hiszen kikerül a közvetlen tanári kontroll alól, a társakkal együttműködve, a társak hozzáállását és véleményét tiszteletben tartva kell tanulnia. Az e-learning sajátossága egyes tanulók számára ezt megkönnyíti, míg mások számára megnehezíti. A projekt feladatok előállítása előtt célszerű megismerni a csoportban résztvevő tanulók személyiségjegyeit, viselkedésformáit, feltérképezni, hogy várhatóan milyen szerepkörbe „kényszeríti" őket tanulási szokásuk, tanulási gyakorlatuk. Az aktív, a reflektív, a kísérletező és az elméleti tanulók eltérő módon közelítenek a megoldandó feladathoz, amely nem hagyható figyelmen kívül sem a feladat összeállítása, sem a kooperatív munkavégzés során.

A tanítási-tanulási folyamatban alapvetően fontos szerepe van az **értékelésnek,** technikai szempontból, pedig annak, hogy elvégezhető-e az értékelés kizárólagosan tanári felügyelet nélkül. Mindemellett, az értékelésnek elegendő sűrűségűnek kell lennie, nemcsak azért, mert eredménye választ ad arra, hogy milyen mértékben valósultak meg a követelmények által kitűzött célok, hanem azért is, mert igen erős motiváló hatással bír, döntően befolyásolja az ismeretszerzés hatékonyságát, a tananyagban való haladás ütemét.

Az e-tanulásban bármilyen sűrűséggel lehetőség van **formatív értékelésre,** amelynek eszközei az egyes tananyag-egységekhez illeszkedő, a pontosan kidolgozott követelmények alapján összeállított feladatlapok, tesztek. A tudásszint-ellenőrző feladatokat célszerű példatárban elhelyezni, egy-egy tananyag-egységhez igazítva a tartalmában, de formai megoldásában is – feleletválasztós, igaz-hamis, lyukas szöveg, labirintus, keresztrejtvény – különböző nehézségi fokú feladatokat. A feladatok leírásánál utalni kell a nehézségi fokukra, fel kell hívni a tanulók figyelmét, hogy a megszerzett ismeretek megerősítése, a tartós tudás elsajátítása érdekében, az önellenőrzéskor javasolt az egyszerűbb feladatoktól haladni az összetettebb feladatok felé. Az önellenőrzés eredményéről a tanuló a feladatok megoldását követően azonnal visszajelzést kap, hiszen a korszerű teszt-szoftverek – Hot Potatoes, Quandary stb.[16] – számszerűen értékelik (az elért eredmény %-ában) teljesítményét, a hibás válaszokat megjelölik, segítő kérdéseket adnak a javításhoz, visszavezetik az alapproblémához, vagy új útvonalra terelve újból megoldatják a sikertelenül megoldott feladatot.

Fontos számolni azzal a ténnyel is, hogy a tanulókban az eredmény megismerésekor „egy produkcióra adott külső reakció belső átélése megy végbe” [17], aminek pszichológiai feldolgozásához, különösképpen negatív eredmény esetén a motiváláshoz, indokolt motiváló elemeket beépíteni a tananyagba

A formatív értékelésre alkalmazott program érdemét – a már említetteken túl – abban látom, hogy felszabadítja a tanárt a fárasztó, időigényes rutinmunka alól, mint tesztek, példák javítása, osztályozása, így több ideje jut a nevelés személyiségformáló feladataira, az elért eredmény elismerési módjainak kidolgozására, hiszen az értékelő elemek állandó továbbfejlesztésre, aktualizálásra szorulnak.

Elektronikus könyveim önellenőrzési rendszerébe „mérföldköveket” építettem be, amelyek teljesítésekor a tanuló „jutalmat” kap. Jutalom lehet például egy tananyagrész játékos formában történő feldolgozásának elérhetősége, megtekintése, részvétel egy tananyagba épített „Jutalom órán”.[18] A tananyag látványos, játékos megjelenítésének hatása abban rejlik, hogy élményekkel kapcsolja össze az ismeretszerzést, hogy színesebbé teszi a tanulást, élénkíti a figyelmet. A tapasztalatok azt mutatják, hogy egy lehetséges jutalom felkelti a tanuló kíváncsiságát, motiválja az ismeretszerzésben, az előrehaladásban.[19]

A formatív értékelés tehát teljes egészében megoldható közvetlen tanári jelenlét nélkül, ugyanakkor a **summázó, végső értékelés, a vizsga,** kizárólag a tanuló - tanár közvetlen kapcsolata lehetőségének megteremtésével lehet megbízható és objektív.

Véleményem szerint a vizsgán, a végső megmérettetésen csak tanári jelenlét mellett zárható ki a vizsgáztató programok alkalmazásának legtöbbet vitatott kérdése, a „csalás” lehetősége (a nem megengedett segédanyag használata vagy személyes segítség igénybevétele), illetve csak így kaphatunk megnyugtató visszajelzést a tanulók valós tudásszintjéről.

.

ÖSSZEFOGLALÁS

Az 1960-as és ’70-es években a programozott oktatás és az oktatógépek elterjedése azzal együtt, hogy szinte „forradalmat” okozott az oktatásban, bizonyos „szorongást” is gerjesztett a szakmai berkeken belül. A szakma megijedt volna saját árnyékától? Képes volt hinni azoknak a nézeteknek, hogy a jövőben a pedagógusok, tanárok szerepe korlátozódik, az oktatógépek helyettesítik őket? A kezdeti ijedtség aztán gyorsan alábbhagyott. Ismét bebizonyosodott, hogy a jó pedagógus semmivel nem helyettesíthető. Belátható az is, hogy az e-learning csak akkor lehet sikeres, ha a tanulói sajátosságok sokszínűségét figyelembe vevő, arra építő tananyagokkal és módszertani megoldásokkal képes támogatni a tanulók ismeretszerző tevékenységét.

A Zrínyi Miklós Nemzetvédelmi Egyetem – ahol évek óta korszerű e-tananyagok segítik a hallgatók tanulmányi munkáját – az elsők között ismerte fel a távoktatásban, az e-learningben rejlő lehetőségeket, az ismeretátadás új színterének szükségességét és jelentőségét: „a Magyar Honvédség részére szükségszerű az új tanítási/tanulási módszerek, eszközök és médiumok bevezetése és elterjesztése. Az egyén versenyképessége közvetlenül kapcsolódik a teljes életpályára kiterjedő tanuláshoz, mely alapvető célja a kreativitás, a rugalmasság, az adaptációs, a problémamegoldó és a tanulási készségek folyamatos fejlesztése. A tanulás és önképzés a pályán maradás és előrejutás feltételévé válik.” [20]

Az egyetem oktatói által kifejlesztett korszerű taneszközök, mind a katonai műszaki tudományok területén [21], mind a hadtudományok területén [22] hatékonyan segítik a hallgatók tanulmányi munkáját, a jövő katonai szakemberei számára szükséges átfogó, összetett, interdiszciplináris ismeretek megszerzését.

Az „Információs műveletek” multimédiás tananyag címlap képe [21]

A „Haditechnikai kutatás-fejlesztés” multimédiás tananyag-címlap html képe [22]

Irodalomjegyzék

[1] Howard Rheingold: Tools For Thought. The People and Ideas of the Next Computer Revolution. New York, 1985, Simon & Shuster. http://www.well.com/user/hlr/texts/tftindex.html

[2] Takács Etel: Programozott oktatás? Budapest, 1978

[3] Dr. Seres György – Dr. Miskolczi Ildikó – Tibenszkyné Dr. Fórika Krisztina – Szegediné Lengyel Piroska – Gerő Péter: Hipermédia az oktatásban – avagy felhőpedagógia, hogyan vált az elektronika az oktatás tárgyából annak színterévé? Hadmérnök On-line tudományos folyóirat, V. évfolyam, 2. szám. 2010. június, ISSN 1788 1919

[4] Desmond Keegan: Foundations of distance education: Frameworks for the future, First, London: Routledge (1990)

[5] Karlovitz János: Tankönyvtípusok, tankönyvmodellek, Új Pedagógiai Szemle, 2001. január

[6] Báthory Zoltán – Falus Iván (szerk.) Pedagógiai lexikon, III. kötet, Keraban Könyvkiadó, Budapest, 1997

[7] Skinner: A tanítás technológiája, Gondolat kiadó, Budapest, 1973

[8] E. B. Fry Teaching Machines and Programmed Instructions c. könyve (New York, 1963)

[9] Shirky: Social Software and the Politics of Groups, http//shirky.com/writings/group/

[10] Dr. Vörös Miklós: Oracle iLearning – internet alapú távoktatási rendszer a Zrínyi Miklós Nemzetvédelmi Egyetemen, https://nws.niif.hu/ncd2005/docs/ehu/067.pdf, (letöltés ideje: 2010. június. 20.)

[11] Pál Gyula, Vágvölgyi Csaba: Szabadforrású e-learning keretrendszerek összeghasonlító elemzése, Informatika a felsőoktatásban konferencia, Debrecen, 2005

[12] http://www.lengyelpiroska.hu/Oktatas.html

[13] http://forika.hu/moodle/

[14] http://miskolczi.net/moodle/

[15] http://www.lengyelpiroska.hu/szamvitele/konyv/Peldatar.html

[16] Dr. Seres György – Dr. Miskolczi Ildikó – Tibenszkyné Dr. Fórika Krisztina – Szegediné Lengyel Piroska – Gerő Péter: Teszteljük a teszteket – Avagy az interaktív ismeretellenőrzés néhány professzionális lehetősége az e-learningben, Repüléstudományi Közlemények, On-line tudományos folyóirat, http:// www.szrfk.hu/rtk/index.html, Repüléstudományi Közlemények Különszám, 2010. április 16, Szolnok, HU ISSN 1789-770X

[17] Nádasi András: Oktatástechnológia és oktatástechnika, Főiskolai jegyzet, Budapest, 2007

[18] http://www.lengyelpiroska.hu/szamvitele/konyv/Eloadas.html

[19] Szegediné Lengyel Piroska: Hatékony virtuális oktatás a pedagógia és a didaktika szemszögéből Hadmérnök On-line tudományos folyóirat, V. évfolyam, 2. szám. 2010. június, ISSN 1788 1919

[20] Vörös Miklós: eLearning a katonai felsőoktatásban http://www.szamalk.hu/eLearning/Default.htm (letöltés ideje: 2009. augusztus 12.)

[21] Dr. Várhegyi István, Dr. Haig Zsolt, Dr. Kovács László: Információs műveletek, Multimédiás tananyag, CD-ROM, ZMNE, 2005

[22] Kende György, Seres György: „Haditechnikai kutatás-fejlesztés", Multimédiás tananyag, http://www.drseres.com/tavoktatas/index.htm

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Bárdos Zoltán
zoltan.bardos@katved.hu

A TERÜLETI RENDELTETÉSŰ ÁRVÍZVÉDELMI KOMPLEX POLGÁRI VÉDELMI SZERVEZETEK SZAKKIKÉPZÉSÉNEK SZEREPE AZ ÖNKORMÁNYZATI ÁR-ÉS BELVÍZ ELLENI VÉDEKEZÉSBEN

Absztrakt

Magyarország vízkár veszélyeztetettsége Európában egyedülálló, megközelítően hasonló Hollandiához. Hazánkban az elmúlt évtizedben több súlyos ár-és belvíz elöntés alakult ki, melyek jelentős károkat okoztak a nemzeti vagyonban, a védművekben, műtárgyakban, ingatlanokban, és a mezőgazdaságban. A védekezésben a jogszabályok alapján, az állami szerveken túl az önkormányzatoknak és a civil társadalomnak is megvan a szerepe és feladata. Az ár-és belvíz elleni védekezést hazánkban a jogszabályok megfelelő módon szabályozzák, igazolják ezt az elmúlt évtizedben végrehajtott sikeres árvízvédekezések. A védekezésben az anyagi és technikai eszközök alkalmazása mellett, óriási szerepe van a kétkezi munkaerőnek. Az emberi élet és az anyagi javak védelme érdekében, a védekezés során alkalmazásra kerülnek a települési és területi polgári védelmi szervezetek. A polgári védelmi szervezetek alkalmazhatóságát alapvetően meghatározza a kiképzettségük. Jelen írásban vizsgálom, hogy a polgári védelmi szervezetek előírt szakkiképzését követően az önkormányzatok ár-és belvíz elleni védekezési feladatainak ellátása milyen módon javul. Javaslatot fogalmazunk meg a védekezésre való felkészítési módszerek vonatkozásában a korszerűsítésre a 2010. március 26-27-én Adonyban végrehajtott területi rendeltetésű árvízvédelmi komplex szervezet felkészítés tapasztalatai alapján.

The risk of the damage caused by flood in Hungary is unique in Europe. It is similar to the Netherlands. In the last decade many serious floods caused significant damage to real estates, protective structures and the whole agriculture. According to the law and regulations not only the state organs have their role in the protection but the local governments and the whole civil community as well. All the successful battles against floods and inland waters in the last decade, confirm the fact that the regulations are adequate. In combination with means and technical equipment, living labour plays an enormous role in protection. The regional services of civil defence are applied to protect both human life and material needs. The level of their training determines their applicability. Present writing reveals the pozitive change in the service of the municipalities due to compulsory training. We make proposals on preparation

methods, using the observations of the complex service training in Adony in March 26-27. 2010.

Kulcsszavak: *ár-és belvíz veszélyeztetettség, védekezés, felkészítés, polgári védelmi szervezetek ~ risk of damage caused by flood and inland water, protection, training, civil defence services*

BEVEZETŐ

Magyarország – földrajzi fekvése következtében – a Kárpát-medence árvízzel, belvízzel és aszállyal nagymértékben veszélyeztetett területe. Hazánkban az elmúlt évtizedben a rendkívül szélsőséges időjárás következtében az ár-és belvizek, valamint a helyi vízkárok is jelentős gondokat okoztak. Ezek az események ráirányították a figyelmet arra, hogy az emberi élet és a településeken felhalmozott egyre növekvő nemzeti vagyon értékének a védelme, az élhető környezet biztosítása érdekében, az állami szerveken túl a településeknek is fel kell készülni az ár-és belvízvédekezésre. Nemzetközi összehasonlításban Magyarország vízkár veszélyeztetettsége Európában egyedülálló, megközelítően hasonló helyzetben csak Hollandia van. Magyarország a Kárpát-medence magas hegyekkel körülhatárolt földrajzi egységének nagyjából a közepén helyezkedik el. A felszíni vizek 96 %-a külföldről érkezik az ország területére. A vízgyűjtő területek döntő része a határokon kívül helyezkedik el. Az éghajlati és domborzati viszonyaink miatt bármely folyónkon és bármikor kialakulhatnak heves és tartós árvizek. A nyugat-európai óceáni, a dél-európai mediterrán és a kelet-európai kontinentális időjárás egyaránt kifejti hatását, ezért az időjárás szeszélyes, jelentős szélsőségek is előfordulnak. Nagymértékben változik a csapadékvíz nagysága, időbeli és térbeli eloszlása, s gyakoriak a helyi jelentőségű, nagy intenzitású esők, zivatarok.[1]

Az ország természeti adottságai alapján a vizek kártételeinek lehetősége a síkvidéki, a hegy- és dombvidéki településeken egyaránt jelen van. Területének csaknem fele (44 ezer km^2) síkvidéki, valamivel több, mint fele (47 ezer km^2) hegy- és dombvidéki, a magasabb hegyek részaránya mintegy 2%. Az előzőekből adódóan hazánkban az árvízvédelmi művek hossza (4220 km, ebből a Tisza völgyében 2951 km) szintén meghaladja az egyes európai adatokat (Hollandiában: 1500 km, a Pó-völgyében: 1400 km, a Loire-völgyében: 480 km). Az ár- és belvizekkel veszélyeztetett területek nagysága együttesen megközelíti az ország területének mintegy felét. A mértékadó árvizek szintje alatt fekszik az ország területének csaknem egynegyede, ahol 700 településen 2,5 millió ember él.[2]

Statisztikai átlagok alapján 2-3 évenként kisebb vagy közepes, 5-6 évenként jelentős, 10-12 évente pedig rendkívüli árvizek kialakulására lehet számítani. Miközben az árvizek által az ország területének mintegy 25%-a van közvetlenül veszélyeztetve, szélsőséges időjárási körülmények közepette hazánk bármely településen, az év bármely szakaszában keletkezhetnek elöntések és károk, veszélyeztetve a lakosok élet- és vagyonbiztonságát.[3]

Az árvíz elleni szervezett védekezési tevékenység két, jól elkülöníthető tevékenységcsoportra osztható. Egy részük a védekezés műszaki feladatainak szervezésére, irányítására és ellátására irányul. Ez alatt a védekezés időszakában a védelmi létesítményeken folyó azon tevékenységek összességét kell érteni, amelyek a védművek ellenőrzését, védelmi teljesítőképességük megőrzését, azaz szükség esetén a terheléssel szemben lokálisan fellépő védőképességi hiányosságoknak a védekezési munkával, ideiglenes védelmi létesítmények kiépítésével való pótlását foglalja magába. Ez a feladatrendszer a Vízgazdálkodásról szóló törvény[1] (Vgtv.) és a végrehajtására kiadott kormány rendelet[2] szerint, a Környezetvédelmi és

[1] 1995. évi LVII. törvény a vízgazdálkodásról 16. § (4) bekezdés és a 35. § (1) b) pontja

Vízügyi Igazgatóságokhoz (KÖVIZIG), valamint a vízitársulatokhoz tartozik.[4] Másik részük a védekezés államigazgatási feladatainak szervezésére, irányítására és ellátására irányul. Ezen tevékenységen belül kétféle csoportosítás lehetséges: Egyrészt kiemelendő a védekezés műszaki feladatainak ellátása érdekében szükséges tevékenységek, az ezen feladatok ellátására létrehozott szervezetek személyi-és anyagi-technikai felszereltségét meghaladó munkaerő, anyag, eszköz gép és szállítóeszköz folyamatos, a védekezés igényeit kielégítő biztosítása[3] [4]. Ebben az esetben már a védelmi igazgatás rendszeréből a megfelelő szint aktivizálódik (MVB, HVB, polgármester) és ezen keresztül kerülnek az erők–eszközök biztosításra. Másrészt a veszélyeztetett lakosság és anyagi javak „szükség esetén" biztonságba való helyezése érdekében (mentés, kitelepítés) végrehajtott tevékenységek, valamint a lakosság és a védekező erők egészségügyi ellátására, a kitelepítettek szociális ellátására, a járványok megelőzésére, elhárítására, a keletezett károk felmérésére, helyreállítására vonatkozó tevékenységek[5], vonatkozásában a szükséges intézkedéseket szintén a védelmi igazgatás rendszere jogosult meghozni.
Az előzőekből látható, hogy a védekezésnek vannak olyan feladatai melyeket a KÖVIZIG-ok saját védelmi szervezetük aktivizálásával végre tudnak hajtani, de az ár-és belvízvédekezés kiszélesedésével és elhúzódásával elérik lehetőségeik határát. Ekkor lehetőség van a személyi és az anyagi feltételek biztosításához a - jogszabályok adta lehetőségek keretei között[6] - a védelmi igazgatás rendszerében a védelmi bizottságok és polgármesterek által a polgári védelmi szervezetek készenlétbe helyezésére[7].[4] A katasztrófák elleni védekezésre a következmények felszámolására létrehozott szervezetek, különböző védekezési rendszerek és a bevonhatók köre a katasztrófavédelmi törvényben[8] is meghatározásra került.
A cikkben Fejér Megye árvíz-veszélyeztetéséből adódó ár-és belvízvédelmi feladatok során vizsgálom az önkormányzatok helyét, szerepét és a területi rendeltetésű árvízvédelmi komplex szervezet megalakítását, és szakkiképzésének lehetőségeit. A felkészítés elemzéséhez és következtetések levonásához, valamint javaslatok megtételéhez a 2010. március 26-27-én Adonyban végrehajtott szakkiképzés és készségfejlesztő gyakorlat tapasztalatait használom fel.

FEJÉR MEGYE ÁR-ÉS BELVÍZ VESZÉLYEZTETETTSÉGE

Megyénk ár-és belvízveszély szempontjából a közepesen veszélyeztetett megyék közé tartozik. A Duna Ercsi és Kisapostag közötti szakasza Fejér Megye keleti határa. A felszíni vizek vonatkozásában a megye valamennyi részvízgyűjtője a Dunába torkollik. Jellemzően végigvonul időszakonként a jeges ár és a zöldár hulláma a Dunán, amely az árvízvédelem folyamatosan jelentkező igényére figyelmeztet**.** Árvizek mindig voltak és mindig lesznek. Egyelőre elképzelhetetlen, hogy valaha is el tudjuk érni megszüntetésüket, de kártételük korlátozható, mérsékelhető. Az árvizeket mindenkor a folyó vízgyűjtőjén[9] fellépő különleges időjárás okozza. Ebből következik, hogy a vízgyűjtő terület nem ismeri a határokat. A nagy folyókon tehát, amelyek vízgyűjtő területe több országra terjed ki, az árvizek ellen csakis

[2] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 3. § (1-3) bekezdés
[3] 1995. évi LVII. törvény a vízgazdálkodásról 17. § (7) bekezdés b) pontja
[4] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól 7. § (4) bekezdés
[5] 1995. évi LVII. törvény a vízgazdálkodásról 17. § (6) bekezdés (7) bekezdés (c-f) pontja
[6] 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről 32. §
[7] 1996. évi XXXVII. törvény a polgári védelemről 9. § (1) a), e) pontja, 10. § (2) c) pontja
[8] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről 2. § (1-2) bek.
[9] A *vízgyűjtő terület* a folyó egy pontjához tartozó azon terület, amelyről a lehulló csapadék a patakokon, kisebb folyókon keresztül végül eljut a szóban forgó helyhez. (A Duna budapesti szelvényéhez, pl. Magyarország kétszeres területének megfelelő vízgyűjtő tartozik.)

nemzetközi összefogással lehet sikeresen védekezni. A Duna vízgyűjtő területe a 1. sz. mellékletben látható.
Szükséges tisztáznunk az árvíz fogalmát: *árvíz* egy folyóvíz vízszintjének olyan mértékű emelkedése, amikor az medréből kilép. Fontos megkülönböztetni az áradástól, amikor a vízszint ugyan megemelkedik, de a mederből nem lép ki a víz. Az árvizek három nagy csoportját különböztetjük meg, a jégtorlódásból adódó *jeges árvizet* (ilyen volt például az 1838-as pesti ár), az egyszerre olvadó hótömegből keletkező *tavaszi árvizet* (ez okozott a Duna felső szakaszán 150 éve nem látott vízszintet 2006 márciusában), illetve a nagy tavaszi, vagy nyári esőzésekből keletkező *zöldárat*.

A Duna-menti településeket az árvízvédelmet nyújtó gátak, természetes domborulatok, magas partok védik a folyón levonuló árhullámoktól. A gát szerepét a megye területének döntő hányadán önálló földgátként, a 6-os út nyomvonala biztosítja, amely kialakításával kettős szerepet tölt be, egyrészt mint árvízvédelmi elsőrendű védvonal, másrészt, mint fő közlekedési útvonal halad végig a Duna mellett. A fővédvonal kezelője a megye területén a Közép-dunántúli Környezetvédelmi és Vízügyi Igazgatóság (KÖDU KÖVIZIG) Fejér megyei szakaszmérnöksége. Dunaújváros területén az árvízvédelem az Önkormányzat feladata. Dunaújváros térségében az 1964-es komoly partcsúszás, partrogyás után megépült a Komplex Partvédmű más néven Partvédelmi terület a Duna parton, amely az Alsó-foki patak torkolatától a belterületen levő ún. négyes kazettáig biztosít elsőrendű védelmet.

Fejér megyében egy árvízvédelmi öblözet, és kettő belvízvédelmi szakasz található.
Megyénkben a Duna jobb partján a 04.04-es számú, Adony - Ercsi árvízvédelmi szakasz által határolt öblözet veszélyeztetett elöntéssel. A mentesített területen a három település található melyek közül Adony teljes egészében, Ercsi, Iváncsa részben veszélyeztetett árvízi elöntéssel. Továbbá, Sinatelepen, néhány major és mezőgazdasági jellegű épület. Az öblözet területe összesen 50,94 km^2. Ebből az ercsii öblözet 22,58 km^2, az adonyi öblözet 28,36 km^2.
Az I. rendű védvonal hossza a megyében: 31,402 m.
Vízfolyáskénti bontásban:

- Duna jobb part 19,603 m
- Váli-víz jobb part 4,235 m
- Váli-víz bal part: 2,829 m
- Szent László víz jobb part 4,735 m

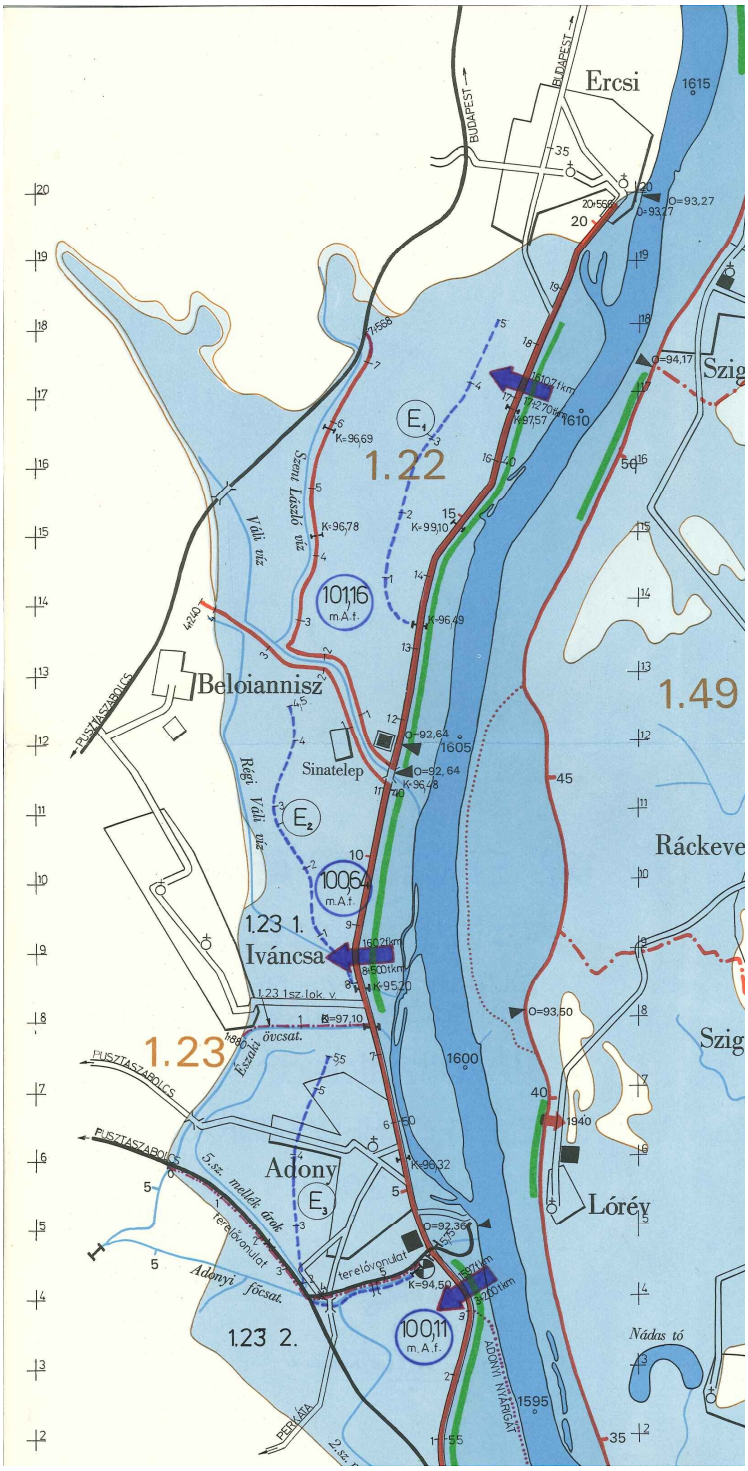
A Duna áradására a 0,5 - 0,8 m/nap a jellemző (pl. zöldár) az ennél nagyobb intenzitású áradás valószínűsége csekély. A két mellékvízfolyás árhullámai akkor okoznak árvízi helyzetet, ha a Duna áradása is hasonló időben történik. A 04.04-es öblözet három gátőrjárásra tagozódik őrjárásonként két fő gátőr-műszaki és egy fő gátőr teljesít szolgálatot. Árvízvédekezés esetén a védelmi központ Adony gátőrháznál működik.

A dunai védvonal kiépítettsége

A fővédvonal mind magasságilag, mind keresztmetszeti méreteiben kiépült a mértékadó árvízszint + 1 m biztonsági magasságra (kivétel a régi 6-os út ercsii belterületi szakasza 1300 m). A mellékvízfolyásokon (Szent László-víz, Váli-víz) csak a mértékadó árvízszintre van kiépítve a töltés, aminek a keresztmetszeti méretei sem megfelelőek. Tartósan magas vízállás esetén, ezen a szakaszokon várhatóan komoly védekezési munkákra lenne szükség. Az árvízvédelmi töltést 39 db műtárgy, vezeték keresztezi. A védvonalban lévő műtárgyak állapota - ellentétben magával a védvonal állapotával - nem megnyugtató. A zsilipek között van, amelyik több mint száz éves (Zichy zsilip). A közlekedés dinamikus növekedése, az intenzív korróziós közeg (sózás) hatására az árhullám levonulása esetén számolni kell az

esetleges tönkremenetelükkel. Az Adony - Ercsi öblözetben 20 műtárgy - árvízvédelmi fővédvonalat keresztező létesítmény - található.
A létesítmények üzemben tartását, illetve karbantartását a vízügyi szakemberek végzik. Évente - jogszabály alapján egy alkalommal[10]- műszaki felülvizsgálat keretében ellenőrzik ezek állapotát, melyen a Fejér Megyei Katasztrófavédelmi Igazgatóság szakembere is részt vesz, a vizsgálatot követően jegyzőkönyvön rögzítik a feltárt helyzetet.
Töltésszakadás, töltés meghágás, illetve műtárgy tönkremenetel esetén a legkritikusabb helyzet Adonyban, Sinatelepen fordulna elő. Ercsit és Iváncsát csak a település mélyebb részein fenyegeti elöntés, a lokalizálás lehetőségét az 1. sz ábra szemlélteti. Az I. rendű árvízvédelmi töltéseken a KÖDU KÖVIZIG irányítja a védekezést. A nyílt ártéren, valamint Adony, Ercsi, Iváncsa települések területén az önkormányzatok feladata a védekezés biztosítása.
Nyílt ártéri területek:
- Ercsi : hajóállomás melletti lakóterület,
- Adony : rév átkelő melletti lakóterület.

[10] 10/1997. (VII. 17.) KHVM rendelet az árvíz- és a belvízvédekezésről 6. § (1) bek.



1. sz. ábra Adony lokalizációs térkép, Forrás[11]

Az árvízvédelmi öblözeten túl, a megyénkben lévő kettő belvízvédelmi szakasza is veszélyeztető hatással bír lakott területek vonatkozásában.

[11] KÖDU KÖVIZIG Fejér Megyei szakaszmérnökség

A 04. 03. számú Adony - Ercsi belvízvédelmi szakasz jellemzése

A belvízvédelmi szakasz a Duna jobb partján az Adonyi belvízrendszerben helyezkedik el, három öblözetre tagozódik (Adonyi, Ercsii, Iváncsai). A belvízvédelmi szakaszt keleten a 6. sz. főközlekedési út, - amely egyben árvízvédelmi fővédvonal -, északon az Ercsi magaslatok, valamint a Budapest - Pusztaszabolcs vasútvonal, nyugaton a Beloianniszi magaslatok, délen pedig a Duna Kulcsi dombhát nyúlványai határolják. A belvízvédelmi szakasz területén egy település, Adony helyezkedik el. A szakasz területe 48 km^2, vízgyűjtő területe 274 km^2. A szakasz védvonalai 0,5-1,0 m-es biztonsággal vannak kiépítve.

Az **Adonyi** öblözet befogadója az Adonyi Főcsatorna, hossza: 4,6 km, mely az adonyi zsilipen keresztül csatlakozik a Dunába. A Duna magas vízállása esetén az adonyi szivattyútelep emeli át a belvízcsatorna vizét. Az átemelőben kettő elektromos meghajtású c.c.k. 500-as típusú, függőleges tengelyű szivattyú található, melyek egyenkénti teljesítménye 0,65 m^3/sec., az együttes teljesítmény ezzel 1,3 m^3/sec. A szivattyútelep fennállása óta még nem került sor a kettő szivattyú egyidejű üzemeltetésére. Az **Iváncsai** öblözet befogadója a Váli víz, mely a Dunába vezeti a vizet. Az esetleges magas vízállás esetén mobil szivattyús átemelés szükséges. Az **Ercsii** öblözetnek nincs közvetlen befogadója, szükség esetén a Szent László vízbe, illetve a Dunába lehet mobil szivattyúkkal átemelni a többletvizet. A belvízvédelmi szakasz területén két közös gát- és csatorna őrház található. A külvizek kizárására szolgáló Cikolai tórendszer, a zsilipek, illetve az Adonyi szivattyútelep összehangolt működésével a belvízöblözetben a vizek károkozás nélküli levezetése megoldható. A belvízvédelmi szakasz kiépítettsége jónak mondható, a védvonalak és műtárgyaik a feladatukat képesek ellátni.

A 04. 05. számú Cece - Ősi belvízvédelmi szakasz jellemzése

A belvízvédelmi szakasz a Nádor- és a Sárvíz-malomcsatorna vonalát követi Cecétől Ősi településig. Alsó határa a Cece - Sáregresi országút, a felső pedig a Várpalota - Péti dombok. A megyéből kilenc települést érint. A szakasz területe 154,5 km^2, melyhez 2661 km^2 külvíz-gyűjtő tartozik. Az öblözetre a hosszú és keskeny belvizes terület a jellemző. A szakasz védvonala majdnem teljes hosszon 0,5 - 1,0 méteres biztonsággal van kiépítve. Elöntés esetén zömmel külterületi rétek, kaszálók, szántók kerülnének víz alá. A belvízvédelmi szakaszokon szakaszvédelmi központ nincs. A védekezés irányítása a KÖDU KÖVIZIG védelemvezetője által, a központi műszaki ügyeleten keresztül történik. A védekezés operatív irányítását a szakaszmérnökség központjából végzik. Az igazgatóság központi ügyelete kapcsolatot tart a szakaszmérnökség ügyeletével, valamint az OVF központi ügyeletével. Szükség esetén a Védelmi Osztagnak is el lehet rendelni a belvízvédelmi szolgálatot az igazgatóság védelemvezetőjének, illetve helyettesének utasítására.

A VÍZÜGYI IGAZGATÓSÁG VÉDELMI SZERVEZETE ÁR-ÉS BELVÍZVÉDEKEZÉS ESETÉN

Az előzőekből is jól látható, hogy megyénkben ár-és belvíz veszéllyel is kell számolni, ezért az ellenük való védekezésre a vízügyi igazgatóságnak és a településeknek is fel kell készülniük. A vízügyi igazgatóságoknak védekezési feladataikat elsősorban saját erővel[12] kell megoldaniuk. A feladataik végrehajtásához létrehozásra került minden vízügyi igazgatóságon egy védekezési szervezet, melyet a szakasz védelem-vezető közvetlenül irányít. A védelmi szakasz felépítését a

[12] 10/1997. (VII. 17.) KHVM rendelet az árvíz- és a belvízvédekezésről 7. § (3) bek.

2. sz. melléklet tartalmazza. A védekezési feladatok során, amikor az ár-vagy belvíz helyzet kezelését a vízügyi igazgatóság már a saját erők és eszközök bevonásával nem tudja kezelni, akkor lehetősége van külső erőforrások bevonására[13]. Ebbe a körbe tartoznak az alkalmi munkások foglalkoztatása, az igénybevételi tervben lebiztosított erők és eszközök igénybevétele, szerződött partnerek eszközeinek, valamint a központi készleteknek, fegyveres és rendvédelmi szervezetek erőinek és eszközeinek a felhasználása. Természetesen azt látni kell, hogy ezeknek az igénybevétele már a védelmi igazgatás rendszerén keresztül a Megyei Védelmi Bizottságon és a polgármestereken keresztül történik.
A cikk további részében a védekezési feladatok ellátása érdekében létrehozott, területi rendeltetésű árvízvédelmi komplex polgári védelmi szervezet felkészítésének és az önkormányzati védekezések során való alkalmazásuk lehetőségeinek kérdéseivel foglalkozom, valamint a felkészítés tapasztalatainak (2010. március 26-27. Adony) jövőbeni hasznosítására teszek javaslatot.

A POLGÁRI VÉDELMI SZERVEZETEK MEGALAKÍTÁSÁNAK ÉS FELKÉSZÍTÉSÉNEK HELYZETE

A polgári védelemről szóló 1996. évi XXXVII. törvény (Pv. tv.) 1.§-a meghatározza a polgári védelem alapvető feladatait: „elősegítse a fegyveres összeütközés, a katasztrófa, valamint más veszélyhelyzet életet és a létfenntartáshoz szükséges anyagi javakat fenyegető hatásai elleni védekezést”, a jogszabály a továbbiakban polgári védelmi feladatok között szerepelteti a vizek kártételei elleni védekezést[14]. A feladatok végrehajtásához a jogszabály polgári védelmi kötelezettségen alapuló polgári védelmi szervezetek megalakítását rendeli el a polgári védelmi kötelezettség alatt álló állampolgárok köréből[15]. A létrehozandó szervezetek munkahelyi, települési és területi rendeltetésűek lehetnek. A szervezetek végrehajtandó feladatai adódnak a nevükből, mivel a munkahelyi szervezeteknek az adott gazdálkodó szervezet tevékenységéből adódó veszélyhelyzetek polgári védelmi feladatainak a kezelése a feladata, a települési szervezeteknek értelemszerűen a településen kialakuló rendkívüli helyzetekből adódó polgári védelmi feladatok megoldása a feladatuk. Területi rendeltetésű polgári védelmi szervezeteket annak a polgári védelmi feladatnak a végrehajtására hoznak létre, amelyet a települési polgári védelmi szervezetek nem képesek ellátni. Az előzőekből is jól látható, hogy a törvényhozók a jogszabály megalkotásakor is a szubszidiaritás elvéből indultak ki, hogy minden adandó veszélyt a lehető legalacsonyabb szinten lehessen kezelni. Ebből következik, hogy az ár-és belvíz elleni védekezés nem csak egy adott település feladata, hanem adott esetben (mikor a védekezés eléri azt a fokozatot) megyei (területi) szinten kezelendő. Területi rendeltetésű polgári védelmi szervezeteket különböző „polgári védelmi feladat” végrehajtása céljából lehet létrehozni, ahogy a Pv. tv. meghatározza, így a vizek kártételei elleni védekezésre is. Fejér megyében az ár-és belvíz elleni védekezési feladatok ellátására a Megyei Védelmi Bizottság Határozatával kettő területi rendeltetésű árvízvédelmi komplex szervezet került megalakításra (2x99 fővel), Adony és Ercsi települések bázisán. A szervezetek megalakításukat követően feltöltésre kerültek és a beosztott személyek pontosítása évente kettő alkalommal történik, a polgári védelmi kirendeltségek és a két érintett település polgármesteri hivatalának bevonásával. Elmondható, hogy a szervezetekbe beosztottak kijelölő határozatai naprakészek, a beosztási névjegyzékek aktualizálása folyamatos. A szervezetek alkalmazhatóságának egyik alapfeltétele a felkészültségük az-az a kiképzettségük.

[13] 10/1997. (VII. 17.) KHVM rendelet az árvíz- és a belvízvédekezésről 7. § (4) bek.
[14] 1996. évi XXXVII. törvény a polgári védelemről 4. § m) pontja
[15] 1996. évi XXXVII. törvény a polgári védelemről 16. § (1) bek.

A polgári védelmi szervezetek felkészítési rendszere

A polgári védelmi szervezetek felkészítését a Pv. tv. vonatkozó pontja[16] alapján kiadott BM rendelet[17] szabályozza. A rendelet meghatározza a felkészítés célját, mely alapján egyértelmű, hogy a természeti és civilizációs katasztrófák következtében kialakuló veszélyhelyzetek elhárítására és felszámolására való felkészülés a feladat.
Ennek a célnak a megvalósítására felkészítések és gyakorlatok szolgálnak. A területi és a települési polgári védelmi szervezetbe beosztott személyeket lakó- vagy munkahelyükön, indokolt esetben a szervezet megalakítási helyén kell kiképezni, a kiképzést a katasztrófavédelem hivatásos szervei végzik. A kiképzési rendszer hierarchikusan épül fel, mivel 6 órás alapkiképzéssel kezdődik, majd 10 órás szakkiképzés követi és vezetői kiképzés zárja, ezeket a képzéseket különböző fajta gyakorlatok követik. Sajnos el kell mondani, hogy az elmúlt évtizedben ezek a felkészítések és gyakorlatok elenyésző számban kerültek végrehajtásra megyénkben a települési és területi szervezeteknél. Ennek oka, hogy a Pv. tv. alapján a felkészítésen, gyakorlaton megjelent állampolgár „polgári védelmi kötelezettségének teljesítésével összefüggésben a munkáltatónál felmerülő és igazolt költségeit", a felkészítést elrendelőnek kell térítenie. Ilyen célra a katasztrófavédelem hivatásos szervei, vagy a települési önkormányzatok pénzügyi forrásokat nem kaptak. A Fejér Megyei Katasztrófavédelmi Igazgatóság 2007-2009 között több településen megpróbált alapképzéseket szombati napokon szabadidőben végrehajtani. A részvételi arány, - mivel a részvétel meghívással történt és nem kötelezéssel -, igen változó 25-60% közötti volt. A felkészítéseket tartó és azon résztvevő saját állományunk szintén szabadidejéből vett részt, így nekik ezt szabadidőben lehetett csak kompenzálni, ez megterhelő volt a napi munkavégzés során. Meg kellett állapítanunk, hogy pénzügyi források nélkül a felkészítések hatékony és eredményes végrehajtása nem várható. A Polgári védelmi szemle 2008. évi 2. számában Dr. Varga Imre mk. pv. ezredes, szintén a polgári védelmi szervezetek felkészítésével foglalkozik egy publikációban és ő is hasonló megállapításra jut, a munkanapon illetve hétvégén való felkészítéssel kapcsolatosan, igaz ő nem foglalkozik a gyakorlati megvalósíthatósággal. /Munkájában a szerző a hétköznapi felkészítést javasolja, igaz a szükséges források biztosításával, számunkra ez nem olyan formában állt rendelkezésre (távolléti díj fizetésére nem volt lehetőség) ahogyan ő írta, ezért mi péntek délután és szombat délelőtt hajtottuk végre./[8]
Kerestük a lehetőségeket, hogy milyen forrásokat lehetne bevonni a felkészítések finanszírozásába és a Megyei Védelmi Bizottság Védelmi titkárságával közösen találtunk 2009-ben egy pályázati forrást, melyet a HM Védelmi Hivatala írt ki és lehetőség volt polgári védelmi szervezetek felkészítésére is pályázni. A pályázaton a Fejér Megyei Önkormányzaton keresztül indultunk és a területi rendeltetésű árvízvédelmi komplex szervezet szakkiképzését tűztük ki célul, és sikeresen pályáztunk.

A szakkiképzés előkészítése és végrehajtása

A vonatkozó rendelet szerint[18] a szakkiképzést 10 órában kell végrehajtani, melyből egy nap legfeljebb 6 óra tartható meg és az órák felében legalább gyakorlati jellegű foglakozásokat kell tartani. [6] A rendelet előírásait szem előtt tartva a felkészítést kettő naposra terveztük, az első napon elméleti jellegű foglalkozásokat terveztünk végrehajtani, második napon pedig gyakorlat jellegű kiképzést. A felkészítésre vonatkozó rendeletben leírtakat kénytelenek voltunk megsérteni, mivel alapképzésben az állomány nem részesült, így az elméleti

[16] 1996. évi XXXVII. törvény a polgári védelemről 42. § (2) bekezdés *d)* pontja
[17] 13/1998. (III. 6.) BM rendelet a polgári védelmi felkészítés követelményeiről
[18] 13/1998. (III. 6.) BM rendelet a polgári védelmi felkészítés követelményeiről 17. § (2) bek.

felkészítésbe beépítettük az alapképzés anyagát is és bővített formában tartottuk meg a képzést. A szervezet specialitásából adódóan, valamint az egyéb nem polgári védelmi témájú előadásokhoz szükségesnek tartottuk a társ szervezetek bevonását is. Az alapképzés és szakkiképzés végrehajtásának konkrét követelményeit a fenti rendelet 1-2. számú mellékletei tartalmazzák, melyek általános és speciális a szakalegység tevékenységéhez tartozó ismeretekből állnak. A felkészítés előtt egyeztetést tartottunk az ÁNTSZ dunaújvárosi kistérségi intézetével, az OMSZ közép-dunántúli regionális igazgatóság Fejér megyei szervezetével, a Fejér Megyei Rendőr-főkapitánysággal (FMRFK) és természetesen a legfontosabbal a KÖDU KÖVIZIG Fejér megyei szakaszmérnökségével. A megbeszélésen megegyeztünk a felkészítés időpontjában, tisztáztuk az oktatandó témákat, valamint a szükséges anyagok és eszközök biztosítását. Nagyon fontos feladat volt Adony város polgármesterének a bevonása már az előkészítés fázisában, hiszen a felkészítés helyét, az ellátást, a szükséges logisztikai feladatokat a településnek kellett biztosítania. A szakkiképzés időpontjának március 26-27.-t jelöltük ki, ennek megfelelően kellett koordinálni az előkészítő feladatokat. Az első napon 4 óra időtartamban elméleti kiképzés terveztünk a másodikon, pedig 6 órában az ár-és belvízvédekezés végrehajtását a településen, illetve az adonyi nyári gátnál. Az előkészítés szervezéséhez mindenképpen szükséges volt egy team létrehozása, mely a feladatba bevont szervezetekkel tartotta a kapcsolatot, előkészítette a levezetési tervet és azt minden bevont szervezet részére is meg kellett küldeni. A team vezetését a megyei katasztrófavédelmi igazgató-helyettes látta el, nála futottak össze a legfontosabb információk a szükséges döntéseket ő hozta meg. Ezt a módszert mindenképpen ajánlom ilyen esetekben a tervezés, szervezés fázisában követni, hiszen a körültekintő előkészítés eredménye lesz a sikeres végrehajtás. A bevont szervezetekkel minden szükséges információ megosztása elengedhetetlen, ennek leggyorsabb formája az e-mail-en való kommunikálás. Ezt a kommunikációs csatornát használtuk mi is az előkészítés teljes időszakában, így a foglalkozási anyagok (prezentációk) időben megérkeztek, a levezetési tervet mindenki megkapta stb..

Az önkormányzatok ár-és belvíz elleni védekezése során a polgári védelmi szervezetekbe beosztottakon kívül önkéntesek is részt vehetnek, a közérdekű önkéntes tevékenységről[19] szóló jogszabály alapján. Megyénkben, az érintett Duna szakaszhoz közeli településeken is, több önkéntes tűzoltó egyesület van. Az önkéntes tűzoltó egyesületek (ÖTE) közül többel felvettük a kapcsolatot, akik felajánlották önkéntes részvételüket a felkészítésen, így Baracsról, Pusztaszabolcsról és Mezőfalváról.

Az első felkészítő napon 4 óra elméleti felkészítést tartottunk, ahol a társ szerveinket is bevontuk a szakterületeik vonatkozásában, így az ÁNTSZ dunaújvárosi kistérségi intézetét, (árvíz alatti és utáni közegészségügyi, járványügyi témában), az OMSZ Közép-dunántúli regionális igazgatóság Fejér megyei szervezetét (sérültek ellátása, elsősegélynyújtás területén), a FMRFK-ot (közrend és közbiztonság, hátra hagyott javak védelme témában) és természetesen a KÖDU KÖVIZIG Fejér megyei szakaszmérnökségét (az árvízi jelenségek és védekezés témában). Az elméleti felkészítés helyszíne az adonyi Művelődési Otthonban volt, ahol a polgári védelmi szervezetbe beosztottak közül 81 fő jelent meg. Ez nagyon jó aránynak mondható, mivel péntek délután 14.00-tól volt a felkészítés, ugyanis a pályázat nem tette lehetővé távolléti díj fizetését a felkészítésen résztvevőknek. A jövőben javasoltuk a pályázat kiírójának, hogy legyen lehetőség távolléti díj fizetésére is, mivel akkor munkaidőben is lehet tartani a foglalkozásokat.

A második napon a gyakorlati foglalkozások kerültek végrehajtásra az ár-és belvízvédelmi felkészítés keretében a komplex polgári védelmi szervezet részére 6 órában, valamin egy törzsvezetési gyakorlatot is tartottunk a Helyi Védelmi Bizottság részére 1 órában. A

[19] 2005. évi LXXXVIII. törvény a közérdekű önkéntes tevékenységről 3. § (1) *a)* pont, 4. § (1-2) bek.

gyakorlati felkészítés alkalmával két jól elkülöníthető feladatrendszer begyakorlását hajtottuk végre, egyrészt megtörtént a belvíz által veszélyeztetett lakóingatlanok bevédése, másrészt az árvízvédelmi fővédvonal megerősítése és az árvízi jelenségek kezelése. Az első helyszínen a Vétus Salina úton, lakóingatlanok bevédése került imitálásra, valamint belvíz átemelés és vízelvezető árok elvezető képességének helyreállítása történt. Ezen a helyszínen Dunaújváros HÖT egy gépjármű fecskendője 4 fővel, valamint Pusztaszabolcs ÖTE 9 fővel, Mezőfalva ÖTE 13 fővel, Baracs ÖTE 7 fővel dolgozott, valamint egy vállalkozó 3 munkagéppel állította helyre a vízelvezető képességét az ároknak. Az önkéntes tűzoltók homokzsák töltését végezték, majd a kapubejáróknál építettek nyúlgátat az ingatlanok bevédése érdekében. A településen élők nagy örömmel fogadták a gyakorlatot, mivel most szembesülhettek először valódi kézzel fogható gyakorlati feladat végrehajtásával az otthonuk közelében. A gyakorlást egy olyan helyszínen hajtottuk végre, ahol 2002-ben a belvíz problémát okozott és akkor az önkormányzat és a lakók sem voltak felkészültek a védekezésre.

1. sz. fotó: Ingatlanok belvíz elleni bevédése
Készítette: Bárdos Zoltán 2010.


2. sz. fotó: Vízelvezetés helyreállítása
Készítette: Bárdos Zoltán 2010.

A második helyszínt az adonyi nyári gátnál jelöltük ki, kifejezetten olyan szándékkal, hogy a valósághoz legjobban megközelítően szemléltethessük a védekezés szükségességét és fontosságát. A gyakorlati feladat helyszínén a KÖDU KÖVIZIG Fejér megyei szakaszmérnökség munkatársainak vezetésével négy foglalkozási helyet alakítottunk ki, ahol a munka forgószínpadszerűen folyt. Ezeken a foglalkozási helyeken igyekeztünk a valós védekezést minél jobban megközelíteni, ezért kialakítottunk egy homokzsáktöltő helyet, a többi foglalkozási helyen pedig a lehetséges árvízi jelenségek elleni védekezést gyakorolták, töltés magasítás, töltés megtámasztás, buzgár elfogás.

Árvízi jelenségek és ellenük való védekezés lehetőségeinek gyakorlása

A magyarországi árvízvédelmi létesítmények túlnyomó része földgát. Az épített támfalaktól eltérően, melyeken az árvízvédekezés viszonylag biztonságosabb, a földgátaknál számos problémával találkozunk egy-egy árvízi eseménynél. A problémák okait a földgátak létesítésében, fejlesztésében és elöregedésében találhatók meg. Az okok az eltérő és nem mindig megfelelő építési anyagra, hibás építés technológiára vezethetők vissza, továbbá az ún. öregedésre, amikor a beépített föld ásványos és szerves „korróziója” előrehalad, átázások, átfagyások, kiszáradások okozta duzzadásos, zsugorodásos mozgás keletkezik. A káros elváltozások tömörségcsökkenéshez is vezethetnek. Komoly gondokat okozhatnak az állatjáratok, állatfészkek üregei is. A különböző árvízi jelenségek oka többnyire a védmű talajának állapotából következik. A védmű alatt a töltést, valamint az alatta lévő talajtömböt

kell érteni. Legtöbbször tehát a jelenség okai között a töltés vagy altalajának, illetve a kettőnek együttes minősége áll. A földgátaknál fellépő jelenségeket részint a védőtöltés magasságát tartósan vagy időszakosan (hullámzás) meghaladó vízszintek váltják ki, részint a tartósan magas vizek által okozott nyomás, amely a töltéstestben, illetve az alatta lévő talajtömbben, más szóval az altalajban idéz elő mozgást.[7]
A védekezés során ezen káros jelenségek ellen szükséges „ellen" megoldásokat alkalmazni, így csökkentve a víz okozta káros hatásokat.

Védekezés töltéskoronát meghaladó árvízszint ellen nyúlgáttal [7]

A töltéskoronát meghaladó vízszint ellen nyúlgáttal, jászolgáttal (vagy ezek kombinációjával, jászolgátra helyezett nyúlgáttal) lehet védekezni. Jászolgátat 80 cm-es vízoszlopnál magasabb vízterhelés esetén alkalmaznak. Lehet alkalmazni a fóliaborítású földgátakat, akár 2-2,5 méter magassággal is, illetve ezek különböző kombinációit nyúl- és jászolgátakkal
A felkészítés során mi a nyúlgát magasítást gyakoroltattuk polgári védelmi szervezet tagjaival, szádfallal kiegészítve. A célunk a mozzanatok begyakorlása és elsajátítása volt, mely véleményem szerint maximálisan sikerült.

3. sz. fotó: Nyúlgát építése
Készítette: Bárdos Zoltán 2010.

4. sz. fotó: Nyúlgát szádfallal
Készítette: Bárdos Zoltán 2010.

Bordás megtámasztás [7]

A csúszásra erősen hajlamos, erősen átázott töltésen, vagy a már megcsúszott töltésnél bordás megtámasztás alkalmazásával lehet jó eredményt elérni. A megcsúszott vagy nagymértékben átázott töltés mentett oldalán ellensúlyként, először a töltésláb menti 2 méter széles sávban, majd ezt követően a rézsűre földes zsákokat, homokzsákokat helyeznek (esetleg több rétegben is) egymásra és egymás mellé úgy, hogy azok között megfelelő hézag maradjon. Az így képzett zsákréteg lényegében a töltésszelvény erősítését jelenti, a töltés megtámasztása mellett súlyával is nyomást ad a rézsűcsúszás ellen, ugyanakkor pedig a töltésen átáramló vizet nem folytja be a töltéstestébe, mert a víz a bordák közötti részen távozhat. Ennél a foglalkozási helynél a gát test megcsúszásának megvédését gyakorolták a foglalkozáson résztvevők.

5. sz. fotó: Bordás megtámasztás
Készítette: Bárdos Zoltán 2010.

6. sz. fotó: Bordás megtámasztás
Készítette: Bárdos Zoltán 2010.

Buzgár elfogás [7]

Az árvízvédelmi gátak legveszélyesebb jelensége a buzgár. A töltésre ható egyoldalú hidrosztatikus nyomás következtében a mentett oldalon alulról fölfelé ható áramlásból kialakult koncentrált vízfeltörés, ami a vízáteresztő réteg finomszemcséjű anyagával keveredve jelenik meg. Az ellene való védekezés leghatékonyabb módja ellennyomó medence kialakításával történhet.

7. sz. fotó: Buzgár elfogás
Készítette: Bárdos Zoltán 2010.

8. sz. fotó: Önkéntesek a védekezésben
Készítette: Bárdos Zoltán 2010.

Az előzőekből is látható, hogy az ár-és belvíz elleni védekezésre való felkészülés jól megtervezett és előkészített formában sikeresen és eredményesen valósulhat meg. A szakkiképzés megszervezése és végrehajtása során ismerte csak fel igazán a település vezetése a felelősségét a vízkárelhárítás, ezen belül az árvíz védekezés területén. A katasztrófavédelmi igazgatóságok felelősek a felkészítésért, de ehhez az adott település vezetésének a támogatása elengedhetetlen, hiszen a helyi lehetőségek ismerete mindennél fontosabb.

ÖSSZEGZÉS

A természeti és civilizációs katasztrófák által okozott veszélyhelyzetek száma nem csökken, sőt bizonyos időszakokban emelkedést mutat. Ezeknek a veszélyhelyzeteknek a kezelésében az elsődleges beavatkozókon túl, nagyon fontos szerep hárul az ún. másodlagos beavatkozókra, ezen belül a polgári védelmi szervezetekre. A polgári védelmi szervezetek

felkészítésére évek óta nincsenek források, ezáltal a felkészítéseket szinte lehetetlenség végrehajtani. A szervezetek alkalmazhatóságához szükség van a kiképzésükre, így meg kell találni (keresni) azokat a lehetőségeket, amelyeken keresztül forrásokat lehet biztosítani a felkészítésre. Ez mai világunkban pályázatok útján lehetséges, ami kissé szomorú, (hiszen a Pv. tv. 38-39. §-ban egyértelműen olvashatóak azok a polgári védelmi feladatok melyek finanszírozása állami feladat).
Mai korunkban egyre többször tapasztalhatjuk a természet erői okozta rendkívüli időjárási helyzetekből adódó veszélyhelyzeteket, ebből adódóan egyre nagyobb szükség van a településeken élők önmentő képességének a növelésére. Az elsődleges beavatkozók egy-egy rendkívüli időjárási helyzetben százas nagyságrendű riasztást kapnak, ezért nem tudnak mindenhová a kellő időben kiérkezni. A bekövetkezett káresemények felszámolásából a településeken élők is ki tudják venni a részüket, - természetesen nem a közvetlen élet vagy balesetveszély esetén – ha megfelelő felkészítést kapnak. Ennek az önmentő képesség növelésének óriási a jelentősége jövőben, mivel ezek az önkéntesek a településeken élnek ők tudnak a leghamarabb beavatkozni és a nagyobb károk keletkezését meg tudják akadályozni. A települések és az egyes emberek kiszolgáltatottságát a természet erőivel szemben, az állami kárelhárító szervekkel való közös összefogással lehet elfogadható mértékűre csökkenteni. Ehhez a civil szférának és az önkormányzatoknak is minden tőlük telhetőt meg kell tenniük, ahogy a katasztrófavédelmi törvény fogalmaz**: „**A katasztrófák megelőzése és az ellenük való védekezés (a továbbiakban: katasztrófavédelem) nemzeti ügy. A védekezés egységes irányítása állami feladat. Minden állampolgárnak, illetve személynek joga van arra, hogy megismerje a környezetében lévő katasztrófaveszélyt, elsajátítsa az irányadó védekezési szabályokat, továbbá joga és kötelessége, hogy közreműködjön a katasztrófavédelemben[20]”.
Cikkemben Fejér megye ár-és belvíz veszélyeztetettségét mutattam be, valamint a megyében megalakított területi rendeltetésű árvízvédelmi komplex polgári védelmi szervezet szakkiképzésének előkészítését és megvalósítását ismertettem, ezzel egyfajta módszert ajánlok a többi szervezet felkészítéséhez, hiszen mi előttünk nem volt egy példa vagy ajánlás, hogy ma ezt a felkészítést hogyan célszerű végrehajtani. Tökéletesíteni, továbbfejleszteni bizonyára lehet, de a kiinduláshoz egy jó alapot szolgálhat. Jelen munkámban nem foglalkozom a 2010. május-júniusi rendkívüli időjárási helyzet következtében kialakult ár-és belvízvédekezésnél az önkormányzatok szerepével, végzett munkájukkal, valamint a polgári védelmi szervezetek alkalmazásával. Ezen témák a következő írásomban kerülnek feldolgozásra és kifejtésre.

HIVATKOZÁSOK

[1] Állami Számvevőszék 0708. számú jelentése a települési önkormányzatok vízrendezési és csapadékvíz elvezetési feladatai ellátásának ellenőrzéséről 2007. április, http://www.asz.hu/ASZ/jeltar.nsf/0/B0E0F387C1F6A2F9C12572D0003024D5/$File/0708J000.pdf letöltés ideje: 2009. 11. 04.

[2] Állami Számvevőszék 0518. számú jelentése a természeti katasztrófák megelőzésére való felkészülés ellenőrzéséről, 2005. május,

[20] 1999. évi LXXIV. Törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről 1. § (1-2) bek

http://www.asz.hu/ASZ/jeltar.nsf/0/C132B0D27D2EDD5CC1257000003EA2CE/$File/0518J000.pdf letöltés ideje: 2009. 11. 05.

[3] Tunyogi Dóra Földi László: 2006. évi magyarországi árvíz során végzett elhárítási munkálatok elemzése, különös tekintettel a Magyar Honvédség szerepvállalására http://www.hadmernok.hu/archivum/2007/2/2007_2_tartalom.html letöltés ideje: 2010. 05. 05.

[4] 1995. évi LVII. törvény a vízgazdálkodásról

[5] 1996. évi XXXVII. törvény a polgári védelemről

[6] 13/1998. (III. 6.) BM rendelet a polgári védelmi felkészítés követelményeiről

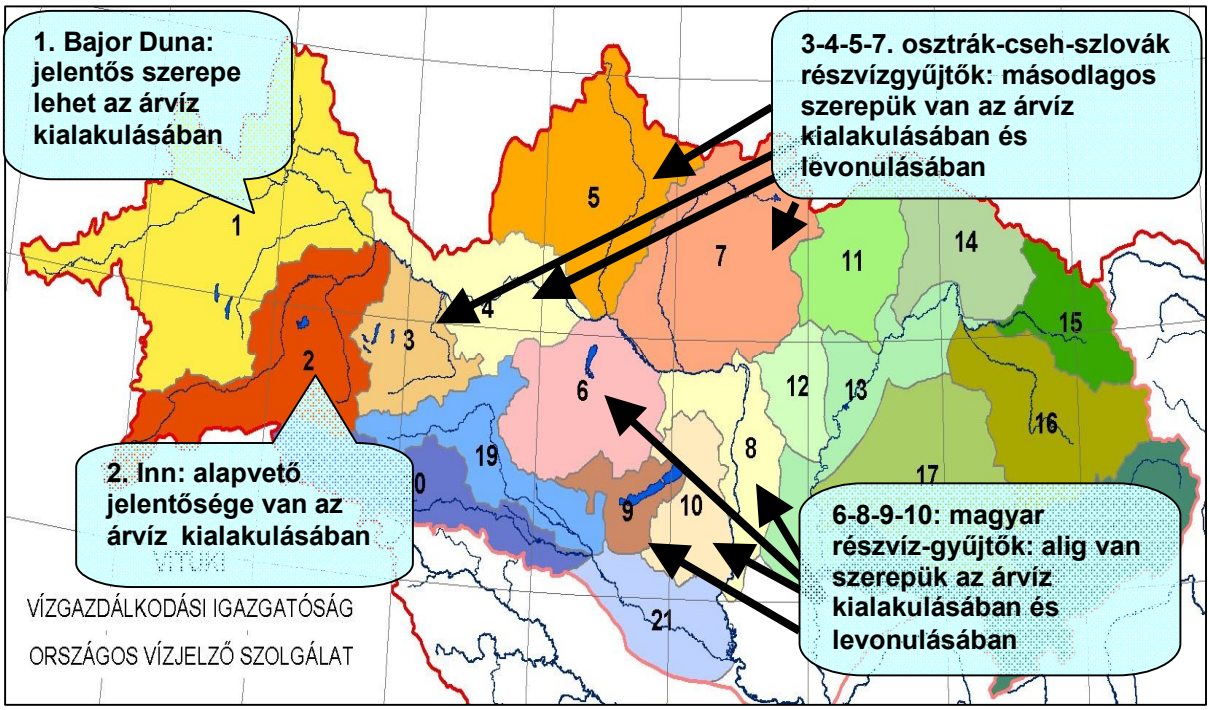
[7] Ismerettár: Árvízi jelenségek http://www.vkki.hu/index.php?mid=350 letöltés ideje: 2010.
05. 04.

[8] Dr. Varga Imre: Elgondolás a polgári védelmi kötelezettség alapján létrehozott szervezetek felszereléséről, felkészítéséről Polgári védelmi szemle 2008. 2. szám 27-40. old
http://www.mpvsz.hu/letoltes/pvszemle/pv2008_2.pdf letöltés ideje: 2010. 05.05.

A Duna vízgyűjtője

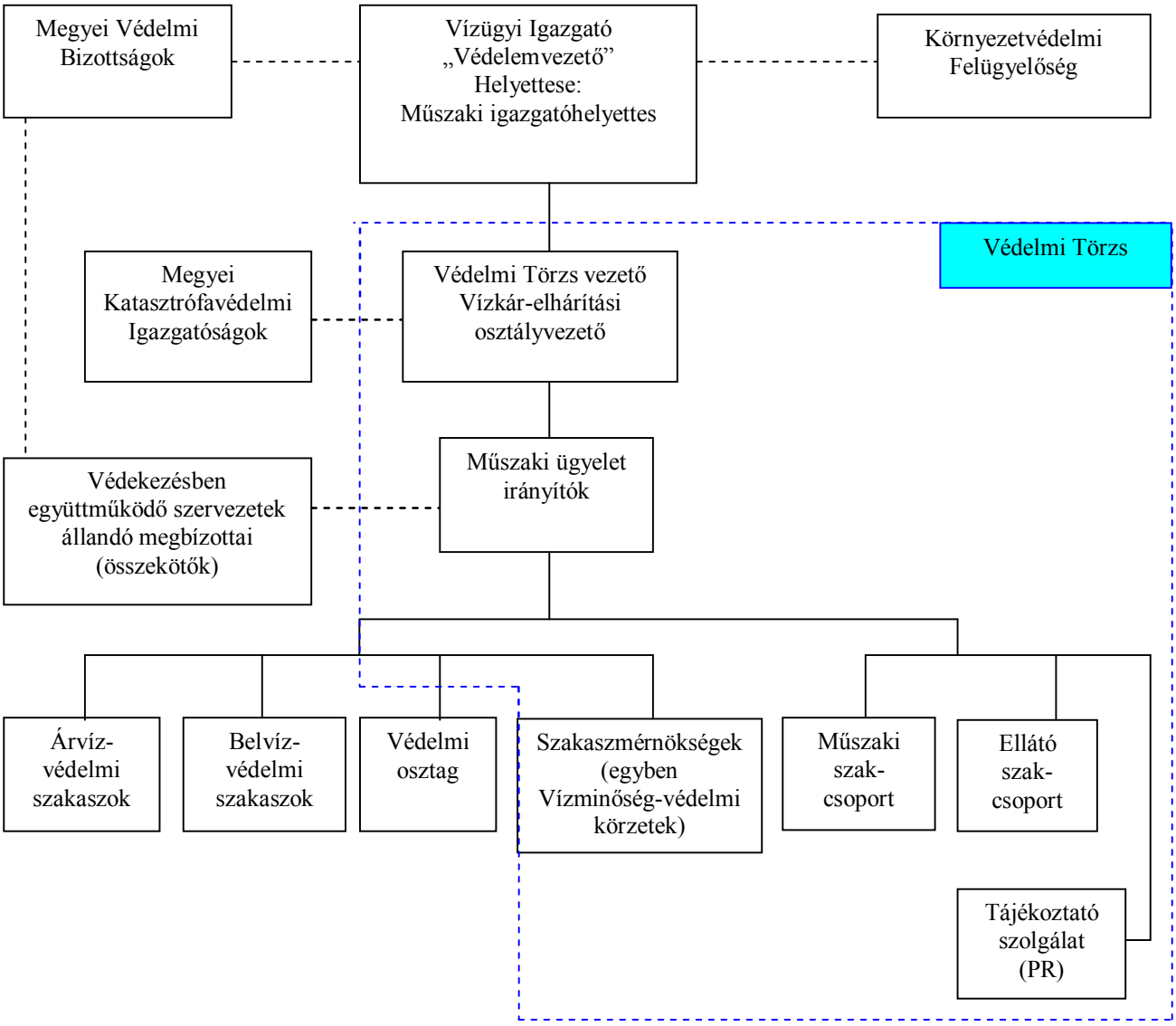
A Duna közvetlenül 10 országot, a vízgyűjtő területe további 9 országot érint. Teljes hossza: 2826 km, teljes vízgyűjtője 817 000 km^2.

A Duna részvízgyűjtői



Forrás: VITUKI Vízgazdálkodási Igazgatóság Országos Vízjelző Szolgálat

A VÍZÜGYI IGAZGATÓSÁGOK VÉDEKEZÉSI SZERVEZETÉNEK VÁZLATA



Forrás:http://www.kdtvizig.hu/

HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Farkas Csaba
csaba.farkas@corvus-aircraft.hu

Óvári Gyula
ovari.gyula@zmne.hu

A MAGYARORSZÁGI REPÜLŐGÉPGYÁRTÁS ÚJJÁSZÜLETÉSE – AZ INNOVATÍV TERVEZÉS ÉS MEGVALÓSÍTÁS ESZKÖZEI

Absztrakt

Kellő előkészítés, megfelelő innovatív tervezés és kitartás még a magyar viszonyok között is lehetővé tehetik, hogy világszínvonalú könnyű repülőgépet állítsunk elő.

Sufficient preparation, innovative instinct and endurance allow, even during the Hungarian circumstances, to manufacture a world's state-of-the art, light, industrially produced aircraft.

Kulcsszavak: *repülőgép, ipar ~ aircraft, industry*

Bevezetés – a Corvus Aircraft Kft-ről röviden

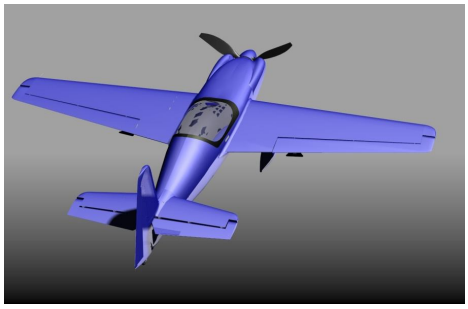
A Corvus Aircraft Kft. megalakulásakor céljául tűzte ki, egy merőben új szerkezeti felépítésű, korszerű saját tervezésű repülőgépek gyártását, szakítva a hagyományos félhéj sárkány építési elvvel, és kompozit repülőgépeket kínálni az ultrakönnyű és túra-, kiképző repülőgépek piacán. Az első ilyen légijárművünk a Corvus Corone MK I típus volt, amit 2005-ben mutattunk be egy németországi kiállításon.

Ennek sorozatgyártása 2006 elejétől indult és ez évben egy újabb típussal jelent meg a cég a Corone MK II ultrakönnyű változattal, amiből később a Corvus CA-21 Phantom (1. ábra) repülőgépet fejlesztettük ki. A Phantom európai export változatát a legmagasabb tervezői szervezet, a német DULV, LTF-UL építési előírásai szerint alakítottuk ki, ami 2008. februárban megkapta a német típusengedélyt. Ennek az amerikai export változata a Corvus Falcon. A Phantom és Falcon modellek kétszemélyes, kiképző-, gyakorló iskolagépek, de közkedvelten alkalmazzák sport és túra célokra is. Teherhordó sárkány szerkezete, teljes egészben prepreg technológiával kialakított kompozit héjszerkezet, bizonyos nem teherviselő és másodlagos teherviselő részek alumínium és hegesztett acél elemekből épülnek fel. A világ

különböző pontjain közel 30 repülőgépünk repül szélsőséges időjárási körülmények között, így Dél-Afrikában, Amerikai Egyesült Államokban, Egyesült Arab Emirátusokban, Thaiföldön, Németországban, Olaszországban, Spanyolországban és természetesen Magyarországon.

A Corvus Aircraft Kft. a legmodernebb CAE (*Computer Aided Engineering* - számítógéppel támogatott mérnöki tevékenység) alapú tervező rendszereket vezette be és integrálta a gyártás egyes munkafolyamataiba. Mindezek eredményeként konstrukcióink fejlesztési ideje és költségei nagymértékben csökkentek. Részben a magas fokú CAE háttér infrastruktúrának köszönhetően vállaltuk el 2008 nyarán, Besenyei Péter, a Red Bull Air Race versenypilótája felkérését, egy korszerű, merőben új tervezői megfontolásokat igénylő, speciális *„air race”* repülőgép kifejlesztésére (2. ábra).

1. ábra *Corvus CA-21 Phantom*



2. ábra *Corvus CA-41 Racer*

Az elhatározást tettek követték, a Corvus CA-41 Racer fejlesztési munkálatai lezárultak és reményeink szerint ezen évadban a Windsori, de legkésőbb a Budapesti futamon Besenyei Péter rajthoz áll új repülőgépével, aminek fő teherviselő szerkezeti eleme a törzsrács, 25CrMo4 nemesíthető acélból készített hegesztett szerkezet, az irányfelületek, a szárny és a borítás kompozit szerkezet.

Korszerű repülőgép tervezés, avagy a CAE előnyei

A fejlett ipari nagyhatalmak repülőgépgyárai körülbelül 30 évvel ezelőtt kezdték el alkalmazni és rendszerükbe integrálni a számítógépes tervezőrendszereket. Voltak olyan kutatóintézetek, melyek külön divíziókat hoztak létre több száz rendszerfejlesztőt foglalkoztatva, hogy a saját maguk igényeinek megfelelően fejlesszék ki tervezőrendszereiket. A NASA például az 1960-as évek közepétől kezdte el fejlesztését a rajzoló-tervező rendszernek (CAD), majd pár év múltán már az FEM (Finite Element Method - véges elem módszer) alapjait fektette le, melynek neve NASTRAN (NASA Structural Analysis) lett.

A számítógéppel támogatott tervezés, avagy CAD (Computer Aided Design) forradalma világviszonylatban a ’90-es évek elején vette kezdetét és napjainkig - közel 15 év alatt - az ipar robbanásszerű forradalmi változása kísérte végig, és fejlődött a addig, hogy lehetővé tette egy termék tervezését, elemzését, gyártás helyességének-használhatóságának ellenőrzését és élettartam-becslését, annak valós fizikai megléte nélkül. Összefoglaló néven ezt nevezzük CAE-nak (Computer Aided Engineering), melynek magyar megfelelője számítógéppel támogatott mérnöki tevékenység. Mindez egy olyan átfogó komplex tervezési eljárás gyűjtőneve, ami olyan egymásra épülve magában foglalja az előzetes koncepció

kimunkálásától, a részletes külső és belső tervezésen keresztül a gyártás folyamata és technológiája kimunkálásának minden elemét, sőt a virtuálisan kész termékkel terhelési és/vagy egyéb működési modell kísérletek végrehajtását is. Az 1. számú táblázat egy ilyen CAE eljárás lehetőségeit, (felülről lefelé haladva) logikai folyamatát mutatja be.

Napjaink mérnöke már más tervezési filozófiával fejleszti az eszközöket, mint elődei tették azt 30-40 éve. A XXI. századi tervezés alapvető mozgatója a költséghatékonyság. A repülés viszonylag magas költségei és az elvárt magas biztonság a világ vezető ipari ágazatává emelte a repülőgépgyártást. A CAE alkalmazások nagy részét is a repülőipar és a hadiipar fejlesztette önmagának, természetesen ma már egyéb ipari szegmenseket is átfog. Repülőipari alkalmazását tekintve a CAE egyik előnye, hogy a prototípus legyártását megelőzően a fő szerkezeti és/vagy gyártási elemeken, de akár az egész repülőgépen is elvégezhetjük a valóság modellezését a virtuális térben. Ezzel pénz, idő és újabb módosított prototípusok legyártása takarítható meg. A virtuális szélcsatorna ellenőrzéseket és szilárdsági vizsgálatokat követően igen jó közelítéssel kaphatóak azon eredmények, melyeket a valós életben megbízhatóan hasznosíthatóak. A virtuális vizsgálatok újrakezdése nem emészt fel plusz járulékos többletköltségeket. További előnye, a parametrikus rendszerekkel integrált szimulációk alkalmazásának, hogy segítségükkel könnyen és gyorsan elemezhetőek a különböző modifikációjú virtuális prototípusok, melyekkel még azt is megbízhatóan prognosztizálható, hogy egyes szerkezeti elemi mikor és melyik keresztmetszetében törnek el, mennek tönkre. Amennyiben a megfelelő integrált CAE rendszer céltudatosan kerül alkalmazásra egy repülőgép fejlesztő üzemben, akkor a prototípus legyártása, földi- és légi tesztjeit megelőzően a múltbéli tapasztalatok alapján, közel 90% pontossággal előre jelezhető olyan aerodinamikai viselkedések és jellemzők, melyek évekkel ezelőtt csak a valós tesztek alkalmával voltak mérhetőek. Ilyen például az emelkedőképesség, a fordulósugár, a különböző külső kormányszervek és/vagy szárnymechanizációs eszközök hatásosság, a terhelés hatására jelentkező rugalmas alakváltozások, lengésképek vagy például a frekventált teherviselő és/vagy funkcionális elemek maximális élettartamra számolt túlélési rátája, stb. A technika fejlődése nem áll meg és a jövőbeli kutatások célja a virtuális modell-kísérletek megbízhatóságának, valósághűségének és komplexitásának további javítása. A CAE rendszerek további lényeges eleme az alkatrészek fizikai viselkedésének modellezésére szolgáló ún. analízis eszközök, melyek egy részét az 1. sz. táblázat harmadik sora foglal össze.

Általános CAE megoldás ***1. táblázat***

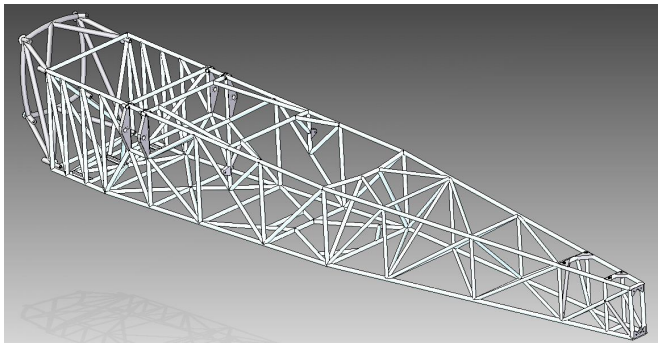
PLM = PRODUCT LIFE MANAGEMENT (ÉLETCIKLUS KEZELÉS ÉS KÖVETÉS)	CAE		
	Mérnöki munka fázis	**CAE program részegység és megoldás**	**Magyar megfelelő**
	Geometria és alkatrész modellezés	CAD 2D / 3D PART	Számítógéppel támogatott tervezés 2÷3 dimenziós test modellezés
	Alkatrész szerelési környezet modellezés	CAD 2D / 3D ASSEMBLY	Számítógéppel támogatott tervezés 2÷3 dimenziós összeállítási környezet modellezés
	Alkatrész és összeállítási környezet fizikai viselkedésének elemzése	FEA, FEM, DYNAMIC SIMULATION, MOTION SIMULATION, FLOW AND THERMAL SIMULATION, ELECTRIC SIMULATION	Végeselem analízis és vizsgálat, dinamikai, mozgástani, áramlástani, hőtani, elektromos viselkedések szimulációja és elemzése
	Alkatrész gyártás előkészítése, gyártási szimulációja	CAM, CAM-TOOL SIMULATION	Számítógéppel támogatott gyártás és gyártás szimuláció
	Elemzés utáni újra tervezés és újra ellenőrzés	CAD 3D PARAMETRIC SYSTEMS, PDM	Számítógéppel támogatott tervezés 3 dimenziós parametrikus környezet, revíziókövetés
	Kisegítő alkalmazások	CAD PHOTORELASTIC, SHEET METAL DESIGN, MOLD DESIGN, PIPING&CABLE DESIGN	Valóskörnyezet fotórealisztikus megjelenítése, lemez forma, öntőforma, kábelezés
	Gyártási és műhelyrajz automatikus generálás	CAD DRAWINGS	Számítógéppel támogatott gyártás kész műszaki rajzok

Innovatív tervezés és gyártás – Corvus Racer 540 Red Bull Air Race Besenyei Péter műrepülő világbajnok új repülőgépének fejlesztése

Hosszú évek során összegyűlt tervezői, gyártói és üzemeltetési tapasztalatok birtokában mondtunk igent 2008 augusztusában egy új, nagyteljesítményű, kimagasló terhelhetőségű és manőverező-képességű repülőgép kifejlesztésére. A Corvus Aircraft Kft 1,5 éves fejlesztői munkájának eredménye, hogy terveink szerint a 2010-es Red Bull Air Race versenysorozat második felétől Besenyei Péter már a Corvus Racer 540 repülőgéppel állhat rajthoz.

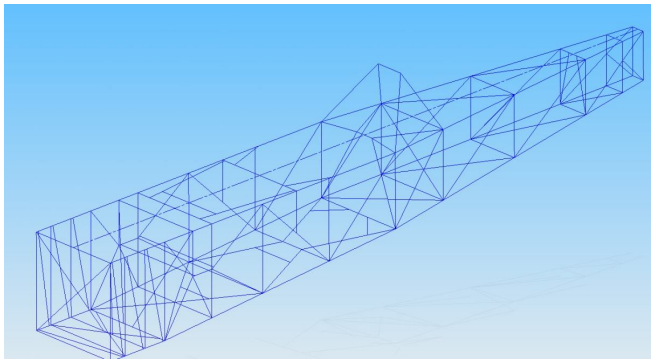
A hegesztett törzsrács tervezési és gyártási folyamata

A repülőgép fő szerkezeti elemének Solid Edge ST rendszerben készített CAD modellje a 3. ábrán látható. A modellezést a tartószerkezet alkalmazás segítségével végeztük el.



3. ábra *Törzsrács Solid Edgeben készült modellje*

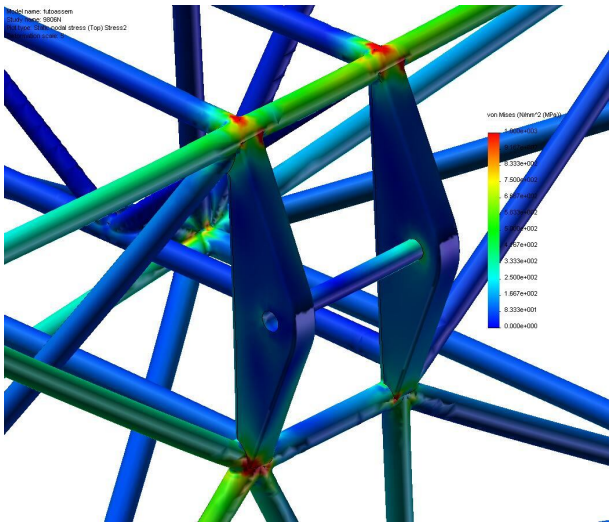
A törzsrács többszörösen összetett, és szilárdsági szempontból az egyik legkritikusabb teherviselő elem. A csatlakozó csomópontjaiban ébredő a koncentrált nyíróerők meglehetősen nagyok, például a szárny bekötési pontban, üzemi terhelés esetén $F = 41.000\ N$ nyíróerő lép fel oldalanként. A tözsrácshoz kapcsolódik minden további sárkányelem (szárny, vezérsíkok, futóművek, motor) és veszi fel az ezekről átadódó terheléseket is, de ebben helyeztük el az üzemanyagrendszert, a műszereket, a mozgató rudazatokat és a pilótát is. E váz szerkezet alapja a 3D „drót modell" vázlata (4. ábra).



4. ábra *A törzs tervezésének alap drótváz modellje*

Ennek megrajzolását, valamint a csőszelvények adatainak megadását követően - figyelve a csatlakozási csomópontok gyártási követelményeire - alakult ki a hegesztett váz. Az egyes csövek illesztése során tapasztalható a Solid Edge ST rendszer „intelligens képessége" azáltal, hogy, folyamatosan figyel a már meglévő és újonnan beépítésre kerülő elemek aktuális helyzetére. A rács gyártása során először az alsó és felső keretet hegesztettük össze sablonban, majd a függőleges elemek bekötése következett, végül a kereszt és diagonál merevítő elemekre került sor. A tartószerkezet tervezése is ebben a sorrendben történt, az egyes elemeket ennek megfelelően lépésről-lépésre illesztettük rá a 3D drótváz modellre. A modellezés befejeztével a gyártáshoz vágási lista és darabjegyzék, valamint minden elemről az önálló alkatrész modell állt rendelkezésre és. A tervezőrendszerbe az alkalmazott csövek, 25CrMo4 anyagminőségét definiálva már a fejlesztés legelején ismerté vált a rács szerkezet tömege. Ennek tervezése úgynevezett párhuzamos vagy un. szimultán eljárással történt, ami azt eredményezte, hogy járulékosqan a szilárdsági méretezés, ellenőrzés is megtörtént. A Solid Edge ST alkalmazási rugalmasságát kihasználva, a numerikus szilárdsági számítások több rács elrendezés is elkészülhetett. Ezeket, külön-külön, egymástól független FEA alkalmazásokban (Cosmos, Femap) elemeztük.

A tervezés során több szimulációs eljárást alkalmaztunk azért, hogy az egyes szerkezeti elemek áramlástani és szilárdsági viselkedését modellezhessük. Az egyik legérdekesebb elemzést a hegesztett törzs rácsszerkezetén és a motortartó bakon hajtottuk végre. Szimuláltuk a szárnyakon, vezérsíkokon fellépő légerők keltette, a törzs bekötési és csatlakozási csomópontjaiban átadódó nyíróerők hatását két állapotra, a *„limit load condition”-re*, azaz repüléskor a maximális statikus üzemi terhelésre, valamint az *„ultimate load condition”-re*, a törő határterhelésre. Utóbbi - a szerkezetet minősítésekor is szükséges bevizsgálás részeként – törést nem, de maradó deformációt megenged. A limit terhelések vizsgálatakor nem találkoztunk olyan kiterjedt területtel vagy varrat-átmenettel, ahol az ébredő feszültség a folyáshatár értékét meghaladta volna, de a törő terheléskor egyes elemi csomópontokban, már néhol lokálisan kimutatható volt a szakítószilárdság értéke, de kiterjedt zónát ebből sem észleltünk sehol. Számunkra a legfontosabb a kritikus csőcsatlakozások és a legjobban terhelt csövek meghatározása volt. Végig figyelembe vettük azt a tényt, hogy a szerkezet rögzítettsége következtében járulékos feszültségek is jelentkeztek az egyes elemeken, ezért döntöttünk úgy, hogy a feszültségek elemzésekor a bennük fellépő átlagos állapotot *(average stress)* tekintjük a méretezés és ellenőrzés kiinduló alapjánk. Az 5. ábra példaként a szárny-törzs csatlakozás, vagyis a főtartó bekötés feszültség eloszlását szemlélteti.



5. ábra *Feszültség eloszlás a főtartó bekötés körül*

A hegesztett törzsrács gyártás-technológiai kidolgozása

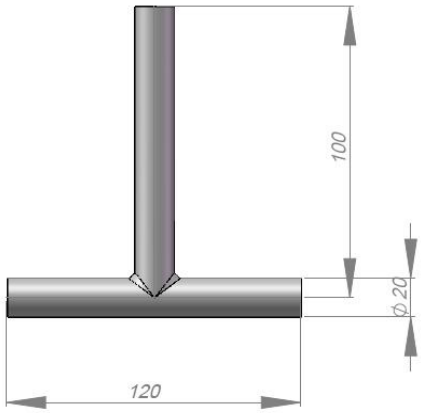
A repülőgép rendeltetéséből adódóan a vázszerkezet igen nagy, váltakozó (túl-) terhelésnek van kitéve üzemi körülmények között, így a bevizsgálás során a 18-szoros szilárdsági túlterhelhetőséget kellett igazolni kellett. A hegesztett rács alap-anyagának ebből adódóan a repülőiparban elterjedt nemesített acélt 25CrMo4 csövet választottunk. Ismert, hogy ezek hegesztése

legtöbb esetben nem egyszerű feladat, csak gondos előzetes és utólagos intézkedésekkel hajtható végre. Ilyen acélok hegesztése során leggyakrabban a hőhatásövezetben hidegrepedés érzékenységgel kell számolni, ami keletkezésének oka összetett, megjelenését rendszerint sok tényező együttes hatása befolyásolja. Nemesített acélok esetében a hegesztéskor keletkező nagy keménységű szövetelemek, (pl. martenzit vagy bainit) kis alakváltozó képességű szövetszerkezetet eredményeznek, ami a hidegrepedés kialakulását elősegíti.

A Tennant GmhH-tól beszerzett csövek kémiai összetétele a következő: C = 0,27%, Mn = 0,71%, Si= 0,27%, S = 0,026%, P = 0,012%, Cr = 1,06%, Mo = 0,24%, Ni = 0,095%

Ebből adódóan a karbonegyenérték:

$$K = C + \frac{Mn}{6} + \frac{Cr}{5} + \frac{Mo}{4} + \frac{Ni}{15} = 0{,}27 + 0{,}118 + 0{,}212 + 0{,}06 + 0{,}0063 = 0{,}66\%$$



6. ábra *A vizsgált próbatest méretei*

Mivel a karbonegyenérték magas értékűre adódott, már ebből látható volt, hogy előmelegítés szükséges a hegesztést megelőzően. A megfelelő kötés vizsgálatához próbatesteket készítettünk és különféle technológiai paraméterek változtatásával, (pl. előmelegítés, utóhőkezelés, áram-erősség) igyekeztünk a legmegfelelőbb eljárást kidolgozni. A próbatestek 20 x 1,0 mm-s csövekből a 7. ábrának megfelelően hegesztett T-idomok voltak.

A vizsgálatok azt mutatták, hogy előmelegítés, utólagos hőkezelés és impulzus technika alkalmazása képes a legstabilabb kötést biztosítani. Így a hőhatásövezet képlékenysége javul, az alakváltozó képessége nő. További előny, hogy az esetleges varrathibákból kiinduló repedések terjedését az anyag képlékeny alakváltozással, nagy valószínűséggel megakadályozza.

A valóság problémája

A valóságban a kemencében történő hőkezelést nem tudtuk elvégezni fizikai korlátok miatt, így minden varratot lokálisan kellet fölmelegíteni valamivel kisebb hőntartási idővel, mint amit a próbavizsgálatok mutattak. Egyebek mellett ez okból is helyeztünk el nyúlásmérő bélyegeket, azaz, hogy meggyőződhessünk arról valós repülési körülmények között mekkora szilárdsági tartaléka van a szerkezetnek a folyáshatárhoz képest.

A törzsrácson a hegesztését követően elvégeztük a varratok anyagvizsgálatát. Ennek során a következő módszereket alkalmaztuk:

- varratok ellenőrzése penetrációs eljárással;
- varratok ellenőrzése nyomáspróbával;
- szilárdsági bevizsgálás, terheléspróba.

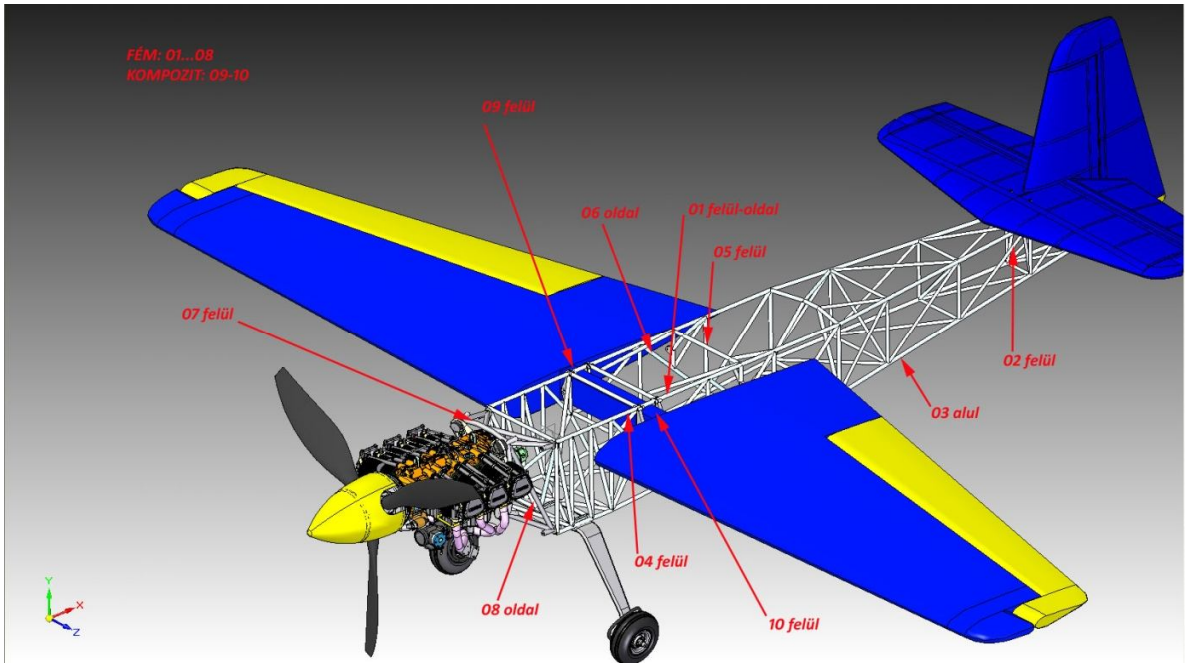
A hegesztést követően, annak megfelelőségét nyomáspróbával ellenőriztük, a csövekben Δp=2 bar belső túlnyomást létrehozva és azt 24 órán keresztül fenntartva. Nyomásesést nem tapasztaltunk.

A szerkezet szilárdsági ellenőrzése

A Racer 540-es típusjelű, nagy terhelhetőségű, speciálisan az *„air race”* verseny-sorozathoz kifejlesztett repülőgép. Ez tette indokolttá egy egyedi fejlesztésű terhelés rögzítő berendezés megépítését, melynek segítségével a szerkezeti elemeken ébredő külső erőhatásokból ébredő feszültségek mérhetőek, tárolhatóak és elemezhetőek. E berendezés segítségével több lépcsős

kontrolt alkalmazhatunk és repülésbiztonsági szempontokat figyelembe véve állapíthatjuk meg a szerkezeti elemek terhelhetőségi tartományait.

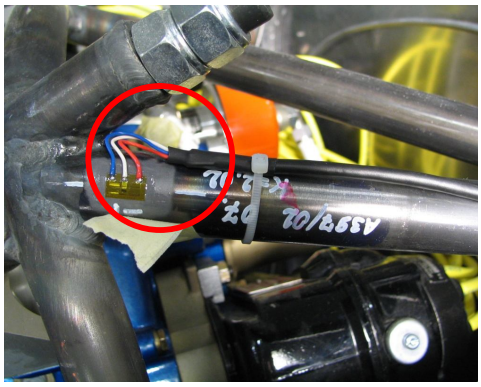
A vizsgálat elsődleges célja, a visszacsatolás, a szilárdsági numerikus és végeselem számítások eredményeinek összehasonlítására, a földi szerkezeti bevizsgálás és a valós légerők okozta hatásokkal. Ebből adódóan a számítások során alkalmazott módszerek és peremfeltételek megfelelősége, azok jósága ellenőrizhetővé válik. Másodsorban pedig megállapítható, hogy az egyes extrém (túl-)terhelések fellépésekor a szerkezet milyen deformációt szenved, az ébredő nyúlások mennyire közelítik meg az anyagszerkezetek rugalmas alakváltozási határainak szélső értékeit. A rendszer kialakítását az SGF Technológia Fejlesztő Kft-vel közösen végeztük, akik igényeinknek megfelelően építették meg a terhelés regisztert és alkották meg a működéshez szükséges vezérlő szoftvert. A DABAS fantázianevű berendezés 16 mérő csatornán képes érzékelni, mintavételezési sebessége másodpercenként 100 darab, minden külön telepített szenzor esetében (egy szenzor egy csatornának felel meg).



7. ábra *A repülőgépen elhelyezett nyúlásmérő bélyegek helye*

A 7. ábrán látható a jelenleg alkalmazott 10 mérőpont, ahová nyúlásmérő bélyegek helyeztünk, az ott fellépő helyi feszültségek regisztrálására. Az alkalmazott „intelligens” szoftver a nyúlásokat [%] automatikusan átszámítja feszültségekre [MPa], így az elemzések alkalmával mindkét értékről elsődlegesen információt kapható.

8. ábra *A DABAS kiértékelő felülete.*



9. ábra *A motortartó bakon elhelyezett nyúlásmérő bélyeg*

A 8. ábrán a szoftver kiértékelő felülete, a 9. ábra a motortartó bakon a nyúlásmérő bélyeg elhelyezése látható.

Összefoglalás

Ismert, hogy az elmúlt évtizedekben Magyarországon több különböző rendeltetésű – döntően sportcélú - könnyűrepülőgép épült. Ezek egy része saját konstrukcióként, több pedig külföldről beszerzett kittek összeállításával született. A létrehozás körülményeit azonban rendszerint az egyedi, eseti, manufakturális (házi) előállítási viszonyok jellemezték. Az elkészült légijárművek korszerűségét, hatékonyságát, vizsgálva, a jellemzők széles spektrumával találkozunk.

10. ábra *Corvus Racer 540*

A **Corvus Racer 540** megépítése (10. ábra) és sikeres alkalmazása igazolja, hogy elszántsággal, kiemelkedő kreativitással, magas színvonalú szakmai felkészültséggel, innovatív hajlammal, a piac elvárásainak ismeretében, megfelelő közgazdasági felkészültséggel, Magyarországon, akár előzmények nélkül is létrehozható, professzionális, korszerű technológiával, iparszerűen előállított, világszínvonalú termék a repülőiparban is.

A létrehozott sikeres konstrukció hozzájárulhat a magyar repülőipar újjáéledéséhez, a szakmai kultúra továbbéléséhez és fejlődéséhez, illetve bázisául szolgálhat további fejlesztéseknek, hazai túra, illetve polgári és katonai hasznosíthatóságú kiképző repülőgépek kimunkálásához.

Felhasznált irodalom

1. Czvikovszky-Nagy-Gaál: A polimertechnika alapjai, Műegyetemi Kiadó Budapest, 2000.
2. Corvus Aircraft Kft belső dokumentációs rendszer, típuskézikönyvek
3. Eger: Proektirovanie letatelnih apparatov (orosz nyelven) MASINOSZTROENIE, Moszkva, 1984
4. G. Lubin: Handbook of Composites Reinhold in New York 2002.
5. Michael C. Y. Niu: Airframe Structural Design Lockheed Aeronautical Systems, Company Burbank, California USA 1990. ISBN No. 962-7128-04-X
6. Óvári Gyula dr.: A repülőgép-tervezés alapjai (multimédiás tansegédlet, kézirat) ZMNE BJKMK RLI, 2008.
7. Serge Aberte: Impact on Composite Structures, Cambridge England 1998. ISBN 0-521-47389-0
8. S. R. Reid and G. Zhou: Impact Behavior of Fibre-Reinforced Composite Materials and Structures Cambridge, England 2000. ISBN 1 85573 423 0