HADMÉRNÖK

A ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR
ÉS A HADMÉRNÖKI DOKTORI ISKOLA
ONLINE TUDOMÁNYOS KIADVÁNYA

VI. Évfolyam 2. szám 2011. június

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: Prof. Dr. Padányi József, a ZMNE mb. rektora
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Dr. Berek Tamás mk. őrnagy – ZMNE BJHMK egyetemi docens

Berki Gábor

Dr. Berkovics Gábor ny. mk. alezredes – ZMNE BJHMK egyetemi docens

Béres Deák Endre – MOL Magyar Olaj- és Gázipari Nyilvánosan Működő Részvény-társaság

Dávidovits Zsuzsanna – ZMNE HMDI doktorandusz

Erdei Gábor

Fleiner Rita – ZMNE HMDI doktorandusz

Gerő Péter – ZMNE HMDI doktorandusz

Prof. Dr. Halász László ny. mk. ezredes – ZMNE BJHMK egyetemi tanár

Harmati István – Budapesti Műszaki és Gazdaságtudományi Egyetem

Horvayné Fehér Judit – ZMNE HMDI doktorandusz

Horváth Tamás – MVM Zrt.

Inkovics Ferenc – ZMNE HMDI doktorandusz

Juhász Zsolt – MH Dr. Radó György Honvéd Egészségügyi Központ

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

Kisfaludi Péter – Budapesti Műszaki és Gazdaságtudományi Egyetem

Prof. Dr. Kende György ny. mk. ezredes – ZMNE BJHMK egyetemi tanár

Kozák Attila – Nyíregyházi Hivatásos Önkormányzati Tűzoltóság

Dr. habil. Krajnc Zoltán alezredes – ZMNE KLHTK egyetemi docens

Kuris Zoltán – ZMNE HMDI doktorandusz

Laczik Balázs – Hivatásos Önkormányzati Tűzoltóság Gyöngyös

Miskolczi Ildikó – ZMNE HMDI doktorandusz

Prof. Dr. Munk Sándor ny. mk. ezredes – ZMNE BJHMK egyetemi tanár

Pálinkás Yvett – Szent István Egyetem

Pápai Tibor őrnagy – Honvédkórház- ÁEK Sürgősségi Betegellátó Centrum

Dr. univ. Potóczki György – ZMNE HMDI doktorandusz

Prekup Zsolt – Nyíregyháza Rendőrkapitányság

Répás József – ZMNE BJHMK hallgató (MSc)

Rohr Linda

Schmidt Petra – ZMNE BJHMK hallgató (BSc)

Schüller Attila – ZMNE HMDI doktorandusz

Dr. Seres Görgy – ZMNE HMDI

Dr. Szakál Béla – Szent István Egyetem, Ybl Miklós Építéstudományi Kar, Tűzvédelmi és Biztonságtechnikai Intézet

Szegediné Lengyel Piroska – ZMNE HMDI doktorandusz

Remetei Dóra – ZMNE HMDI doktorandusz

Tibenszkyné Dr. Fórika Krisztina sz. százados – ZMNE BJHMK egyetemi docens

Török Szilárd

Veres Viktória

Dr. Zsigovits László ny. alezredes – ZMNE

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Berkovics Gábor
berkovics.gabor@zmne.hu

Krajnc Zoltán
krajnc.zoltan@zmne.hu

THE YUGOSLAVIAN/SOUTHERN SLAVONIC AIR FORCE UNTIL 1930

Absztrakt

A cikkben a szerzők bemutatják a délszláv légierő első 18 évét, elsősorban magyar katonai forrásokra támaszkodva. Déli szomszédunk tiszteletre méltó és eredményes erőfeszítéseket tett a XX. század harmadik évtizedében egy ütőképes légierő megteremtésére, fenntartására, s az azt kiszolgáló hadiipari képességek megteremtésére. 1930-ra már rendelkeztek a hadsereg szükségleteit kielégítő repülőerőkkel.

In this article the authors will describe the first 18 years of Yugoslavian Air Force, primarily relying on the Hungarian military sources. Our southern neighbour made respectable and successful efforts to create and maintain a powerful air force in the third decade of the XXth century, and to build up the military-industrial capabilities serving it. By 1930, they already had an air force which could serve the needs of their army.

Kulcsszavak: *légvédelmi tüzérség, légvédelem, „kis Antant” ~ Air Force, Yugoslavia, “small Entente”*

INTRODUCTION

In the first two decades of the twentieth century the spread and development of a still relatively new means of air warfare were explosively fast. In 1900 the first steerable ZEPPELIN type airship was built. The Wright brothers (Wilbur and Orville) drew the military's attention to airplanes with their successful experiment on 14 September 1903, of which military applicability became obvious very soon. Mainly German and French military circles devoted great care to them, but soon all the states - the so-called *"small states"* as well – and their armies too, began to build or buy fighters.

The military spread and the speed of their application were indicated by their usage in 1911 in French, German and Austro-Hungarian *"great practices"* for both reconnaissance and courier services. Its battle application took part no long after it: in 1912 the Italians used air devices in the Tripoli war not only for reconnaissance but for adjustment of fire and bombing as well.

For the question: *"How could these devices be repelled?"* there were two answers those times. One was by the plane itself. The other possible means – not excluding the first one, moreover along with it – was the developping of the artillery (anti-aircraft artillery soon). All European nations dealt with the latter question too, though they put less emphasis on them than on the airplanes.

During World War I it became increasingly common to *"extend warfare into the third dimension."* During the war aircrafts didn't only fulfill tasks like reconnaissance, courier service, battery control and fire adjustment, but also increasingly bombing troops and objects. Their roles and importance gradually increased and widened. This process didn't stop after the war, it is still a trend.

The air forces dealt with in this article was a part of military power of a nation, which was transformed in territory and name several times during the examined period.

They belonged to the Kingdom of Serbia until 1. December 1918, from that time on to Serbian-Croatian-Slovenian Kingdom, and from 3 October 1929 to the Kingdom of Yugoslavia.

THE BEGINNINGS OF MILITARY AVIATION IN SERBIA

For the need of the capability in the third dimension, Serbia deployed air forces relatively early, in 1912, when it sent officers to France to learn engineering and it organized an air squad out of French airplanes. This squad was destroyed very early in 1914 due to the lack of resupply in the beginning of WWI.[1] The French reconnaissance squad commanded here was also destroyed in 1915 in retreat.[2] A new own squad was only set up again in 1916. During the break-up of Austro-Hungarian Monarch and the fronts, the Serbian forces acquired a significant quantity of aircrafts, which majority was taken from the Monarchy's stock from the southern airports, primarily from Újvidék[3], from the remaining aircraft stocks. This way they were able to set up four aircraft squadrons.

1 Vitéz Szentnémedy Ferenc: Jugoszlávia mint légi hatalom, Magyar Katonai Közlemények 1930/9. p. 882

2 same source

3 We use the names of territories according to how they were used those times or how you can find them in military sources.

Year	Yugoslavia		Source
	pieces of aircraft	air squads	
1912		1	MKK 1930/9. p.882.
1916		1	MKK 1930/9. p.882.
1918		4	HL, VKF p.1. 5149/T 1928.
1919	200		MKK 1930/9. p.882.
1922		5	HL, VKF p.1. 5149/T 1928.
1922	70		MKK 1930/9. p.883.
1923	70	6	HL, VKF p.1. 5149/T 1928.
1925	110		MKSZ 1931/5. p.245.
1926	160		HL, VKF VI-p.1. 6236/T 1926.
1927	160	11	HL, VKF p.2. Szn./528 B 1927.
1927	200	25	HL, VKF p.1. 5149/T 1928.
1928	248		HL, VKF p.2. 23693/T 1928.
1929	400	25	HL, VKF p.1. Hr.1999. 1929.
1930	650	29	HL, VKF p.2. 118985/Eln. 1931.

1. table. The squads and the amount of aircrafts of Yugoslavian Air Force[4]

On[1] December 1918 the Serbian-Croatian-Slovenian (SCS) Kingdom was formed, which already owned a already relatively huge amount of air force, though it very early became outworn. In 1919, the air force of SCS consisted of about 200 planes either preyed from the Monarchy or given by the French. These devices became, however, very quickly worn-off, and because of the problems arisen from their need of serving, repairing and obsolescence, they became inapplicable in battle. By 1922, there remained only 60-70 pieces of applicable aircrafts. These times the SCS only owned three very low-power but unquestionably modern aircraft factories, and further nine factories manufacturing aircraft supply materials and devices.

For all these reasons - despite the aviation industry improvements later on - the Yugoslavian Air Force practically needed significant import during the examined period. After the World War I, states not affected by peace treaties - including the SCS as well - faced new military tasks. The construction, operation and continuous modernization of air defense and air forces in peacetime became a current problem. Important areas had to be grounded in theory and implemented in practice.

4 The resources available to know the amount of air devices and squads often raise doubts. As for example Magyar Katonai Közlemények and Magyar Katonai Szemle often merge the information about battle ('front line') aircraft, training, supply and civilian aircraft.

NAME	FUNCTION	WHERE FROM	YEAR	VMAX (KM/H)	PEAK (M)	MOTOR TYPE AND EFFICIENCY (HP)	D-CO.(KM) OR FLYING TIME (HOUR)
Spad 7	hunter	imported (French)	1916	191	5485	Hispano 175	2.25 hours
Spad 20	hunter	imported (French)	1921	274	8500	Hispano 300	2.5 hours
Devoitine D1	hunter	imported (French)	1923	230	8500	Hispano 300	2.5 hours
Breguet XIX A-2	reconnaissance. bomber	by license, national	1923	240	8500	Lorraine 400	3 hours
Breguet XIX B-2	bomber	by license, national	1923	215	8000	Renault 450	3 hours
Devoitine D9	hunter	imported (French)	1924	228	8000	Bristol 400	2.5 hours
Potez XXV	reconnaissance. bomber	by license, national	1924	230	7200	Lorraine 450	2.5 hours
Junker G-24	bomber	imported (German)	1925	175	3800	Junkers 690	
Fokker T9	bomber	imported (Dutch)	after 1925	208		3x365	1200 kms
Fizier	reconnaissance	national	1926	192	6000	Maybach 260	
Ikarus I.M.	reconnaissance	national	1926	200	6500	Liberty 400	
Ikarus I.O.M.	reconnaissance	national	1927	170	4500	Liberty 375	
BH-33	hunter	imported (Czechoslovakian)	1927	270	9500	Bristol 420	

2. table. The important types of A/C of the Yugoslavian Air Force[5]

THE ORGANIZATIONS OF YUGOSLAVIAN/SOUTHERN SLAVONIC AIR FORCE IN THE TWENTIES

By 1922, air force squads were increased to five, and from1924 they began to purposefully build out the air force, and two aircraft regiments were set up.[6] According to plans they intended to make as many air force units as they had on land, which meant five.

From 1925 they started to implement their own production of aircrafts, though, then they only equipped their flying schools with Icarus products. In 1927, the 3rd aircraft regiment was founded and the already existing two air units were also filled up, especially with foreign supplies. 400-450 aircrafts were purchased mainly from French suppliers, and by French military equipment loan. By the end of the twenties, the SCS Air Force –according to the battle order - owned seven aircraft regiments, but not all of them were actually formed or

5 Repülőgép Enciklopédia. Gemini kiadó. Budapest 1992.

Angelucci. Enzo: The Rand McNally Encyklopedia of Military Aircraft. 1914 to the Present. Crescent Books New York 1981.

Munson Kenneth: A hadviselő felek valamennyi repülőgépe. Műszaki Kiadó. Budapest 1994.

TASCENBUCH DER LUFTFLOTTEN. V. JAHRGANG. Herausgegeben von Dr. Ing. W. von Langsdorf. 1926.

own work by the sources of. HL. VKF 1923-1930

6 Hadtörténeti Levéltár (HL), VKF p.1. 5149/T 1928.

stocked up.[7] They consisted of 29 air squads with about 650 military (reconnaissance, fighter, bomber, school) aircrafts.[8]

The actual number of aircrafts is really hard to determine on the basis of available resources. Annuaire Militaire, which can be considered relatively reliable, often published two or three years old data, Magyar Katonai Közlemények (Hungarian Military Communications) and Magyar Katonai Szemle (Hungarian Military Review) often merged the information about battle (*"front line"*) aircrafts with those for training, spare and civilian means. Civilian means, of course were also applicable for military purposes, but not with the ability of immediate implementation, and many of them were less effective as well. The other complicating factor is that reconnaissance aircrafts were often recorded as fighters at the same time as well in the twenties. These devices were generally able to carry bombs, but only with very small loads. Therefore their effectiveness in bombing was questionable.

In 1930, the Air Force staff consisted of more than 600 officers, 700 non-commissioned officers and 6000 crew soldiers.[9]

The military had about 1200 trained pilots. The settlements of the regiments were the following:

- 1st regiment in Újvidék (Novi Sad) (5 reconnaissance and 2 bomber squads);
- 2nd regiment in Sarajevo (4 reconnaissance and 1 bomber squads);
- 3nd regiment in Skopje (3 reconnaissance and 1 fighter squads);
- 4th regiment in Zagreb (3 1 reconnaissance and 1 fighter squads);
- 5th regiment in Nis (was not filled up);
- 6th regiment in Ljubljana (2 reconnaissance and 1 fighter squads);
- 7th regiment in Mostar (2 bomber squads).[10]

Two more flying schools belonged to them with their training air squads and also 13 airports (Novi Sad, Zagreb, Sarajevo, Mostar, Zemun, Skopje, Kraljevo, Bitolj, Osijek, Witch, Marburg, Pancevo and Podgorica).[11] The flying water group, which contained 3 squads (Kotor, Susak, Sebenico) and about 60 flying devices, was also a part of the air force.

AIRCRAFT IMPORT AND AIRCRAFT-INDUSTRIAL DEVELOPMENTS IN THE TWENTIES

In the early twenties primarily the French (as we already mentioned, until 1927 about 400-450 pieces), the British and the Czechoslovakian delivered fighter aircrafts to Yugoslavia. From 1923, the latter sold a wide variety of munition to our southern neighbour.12 Until the end of the decade, the French exported 546, the Czechoslovakian 60, the Dutch 50, the Swiss 3 aircrafts to Yugoslavia.13 The military mainly acquired DEVOITINE, BREGUET, and SPAD hunters, BREGUET 19A scouts and BREGUET 19B bombers.

From 1925, the national aircraft- industry also got powerful support. ICARUS factory founded in 1923 was able to satisfy the military's needs for school machines from 1925, then, from 1928 it started the production of its own construction, the FIZIER bomber.14 Its annual capacity was 150-200 aircrafts. In 1929, the Kraljevo National Aircraft Factory's (which was

7 HL, VKF p.2. 19541/T 1929

8 We concluded the probable amount of air squads and aircraft in Table1.

9 Magyar Katonai Szemle (MKSZ) 1931/9. p.210.

10 HL, VKF. p.2. 19541/T 1929. This sorce is unreliable, because the 1930/2 volume of Rivista Aeronautica provides different data about the1st and 4th regiments.

11 HL, VKF p.2. 23693/T 1928. and HL, VKF p.2. 118161/Eln. 1931

12 MKSZ 1933/8. Hírek p.264 –265.

13 HL, VKF p.2. 118985/Eln. 1931.

14 We listed the most common types in Table2.

founded in 1926) product made by French license, the BREGUET came out.15 The factory was built between 1926 and 1928, with Czechoslovakian assistance. It had a 250 aircrafts per year maximum capacity. The production of "Vlajkovics" (from 1926) and "Rogozsarszki" (from 1923) factories manufacturing school machines was no significant with a maximum of 50-50 aircrafts per year.16 On 11 August 1928 in Rakovica a major aircraft factory opened, which had an annual capacity of 150 pieces.17 In the end of the twenties the Yugoslavians ordered further 103 aircrafts from the French and the Czechoslovakians to modernize and supply their own air force.18

THE BUDGET FRAMEWORK OF THE AIR FORCE

The Yugoslavian political and military leadership always devoted significant resources to build out, maintain, and modernize their air force. In the twenties – from the Army's budget – they spent an increasing proportion and amount on aircraft design, manufacture, maintenance of existing structures and expansion. The continuous support of resources grew dramatically in 1926. This may be explained as follows: in 1927 they formed the 3rd air regiment, and the existing two air units were also filled.

The global economic crisis also affected negatively the development of the army, but it didn't affect significantly the air force because of the previous improvements and modernizations. Although the data of International Military Yearbook sometimes contradict even with themselves, - in the given and actually spent amount of money in 1929 and1930 - the differences are not significant.

Years	Military spending (millions of Dinar)	On air force (millions of Dinar)	%	Source
1922-23	1127.803	25.6	2.27	Annuaire Militaire 1926th Geneva 1926
1924-25	1956.001	39.77	2.03	Annuaire Militaire 1926th Geneva 1926
1926-27	1127.803	116.27	10.31	Annuaire Militaire 1927th Geneva 1927
1927-28	2398.6	146.14	6.09	Annuaire Militaire. Geneva 1931
1928-29	2428.6	166.528	6.85	Annuaire Militaire. Geneva 1931
1929-30	2428.6	178.865	7.36	Annuaire Militaire. Geneva 1931
1930-31	3081.9	238.7	7.74	Annuaire Militaire 1932nd Geneva 1932

3. table.

15 HL, VKF p.2. 118985/Eln. 1931

16 HL, VKF p.1. 5149/T 1928.

17 HL, VKF p.2. 23693/T 1928.

18 same source

CONCLUSION

During the examined period the Yugoslavian air force represented a rational size, well-organized, and continuously maintained power considering the possibilities and needs of the country. They solved their problems coming from technical level, manufacturing possibilities and capabilities by purchasing assets and licenses from abroad.

Reading the analyses of the examined era, it becomes clear, and the principle could also still be considered to be true, that besides owning technical equipment (aircrafts, *"leadership support"* systems, etc.) it was also essential for successfully applying air force to develop a new way of thinking and a complex approach to deal with air military. We think that Yugoslavia was on the right way to create at once its technical, infrastructural conditions and the right mental state for the success of its air force in military.

REFERENCES

[1] The Aircraft Yearbook for 1934. Aeronautical Chamber of Commerce of America, inc. 22. East fortieth street, New York 1934.

[2] Angelucci, Enzo: The Rand Mc Nally Enciklopedia of Military Aircraft 1914 to Present, Crescent Books, New York 1981.

3] Annuaire Militaire 1924, 1926, 1927, 1928, 1929, 1930, 1930–31, Geneva

Rivista Aeronautica 1930/2 Rome, 1930.

[4] Groehler, Olaf: A légi háborúk története 1910–1970, Zrínyi Katonai Kiadó, Budapest 1980.

[5] Vitéz Szentnémedy Ferenc: Jugoszlávia mint légi hatalom, Magyar Katonai Közlemények 1930/9.

[6] Taschebuch der Luftflotten 1928/29, Frankfurt am Main 1928.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Répás József
jozsef_repas@hellokitty.com

IGBT MŰKÖDÉSE ÉS ALKALMAZÁSÁNAK LEHETŐSÉGEI A BIZTONSÁGTECHNIKÁBAN

Absztrakt

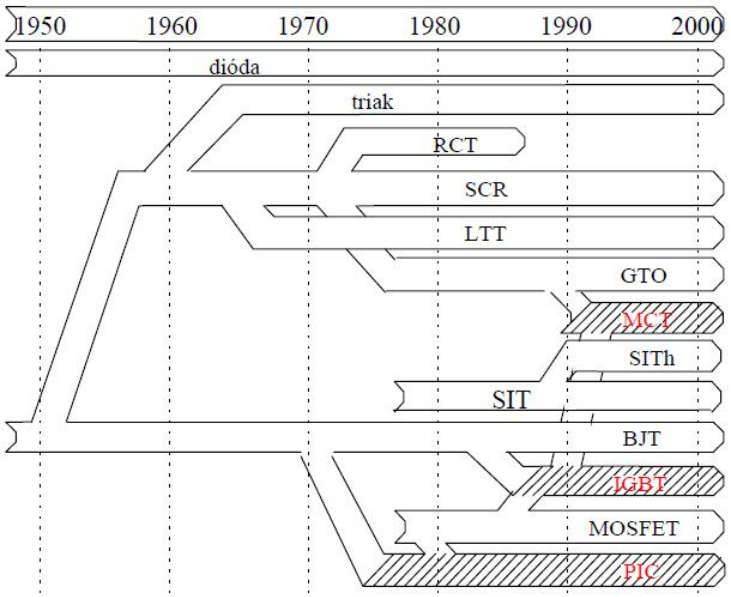
Világszerte évről évre növekszik az érdeklődés az elektromos energia iránt. A növekvő energiaköltségek, a CO2 kibocsátás, a fosszilis tüzelőanyagok behatárolt rendelkezésre állása, megköveteli a szignifikáns energiaspórolást. Nagy megtakarítási lehetőséget kínál sok ipari felhasználás, mint például a hajtás és áramellátó rendszerek. Hangolt rendszereknél megnövekedett szükséglet az „intelligens" vezérlő és teljesítménykapcsolás. Az IGBT-k kulcselemként kínálkoznak az ipari felhasználás kínálatában. Az IGBT egy szigetelt kapujú bipoláris tranzisztor (Insulated-Gate Bipolar Transistor) a MOSFET továbbfejlesztése. Kimagasló technikai tulajdonságai alapján széles körben alkalmasak biztonságtechnikai területen való felhasználásra.

All over the world the interest for electrical energy is increasing. The increasing energy costs, CO2 emission, the limited availability of fossil fuels make compulsory the significant energy-saving. Different industrial applying gives a lot of saving possibilities like drive and power systems. By tuned systems more and more intelligent controller and power switching needed. The IGBT-s has key functions in the offer of industrial applying. IGBT is an isolated based bipolar transistor (Insulated-Gate Bipolar Transistor), an upgraded MOSFET. By their extra high technical properties they can be used widely in safety.

Kulcsszavak: *hangágyú, IGBT, teljesítményerősítő, ultrahang ~ LRAD, IGBT, power amplifier, ultrasound*

IGBT KIALAKULÁSA

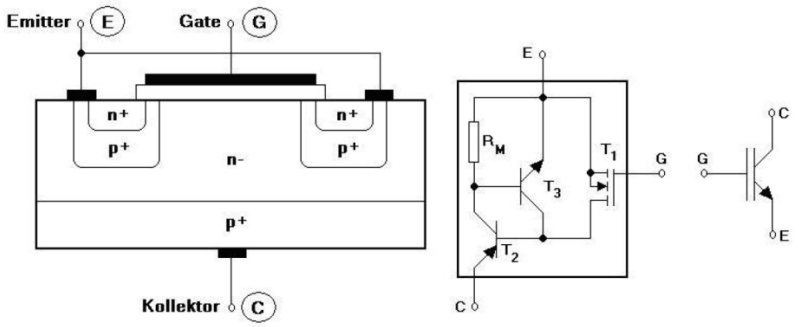
A szigetelt kapujú bipoláris tranzisztorok /IGBT/ átmenetet képeznek a bipoláris tranzisztorok és a MOSFET-ek között. Először 1979-ben állították elő, ez idő alatt a technológiai és gyártástechnikai fejlődés az elektronikában nagyteljesítményű elemet eredményezett. Teljesítményerősítés területén az IGBT-k, a feszültségerősítés és áramerősítés területén egyaránt jeleskednek. Feszültségerősítés területén a több száz volt és több kilóvolt közötti területen mozog, míg áramerősítés területén a néhány kilóamperig jut el. Egyesíti a bipoláris tranzisztorok - BJT ***/Bipolar (Junction) Transistor/ és a MOSFET-ek*** /metal–oxide–semiconductor field-effect transistor/ előnyeit. Feszültséggel vezérelhető, magas kapcsolási frekvencia, és kis feszültségesés. A bipoláris tranzisztorhoz hasonlóan az IGBT is kis vezetési veszteséggel rendelkezik, a MOSFET-ekhez hasonló nagy bemeneti impedancia mellett.



1. ábra. Félvezető elemek fejlődése [1]

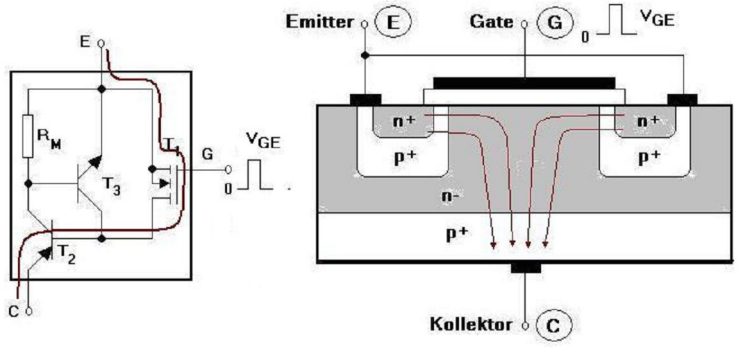
INSULATED-GATE BIPOLAR TRANSISTOR MŰKÖDÉSE

Bipoláris tranzisztorokhoz hasonlóan a főáramot kétféle töltéshordozó (elektronok és lyukak) alkotja. Ezen kívül alacsony saturációs feszültségben, magas áramterhelhetőségben és specifikus kapcsolási tulajdonságaiban hasonlítanak [2]. MOSFET tranzisztorokra az alacsony I_G vezérlőáramban, nagy kapcsolási sebességben és feszültségvezérelt jellegében hasonlítanak. IGBT lényegében a vertikális MOSFET továbbfejlesztett változata, amelyben az ismert MOSFET struktúrát egy *p* réteggel egészítették ki.



2. ábra IGBT cella kialakítása, helyettesítő képe, rajzjele [3]

Ha az IGBT-t E-C feszültségre kapcsoljuk, és $+V_{GE}$ feszültséget kap, akkor a 3. ábrának megfelelően alakul ki az áramvezetés egy IGBT cellában. IGBT is cellák ezreiből áll, hasonlatosan a teljesítmény MOSFET-hez.



3. ábra Áramutak egy IGBT cellában [4]

Mára a teljesítményelektronika gyakorlati alkalmazásaiban az IGBT-k nagyon népszerűek lettek.[5] MOSFET-ekhez hasonlóan készülnek, létezik N-csatornás és P-csatornás változata. P-csatornás IGBT-nél a rétegek szennyezettsége ellentétes. P-csatornás IGBT szimbólumánál a nyíl ellentétes irányú. Lényeges különbség a MOSFET-ekkel szemben abban áll, hogy a P és N zóna duplán diffundált.

Leegyszerűsítve, az IGBT úgy működik, mint egy olyan MOSFET, amelynek a drift-tartományát kisebbségi töltéshordozók (N-csatornás IGBT esetén lyukak) injektálásával vezetőképességében moduláljuk. Az IGBT vezérlési oldalról alapvetően egy MOSFET, tehát a gate-emitter-feszültség vezérli az eszköz állapotát.[6]

Utóbbi időben jelentős haladást értek el a veszteségek leredukálását illetően a kis chipméretek készítésénél is. Ezáltal kialakítható egyre kompaktabb és kedvezőbb árú rendszer. Manapság a gyártók keresik a megoldást az IGBT-k és az egyenirányító diódák felhasználási feltételeinek egyeztetésére. A technológia előrehaladásával, az IGBT-k, IGBT-modulok olyan technikai jellemzőkkel rendelkeznek, ami alapján felvetődik az analóg alkalmazás lehetősége.

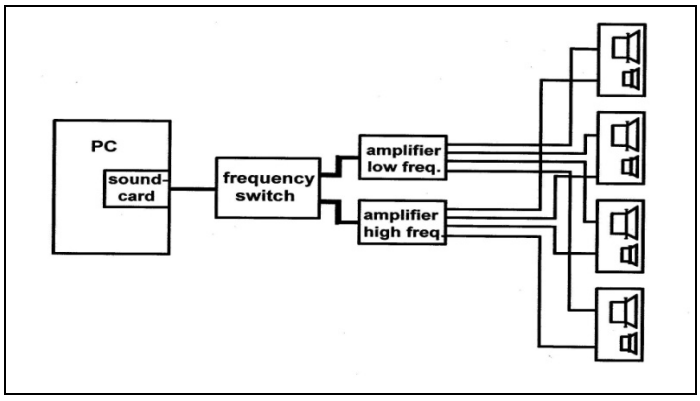
IGBT ALKALMAZÁSA A BIZTONSÁGTECHNIKÁBAN

Kezdetektől fogva fontos szempont a magántulajdon védelme. Vagyon elleni bűncselekmények számának növekedésével egyre nagyobb hangsúlyt kell fektetni az önálló védekezésre. Az ember a történelem évezredei során mindig küzdött azért, hogy társai ne veszélyeztessék tulajdonát. Így aztán már az ősember is gondosan őrizte a barlangját, s az

elkövetkező korok emberei igyekeztek jobb és jobb megoldásokat találni, hogy biztonságban tudhassák eszközeiket. A tudat, hogy egy idegen járt, az engedélyünk nélkül a magántulajdonunkban, talán az okozott anyagi- és eszmei- kárnál is fájdalmasabb tud lenni.

Az IGBT nagy teljesítménye miatt megfelelő kapcsolásban alkalmazható figyelemfelkeltésre, megzavarásra, elüldözésre, bénításra. Intelligens épületek vezérlésében is alkalmazható, mind az energiaellátás, vezérlés és optimalizálás területén, mind a Home Audio rendszerek esetén. A figyelem felkeltésére és megzavarásra erősítő fokozatba kapcsolva lehet alkalmas, ahol nagyteljesítményű hangszórókkal kiegészítve a kapcsolást riasztó hangot képes kiadni. Elüldözésre, bénításra hangágyúként való használatban lehet alkalmas, ahol szintén a nagy teljesítményerősítést kihasználva építhető olyan eszköz, amely mind a hangfrekvenciás, mind ultrahangos tartományban képes nagy intenzitású hangot kibocsátani. Intelligens otthonok esetén az épületautomatizálásban is alkalmazható a nagy kapcsolóteljesítmény miatt, Home Audio rendszereknél pedig hangfrekvenciás erősítőkben alkalmazható és kiváló hangzás biztosítható vele.

Egy korábban általam tervezett IGBT-s erősítőkapcsolás /J-17-es IGBT-s teljesítményerősítő/ az épületvezérlés kivételével a jól alkalmazható, jelen cikkben csak a hangágyúként való alkalmazást tárgyalom. Figyelemfelkeltésre nagy teljesítményű hang sugárzásával tehető alkalmassá. A kapcsolás széles frekvencia átvitelének köszönhetően ultrahang erősítésre is alkalmas, ami a hangágyúként való alkalmazás esetén szükséges. A 4. ábrán látható elrendezés szerint a végerősítő fokozatban (az ábrán: amplifier low freq. és amplifier high freq.) van lehetőség IGBT alkalmazására.



4. ábra IGBT alkalmazási lehetősége [7]

A betörő, aki komoly veszélyeztetést jelent vagyonunkra - gyorsan és feltűnésmentesen dolgozik. A legtöbb betörő különösen értékeli a nyugodt munkát. Minden, ami hangos, felhívhatja egy harmadik személy figyelmét. Az idő pénz – a betörőnek is. Célirányosan azokat az épületeket keresi, amelyekbe rövid idő alatt behatolhat. Az egyes objektumok kinyitása gyakran csak pár percet igényel. Minden betöréses lopás elleni biztonsági intézkedés alapja a mechanikus és elektronikus biztonságtechnika együttes alkalmazása. Az elektronikus biztonság kialakításának egyik lehetősége az ultrahang vagy ultrahang-közeli frekvenciájú hangágyú kialakítása.

HANGÁGYÚ ÉS MŰKÖDÉSI ELVE

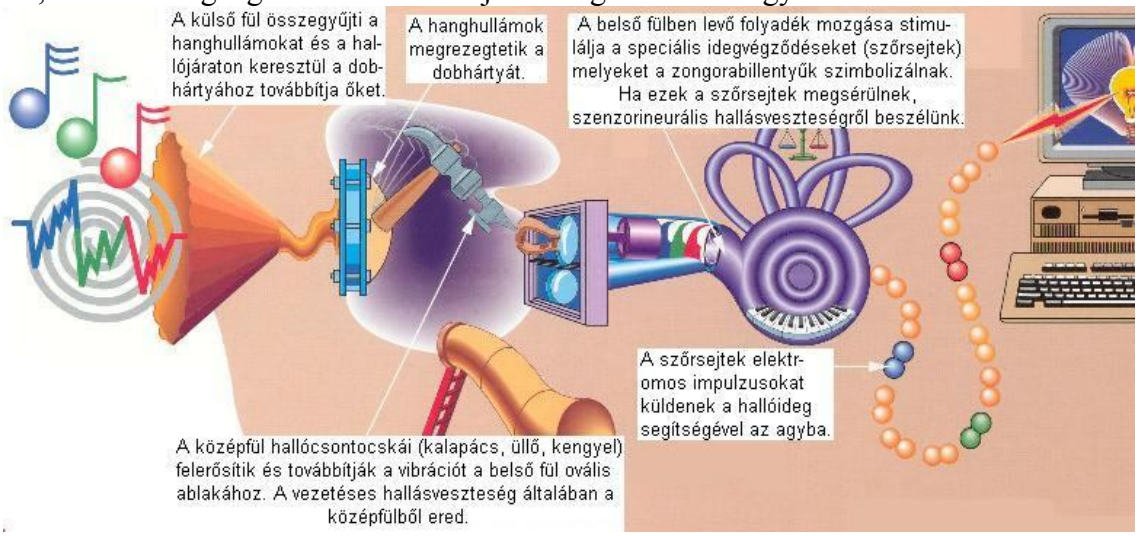
A hang fegyverként való alkalmazására már az ószövetségi írásokban is tettek utalást. Jerikó város falai a zsidó kürtök hatására omlottak össze. Bár Jerikó falai összeomlásának bibliai magyarázatát kutatók erősen vitatják, mégis a történet utal arra, hogy a hang fegyverként való alkalmazására már az ókorban is voltak elképzelések. Az ember a hangot,

mint „eszközt” a történelme során a kommunikáció mellett már a kezdetektől fogva elrettentő eszközként, azaz fegyverként is alkalmazta, mind önvédelmi, mind támadó értelemben. Az emberi fejlődés, a fizikai törvények mind mélyebb megismerése, az orvostudomány fejlődése egy idő után azonban elértek egy olyan szintet, amikor az orvosok már megfelelő ismeretekkel rendelkeztek arra vonatkozóan, hogy a hang különböző formái milyen hatással vannak az emberi szervezetre. A haditechnikai fejlesztéssel foglalkozó szakemberek pedig - felhasználva az elért tudományos és műszaki eredményeket – kifejezetten azt kutatták, hogy a hangot hogyan, milyen formában lehet fegyverként alkalmazni.[8]

HANG ÉS HALLÁS

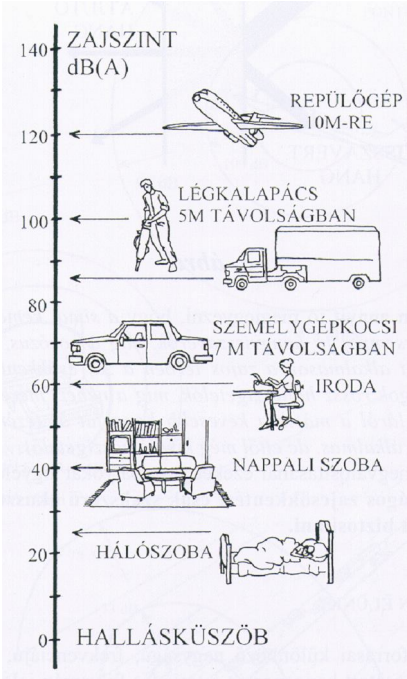
A hang longitudinális nyomáshullám (Longitudinális hullám esetén a hullám terjedési iránya megegyezik a rezgésiránnyal, sűrűsödési és ritkulási helyek követik egymást). Levegőben 330 m/s, vízben, szilárd anyagokban anyagtól függően akár 1500 m/s körüli sebességgel terjed. Hangot főként a fülünkkel halljuk, de a bőrünk, koponyacsontjaink is részt vesznek az érzékelésben.[9]

Hallás során a hanghullámok megrezegtetik a dobhártyát, aminek a rezgését a hallócsontocskák átviszik az ovális ablakra. Ennek hatására a csigában lévő folyadék mozgásba jön. A hang frekvenciájától függően a folyadék más-és más szőrsejteket hoz mozgásba, amik az idegvégződéseknek át adják az ingerületet az agyba.



5. ábra Hallás folyamata [10]

A hallható hangok frekvenciája 20-20.000Hz-ig terjed. Fülérzékenysége a 3000Hz körüli tartományban a legjobb. Legkisebb halható hang (hallásküszöb) és legnagyobb fájdalmat még nem okozó hang (fájdalomküszöb) közötti 120dB-es hangerőkülönbség elviselését az teszi lehetővé a fül számára hogy az érzet erősége az ingernél lassabban nő, a logaritmikus skála szerint.



6. ábra Hangnyomásszintek[11]

Ezt a fájdalomküszöböt kihasználva lehetőség van olyan riasztó eszköz építésére, amely az ultrahanghoz közeli és ultrahang frekvenciájú hangokkal igyekszik elüldözni a behatolót.

A 20 000 Hz-nél magasabb és 100 MHz-nél alacsonyabb frekvenciájú hangokat ultrahangnak nevezzük. Egyes irodalmak, ezt a az alsó küszöböt 16-18 KHz-re teszi. Sok esetben a 100 MHz-en felüli hangokat is ultrahangnak tekintik. Az ember hallása nem olyan fejlett, hogy hallja az ultrahangot. Az embertől valamivel magasabb hangokat még hallják a kutyák, és a macskák, ez körülbelül 35 – 40 KHz - ig terjed, de egyes rágcsálók érzékelik a 100 KHz - es hangokat is. Az ultrahang természetesen az élő szervezetekre is hatással van. Ultrahangos kezelést alkalmaznak a gyógyászatban egyes ideg-, izom- és csontrendszeri megbetegedések gyógyítására. Talán legismertebb szerepe mégis az, hogy szervezeten belüli diagnosztikai vizsgálatokra használják, segítségével megállapíthatnak egyes betegségeket, vagy például a magzat elhelyezkedését a méhben.[12]

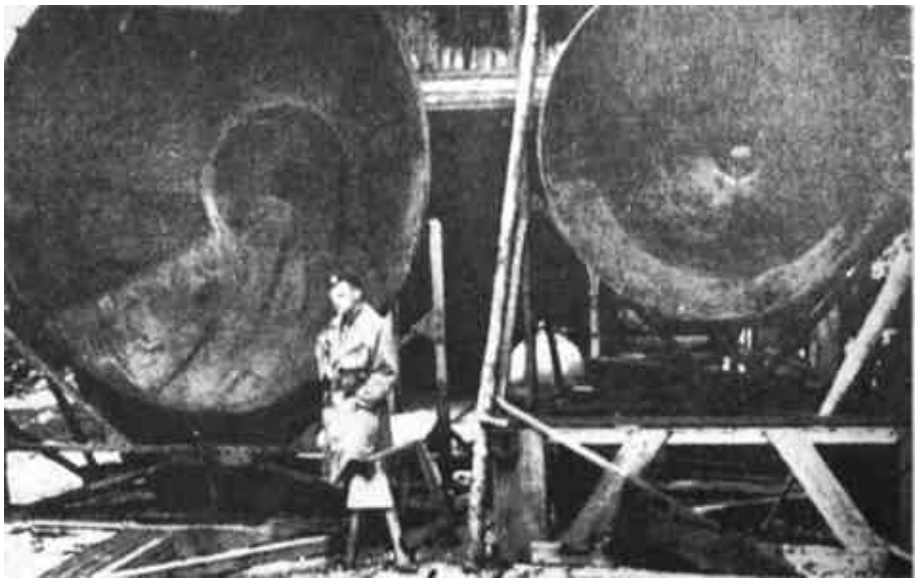
Az ultrahangok mechanikai rezgések, amiket már nem érzékelünk hangként. Biológiai hatásuk a dózistól függően lehet az életfunkciók serkentése vagy az életfolyamatok gátlása. Ultrahang a sejt közötti állományt fellazítja, a sejteket elroncsolja. Különösen érzékeny rájuk a középfül és a szem. Bőrünk az ultrahangot zömmel visszaveri, a szőrzettel borított test azonban hőenergiává alakítja. Ultrahang pontos biológiai hatása még nem tisztázott.[13]

Ezeket az információkat felhasználva, készíthetünk egy olyan berendezést, amely egy esetleges behatolás alkalmával képes lehet a bénításra, elüldözésre, mivel nagy teljesítménnyel sugározva az ilyen hangokat, az ember számára elviselhetetlen.

SZÉL ÉS HANGÁGYÚ

Az első olvasatra könnyen fantazmagórikusnak és komolytalannak tűnő fegyvereket a folyamatos és egyre súlyosabb károkat okozó szövetséges légitámadások elleni eszközökként fejlesztették ki 1945 elején. Bár a túlzóan merész tervek a háború elején még valószínűleg a hadvezetés ellenállásába ütköztek volna, az 1945-ös év beköszöntével már szinte válogatás nélkül finanszíroztak olyan programokat, amik az adott helyzetben akár minimális sikerrel kecsegtetett volna. Egy osztrák mérnök, Dr. Zippenmayer által felvázolt szélágyú koncepciója

minden furcsasága ellenére elnyerte a vezetés támogatását (főleg Adolf Hitlerét!) és a program zöld utat kapott. Dr. Zippenmayer vezetésével működő csoport másik "találmánya" a hangágyú volt, amely abból az ötletből sarjadt, hogy bizonyos frekvenciájú és intenzitású hanghullámok képesek kárt tenni a mind a repülőgépekben és, vagy annak személyzetében. A furcsa szerkezetben metánt és levegőt égettek, az ezzel előidézett robbanásokat ezután hangtükrök segítségével irányították. Mivel a robbanások rövid időközönként követték egymást, ezért a hangjukat sikerült nagyfrekvenciájú hullámokká alakítani. Egyes jelentések szerint épült egy prototípus ebből a furcsa ágyúból, amit aztán teszteltek. A konstrukció hiányosságaiból adódóan azonban képtelen lett volna a hanghullámokat nagy magasságba feljuttatni és minden valószínűség szerint sosem került bevethető állapotba. A szélágyúból egyetlen egy példány élte túl a háborút (a vélemények megoszlanak, hogy a korai prototípus e az vagy a harcban is bevetett változat, nos ezt nem tudni), amit az amerikai katonák találtak meg a hillerslebeni lőtéren. A hangágyúról sem makett, sem tervrajzok, sem pedig prototípus nem maradt fent.[14]



7. ábra Dr. Zippenmayer féle hangágyú[15]

MODERN HANGÁGYÚ

Napjainkban a hajózási vállalatok a nemzetközi katonai támogatás mellett egyre inkább megpróbálják saját maguk védettebbé tenni járműveiket a mind gyakoribb kalóztámadások ellen. A tengeri rablók az év első napján is megkaparintottak egy egyiptomi teherhajót Afrika szarvánál. A védelmi eszközök közül különösen divatosnak számítanak manapság a fejlett technológiájú, úgynevezett nem halálos fegyverek.

Kalózok idejekorán való megfékezésére a legkeresettebb high-tech eszköz a hangágyú (LRAD - Long Range Acoustic Device). A fegyvert az amerikai haditengerészet a USS Cole hadihajó elleni, 2000-ben elkövetett támadást követően állította hadrendbe. Fegyver lelke egy kerek, kissé parabolaantennára emlékeztető eszköz, amely, akárcsak egy megafon, nagyon erős hangot bocsát ki. 150 decibel erejű hangorkánt a közelben lévő célpont, amelyre irányozták, elviselhetetlennek tartja. Alapváltozatban a fegyver hatótávolsága ötszáz méter.

Hangágyút fejlesztett ki és vetett be a palesztin tüntetők ellen az izraeli hadsereg. A morajló hangot adó készülék a fül belső kamráit zavaró elektromos frekvenciákat bocsát ki és ezáltal a céltömegben tartózkodó embereken egyensúlyzavar, szédülés és hányinger lesz úrrá.

Az izraeli hadsereg és a városi rendőrségek komoly reményeket fűznek a sikeresen bemutatkozott új tömegoszlató fegyver iránt.[16]

8. ábra LRAD alkalmazása[17]

Kisteherautó platójára erősített szerkezet (8. ábra) 10 másodperces időközönként „lőtt" az emberek közé, és a csodálkozó palesztin fiatalok fülüket befogva, tántorogva igyekeztek elszaladni a helyszínről. Egyik helyszínen jelen lévő tudósító elmondta, hogy hiába tapasztotta tenyerét a fülére, mert a mélyen dübörgő hang a kezén át behatolt a fejébe és hamarosan erős szédülés és hányinger fogta el. Az izraeli hadsereg és a tüntetések elfojtásában nagy gyakorlatot szerzett városi rendőrségek komoly reményeket fűznek a sikeresen bemutatkozott új tömegoszlató fegyver iránt. „Sikerült megoldanunk azt a hármas célt, hogy a terroristák távol maradjanak a katonáinktól és minél hamarabb megtisztítsuk a terepet olyan módon, hogy a tüntetők közül sem sérüljön meg senki" – fejtette ki véleményét egy magát megnevezni nem akaró izraeli katonatiszt.[18] Hazánkban is alkalmazzák riasztásra. A Szelíd-tavat az elmúlt évekig alkalmanként leadott puskalövésekkel próbálták védeni, de tavaly nyáron korszerűsítésként hangágyú lett üzembe helyezve.[19] Ezt azonban nem alkalmazták sokáig.

ÖSSZEGZÉS

A nagy teljesítményű hang előállítására különböző lehetőségek állnak rendelkezésre. Az erősítő elemek választásának kritikus pontja a torzítás, átvitel és hatásfok. Elektroncsövek jó 2/3-os karakterisztikájuk miatt alkalmasak erősítésre, azonban rossz hatásfoka, nagy maradék feszültségesés a fűtés miatt nem a legmegfelelőbb eszköz. Tranzisztorok, mint a legelterjedtebb félvezetőelemek exponenciális karakterisztikája miatt nem a legmegfelelőbb elem a torzítási probléma miatt. MOSFET tranzisztorok négyzetes karakterisztikájuk miatt megfelelőek, de a csatorna ellenállás miatt rossz a hatásfoka. Az IGBT tranzisztorok szintén négyzetes karakterisztikája, bipoláris kimenete, magas áramterhelhetősége, csaknem veszteség nélküli erősítése, magas hatásfoka, gyors kapcsolási jellemzői miatt alkalmas

nagyteljesítményű teljesítményerősítőben való alkalmazásra. Ez alapján felhasználható ultrahangos riasztó és hangágyú tervezésénél. A tervezett eszköz hatékonyan alkalmazható egy adott hely vagy terület kiürítésére, tömegoszlatásra köszönhetően az IGBT kiváló technikai jellemzőinek.

Irodalomjegyzék

[1] Blága Csaba, *Teljesítményelektronika*. jegyzet, Miskolci Egyetem http://www.uni-miskolc.hu/~elkblaga/villkesz/POWEL1n.pdf (letöltés: 2010-01-11)

[2][6] Badacsonyi József, *Teljesítményelektronika kapcsolóelemei II.* BMF – KVK Főiskolai jegyzet Budapest 2002

[3][4][5] Puklus Zoltán, *Teljesítményelektronika.* Széchenyi Egyetem Győr 2007 ftp://jegyzet.sth.sze.hu/!Tais_cuccok/BSc/Szakiranyos/Automatizalasi/NGB_AU019_1_Teljesitmeny_elektronika/teljes/Teljesitmenyelektronika.pdf 58-59. o. (letöltés: 2011-03-27)

[7][8] Bartha Tibor: *Személyek elleni akusztikus fegyverek, mint nem halálos eszközök.* ZMNE egyetemi jegyzet 2004

[9] *Az ultrahang* http://ultrahang.l5.hu/index.php (letöltés: 2011-03-27)

[10] *A hallás folyamata* http://www.starkey.hu/images/sematikus.jpg (letöltés: 2009-11-21)

[11] WERSÉNYI, GY. *Műszaki Akusztika*. http://vip.tilb.sze.hu/~wersenyi/MA1.pdf Egyetemi jegyzet, Széchenyi István Egyetem, Műszaki Tudományi Kar, 2004-2009 (letöltés: 2010-11-11)

[12] *Az ultrahang* http://iar.bmfnik.hu/2002_2003/ultrahang/ultrahang.htm (letöltés: 2011-03-27)

[13] *Zajok fiziológiai hatása* http://szilaster.freeweb.hu/Zaj_fiziol_hat.doc (letöltés: 2011-03-27)

[14][15] *Szél és hangágyú* http://www.masodikvh.hu/index.php?option=com_content&task=view&id=356&Itemid=189 (letöltés: 2009-12-11)

[16] *Ultramodern fegyverekkel szerelik fel legújabban a teherhajókat.* http://www.nepszava.hu/articles/article.php?id=63879 Népszava online 2009. január 03., 05:30 (letöltés: 2011-03-18)

[17] *LRAD* http://www.securityprousa.com/loraacde.html (letöltés: 2009-07-11)

[18] *Hangágyúval az ellenség ellen*. http://www.mno.hu/portal/289463 Magyar Nemzet Online 2005. június 12. 09:52 (letöltés: 2011-04-23)

[19] Tüske Emil: Riasztó tevékenységek a Szelíd-tavon http://www.biatorbagy.org/aktualis/biatorbagy-szelid-to (letöltés: 2011-03-27)

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Berek Tamás
berek.tamas@zmne.hu

ABV (CBRN) ANALITIKAI LABORATÓRIUM BELÉPTETŐRENDSZERE A BIZTONSÁGOS ÜZEMELTETÉS SZOLGÁLATÁBAN

Absztrakt

Egy olyan objektumban, mint az ABV védelmi laboratórium, ahol veszélyes anyagot, radioaktív izotópokat tárolnak és használnak fel és ionizáló sugárzás, valamint mérgezés veszélyével járó munkakörben, fontos a laborbiztonsági rendszabályok betartása. A szerző bemutatja, hogy a vagyonvédelmi komplexum elektronikus biztonsági komponensének eszközei, a felügyeleti informatika és az épületautomatika segítségével megvalósítható integrált épület-felügyelet hogyan csökkentheti az emberi tényező hibalehetőségeiben rejlő biztonsági kockázatokat.

An object, which the CBRN defense laboratories, where hazardous materials, radioactive isotopes are stored and used for a job under the risk of poisoning and ionizing radiation, it is important to compliance with the safety regulations. The author demonstrates that how to reduce the security risks of the mistake of human element through an integrated building monitoring, which is feasible by the security component of the complex electronic security tools, such as IT-management and building automation.

Kulcsszavak: *hangágyú, IGBT, teljesítményerősítő, ultrahang ~ LRAD, IGBT, power amplifier, ultrasound*

AZ ABV ANALITIKAI LABORATÓRIUM LÉTJOGOSULTSÁGA

A tavalyi esztendő áprilisában aláírt START-III szerződés keretében Oroszország és az Egyesült Államok megállapodtak abban, hogy a 2017-re mindkét ország 1550-ra csökkenti hadászati robbanófejeinek számát és a hordozóeszközök számát pedig 800-ban, maximálták.

A nukleáris leszerelési folyamat lényegesebb fázisaiban általában felerősödnek a tömegpusztító fegyverek proliferációjával, és a nukleáris terrorizmus térnyerésével kapcsolatos aggodalmak.

Az Európa Tanács 2003. december 12-én elfogadta a tömegpusztító fegyverek elterjedése elleni EU-stratégiát, továbbá az Európai Unió 2006. február 27-én a Biológiai és Toxin Fegyver Tilalmi Egyezmény (BTWC) tekintetében együttes fellépésről állapodott meg, melynek célja az egyezmény egyetemessé tételének elősegítése, valamint az abban részes államok általi végrehajtása támogatásának biztosítása.

Az európai biztonsági stratégia végrehajtásáról szóló 2008. decemberi jelentés (S407/08) ugyanakkor kinyilvánította, hogy a tömegpusztító fegyverek általi fenyegetettség fokozódott, és hogy ez az ügy továbbra is kiemelt helyen szerepel az EU politikai napirendjén.

A katonai műveletek ABV környezete pedig determinálja a jövő hadműveleteinek ABV kockázatát. Mindezek mellett a rombolódott ipari üzemekből és nukleáris létesítményekből is egészségre ártalmas anyagok szabadulhatnak ki.

Az ABV helyzetről érkező információk fontos szerepet töltenek be a parancsnok harcászati helyzetértékelésében, az ABV csapások, kibocsátások tényéről és a következtükben kialakuló veszélyekről információt pedig a felderítés szolgáltat. Az ABV felderítés alapvető célja az ABV szennyezettség detektálására és azonosítása annak megállapítása érdekében, hogy mi ellen és mennyi ideig kell védekezni. Az ABV felderítésnek az ABV esemény paramétereit leíró információkat minél hamarabb rendelkezésre kell bocsátani a műveletet irányító parancsnoknak, hogy annak döntéshozatalában segítségül szolgáljon az ABV veszélyek elkerülése érdekében, az ABV védelmi feladatok tervezésekor és a biztosításuk feltételeinek meghatározásakor a legfontosabb a pontos, megbízható, adatok felhasználása. Többek között ezen feladatok feltételei biztosításának számvetését hatékonyan támogathatja ABV analitikai labor vizsgálata. [1]

Az ABV analitikai labor vizsgálata és az ehhez kapcsolódó mintavételi műveletek különösen fontosak abban az esetben is, ha korábban ismeretlen anyag alkalmazására kerül sor, illetve a vegyi-, és biológiai harcanyag elsőkénti alkalmazása esetén. [2] A jó minőségű mintavétel és a minták azonosítása a biológiai vagy mérgező harcanyag első alkalmazásának megállapítása szempontjából kiemelkedő jelentőséggel bír, különösen, ha a mintákat törvényszéki bizonyítékként kívánják felhasználni. Olyan minták vizsgálata, amelyeknél felmerül a gyanú, hogy mérgező harcanyagot tartalmaznak, akkreditált ABV analitikai laboratóriumban végezhető el.

Az elemzési módszerek fejlesztésének műszaki lehetősége korlátozott, ezért – és különösen ismeretlen ágens azonosításában – az identifikálási eljárás nemzeti háttér-laboratóriumi kapacitással történő támogatása elengedhetetlen.[3]

A HÁTTÉR-LABORATÓRIUM FELADATAI

Az ABV védelmi háttérlaborban az oktatás és kiképzés területén alapvetően a vegyivédelmi szaktisztek-, tisztjelöltek képzése kell, hogy megvalósuljon, azonban alap és mesterképzésben szakismeretek, valamint különböző szaktanfolyamok és speciális ABV képességek elérését biztosító tréningek megszervezésének helyszíne is lehet. Mintavételi (SIBCRA)[1] csoportok AEP-10 és AEP-49 (mintavételi kézikönyvek) szerinti kiképzése és felkészítése, valamint szinten-tartó gyakoroltatása kiemelt fontosságú, melynek színtere és kiszolgáló bázisa a nemzeti háttér-laboratórium. Kutató műhelyként továbbá az ABV háttér-

[1] Sampling and Identification of Biological, Chemical and Radiological Agents - biológiai-, vegyi- és radiológiai anyagok mintavételezése és azonosítása

laboratóriumi kapacitás hatékonyan hozzájárulhat a vegyivédelmi szaktevékenységek fejlesztéséhez. Az ABV labor kapacitásának meghatározásakor a szabályzat (STANAG 4632), egyébként a hadműveleti területre telepíthető és megadott időtartalmú készenlétű laboratórium számára előírt képesség-követelményét lehet alapul venni, azonban az ABV (CBRN) védelmi háttér-laboratóriumot meg kell feleltetni az oktatás céljainak és jogos elvárásként, új metódusok kialakításának követelményeinek. A funkcionalitásában többrendeltetésű háttér-laboratórium biztonsági rendszerének tervezésekor és kialakításakor ezt figyelembe kell venni.

Az ABV (CBRN) mintavételi műveletek olyan képzett és tapasztalt személyi állományt igényelnek, melyek tagjai járatosak a sugárvédelmi eljárások, a felderítő eszközök és módszerek, valamint a mintavétel eljárások terén. Kiképzésük magában foglalja egyrészt a szükséges elméleti ismeretek megszerzését az iskolai felkészítés során, valamint a gyakorlati ismeretek elsajátítását, melyeknek ki kell terjednie többek között mintavétel metódusokra, a felderítő műszerek, a kommunikációs eszközök, valamint a helymeghatározó eszközök használatára Ennek érdekében laborgyakorlatok, terepgyakorlatok során kell készség szintre fejleszteni a szakmai jártasságot. Ennek elengedhetetlen eleme a szituációs gyakorlati képzés, hogy a képességek fejlesztése valósághű körülmények között történjék. [4] Amennyiben a technikai és a biztonsági feltételek lehetővé teszik, éles mérgező harcanyag felhasználásával kell a személyi állomány jártasságát biztosítani – természetesen inaktív anyagok felhasználását követően - , abban az esetben, ha az éles harcanyagok alkalmazása egyebek mellett környezetbiztonsági kockázatokat rejt, a minták begyűjtésére, szállításra történő előkészítésre, szállítására és azonosítására kiterjedő kiképzés során fizikai és kémiai szempontból analóg vegyületek használata indokolt.

A speciális mintavevő csoport képességeit, mintavételezési eljárásait és módszereit meghatározó szabályzatok előírják tehát annak kiképzési, illetve felkészítési követelményeit, melyek alapján elmondható, hogy a felkészítés egyik szükséges bázisa az ABV védelmi analitikai háttér-laboratórium. A laborkomplexummal szemben ugyanakkor jogos elvárás továbbá, hogy a jövőbeni ABV kihívásokkal szemben ellenpontot képviselve és válaszlépéseket téve, előremutató jelleggel új és korszerű elvek és metódusok kialakításának színtere legyen.

Az ABV védelmi laboratórium bármely funkciójában – akár oktató,- kiképző-, kutató,- akkreditált analitikai háttér-laboratóriumként – az ott végzett tevékenység veszélyes radioaktív, mérgező, esetleg fertőző anyagok esetenként mérgező harcanyagok szükségszerű felhasználásával történik. A laborkomplexumban kialakított ellenőrzött munkaterületek és munkafolyamatok ideértve az azokban résztvevő személyi állomány és a veszélyes anyagok, valamint a hulladékok tároló-helyiségei védelme kiemelt fontosságú. Nem kisebb súllyal igénylik a védelmet a munkaterületnek nem minősülő terek és laboratórium külső környezete.

ABV védelmi analitikai laboratóriumban annak rendeltetésének megfelelően különböző műveleteket kell végezni veszélyes anyagokkal (radioaktív, vegyi, biológiai) vagy éppen azok azonosítását kell végrehajtani. Napjaink egyik, biztonságot fenyegető tényezője a terrorizmus elleni védekezés is megköveteli a veszélyes anyagok monitorozását, azonosítását ilyen kiemelt objektumok felügyelete során is. Számos olyan anyag kerül ideiglenesen vagy tartósan letárolásra ugyanis a laboratóriumban, amelyek önmagukban vagy csekély módosítással felhasználhatóak bűnös céllal. A biztonsági rendszer felépítése érdekében kialakított védelmi filozófia alapjául szolgál a biztonsági kockázatelemzés, melynek ki kell térnie a laboratóriumban felhasznált veszélyes mérgező és radioaktív anyagok külső környezetbe történő kerülésére, gondatlan-, vagy bűnös szándék, vagy akár technológiai hiba közrehatásának eredményeként.

Egy olyan objektum kialakításakor és későbbi működtetésekor, melyben ideiglenesen vagy üzemszerűen tárolt anyagok jelenléte önmagában is veszélyforrást jelent, lényeges biztonsági elem a veszélyforrásoknak megfelelő ABV detektorok monitor-hálózatban, történő felszerelése, ami napjainkban alkalmazott gyakorlat. Az ABV detektorok és a biztonságtechnikai-vagyonvédelmi érzékelők közös platformon történő elhelyezése és egy vezérlőegységgel történő üzemeltetése további lehetőségek előtt nyitja meg a kapukat a biztonsági rendszer fejlesztésének területén. Az ABV analitikai labor védelmi rendszerének fontos része kell, hogy legyen a beléptető rendszer, a nukleáris, biológiai, és vegyi detektorokról, valamint a biztonsági rendszer érzékelőiről érkező jelzéseket olyan rendszernek kell feldolgoznia, amely alkalmas azok együttes kezelésére és vezérelni tudja a jelző-riasztó egységeket a vagyonvédelmi rendszer elemeivel és a szükséges épület-felügyeleti berendezésekkel együtt.

A biztonsági és beléptető alrendszernek és az ABV védelmi alrendszernek tehát egymással együtt kell működnie, a biztonságtechnikai rendszer, illetve annak beléptető moduljának tervezésekor a NATO STANAG 4632 szabvány által meghatározott a NBC analitikai laboratóriumok képességeit kell alapul venni.

ABV ANALITIKAI LABORATÓRIUM KÉPESSÉGEI, MINT VESZÉLYFORRÁSOK

Az ABV analitikai laboratórium alapvető rendeltetése az AEP 10, illetve az AEP 49 alapján vett minták igazságügyi szintű szakértői azonosítása, az egyértelmű azonosítás.

Alaprendeltetésén felül tudományos bázisául szolgál az ABV kihívásokra tervezett válaszlépések érdekében végzett kutatásoknak, valamint személyi állományának felkészültsége révén alkalmas a hadműveleti területen bekövetkezett ABV csapások következtében kialakuló veszélyeztetettség, illetve nem csapásból származó veszélyes ipari anyagok (vegyi, biológiai, radiológiai) kiáramlása révén kialakuló veszélyeztetettség katonai műveletekre kifejtett hatása kockázatának értékelése okán különböző vizsgálatok elvégzésére.

Alaprendeltetésének megfelelően biztosított képességeinek köszönhetően szakértői állásfoglalás kiadását megalapozó analitikai eljárásokat dolgoztak ki, melyeket a STANAG 4632 szabványban rögzítettek.

Az ABV analitikai laboratóriumok mérgező harcanyagokra megállapított alapképességének meghatározása a toxicitási, illetve a harctéri alkalmazhatóság egyéb mutatóinak figyelembevételével történik. A mérgező harcanyagok tekintetében ezt alapvetően három területre korlátozva rögzítették a STANAG 4632-ben meghatározva az analitikai eljárás eszközét is. Így az ABV analitikai laboratóriumnak képesnek kell lennie hólyaghúzó-, idegbénító mérgező harcanyagok, illetve toxikus ipari anyagok (TIC[2]) kimutatására a következő felosztásban.

Tic	Kimutatási eljárás
Akrilnitril	Gc-ms
Ammonia	Tömegspektrométer (ms)

[2] (TIC=Toxic Industrial Compounds)

Bróm	Tömegspektrométer (ms)
Klór	Tömegspektrométer (ms)
Etilén-oxid	Gc-ms
Formaldehid	Gc-ms
Sósav	Tömegspektrométer (ms)
Hidrogén-cianid	Tömegspektrométer (ms)
Hidrogén-fluorid	Tömegspektrométer (ms)
Kénhidrogén	Tömegspektrométer (ms)
Salétromsav	Tömegspektrométer (ms)
Foszgén	Gc-ms
Foszfor-triklorid	Tömegspektrométer (ms)
Kénsav	Tömegspektrométer (ms)

1. táblázat. ABV AL toxikus ipari anyagokra megállapított alapképessége (STANAG 4632 alapján)

Általában három olyan analitikai eljárás alkalmazott a laboratóriumi gyakorlatban, amelyek kielégítik a mérgező harcanyagok egyértelmű azonosításának (STANAG 2112) kritériumát. Ezek a tömegspektrometria (MS), a fourier-transzformációs infravörös spektrometria (IR) és a mágneses magrezonancia spektrometria (NMR). A mérgező harcanyagok elválasztására, kimutatására és azonosítására jelenleg használt egyik legalkalmasabb kapcsolt technika a gázkromatográfia-tömegspektrometria (GC-MS).[5]

Idegbénító mérgező harcanyagok		
Nato kód	Harcanyag típus	Kimutatási eljárás
Dfp	Diizopropil-fluorfoszfát (dfp)	Gc-ms
Ga	N,n-dimetilamid-0-etil-ciánfoszfát (tabun)	
Gb	0-izopropil-metilfluorfoszfonát (szarin)	
Gd	0-(3,3-dimetil-sec butil) metilfluorfoszfonát (szomán)	
Gf	0-fenil – metilfluorfoszfonát (etilszarin)	
Vx	0-etil-s-(n,n-diizopropilaminoetil)-metiltiolfoszfonát	
Hólyaghúzó mérgező harcanyagok		

Nato kód	Harcanyag típus	Kimutatási eljárás
Hd	2, 2'-diklórdietilszulfid (kénmustár)	Gc-ms
Q	Etilén 2, 2' diklórdietilszulfid (szeszkvimustár)	
Hn3	Triklórtietilamin (nitrogénmustár)	
Hn2	N-metil, 2, 2' diklórdietilamin' (nitrogénmustár)	
Hn1	N-etil 2, 2' diklórdietilamin (nitrogénmustár)	
L1	2 – klórvinil – arzindiklorid (α luizit)	
L2	Di – 2 - klórvinil – arzindiklorid (β luizit)	
L3	Tri – 2 - klórvinil – arzin (γ luizit)	

2. Táblázat. ABV AL idegbénító-, és hólyaghúzó mérgező harcanyagokra megállapított alapképessége
(STANAG 4632 alapján)

Az ABV analitikai laboratórium alapképességébe tartozó biológiai ágensek tekintetében minimum követelményt határoz meg a STANAG (10 ágens/5 toxin) a következő felosztásban

Biológiai ágensek	
Típus	Kimutatási eljárás
Bacillus anthracis (anthrax)	Pcr[3], kimutató kit
Yersinia pestis (pestis)	
Coxiella burnetii (q- láz)	
Francisella tularensis (tularemia)	
Brucella melitiensis (brucellosis)	
Sárgaláz vírusa	
Burkholderia mallei	
Vibrio cholerae	
Vle	Rt pcr[4], kimutató kit

[3] PCR: Polymerase Chain Reaction

Orthopoxviridae (variola major)	Rt pcr, kimutató kit

3. Táblázat. ABV AL biológiai harcanyagokra megállapított alapképessége (STANAG 4632 alapján)

A NATO követelmények (STANAG 4632) által előírt bizonyított azonosítás érdekében a megerősítő analízist két független módszer segítségével kell elvégezni. Így az agens-specifikus kimutató kit mellett az eredményt meg kell erősíteni PCR módszerrel.

A polimeráz láncreakció (PCR) módszer segítségével akár egyetlen DNS molekulából kiindulva, a további vizsgálatokhoz elegendő mennyiségű DNS-t lehet előállítani. Napjainkban széles körben használják többek között a kutatásban, az orvosi diagnosztikában. Alkalmazásából levont tapasztalatok bizonyították azt a tényt, hogy a PCR technika megbízható, pontos és gyors eredményeket biztosít. [6]

Toxinok	
Típus	Kimutatási eljárás
Staphylococcus enterotoxin b (seb)	Kimutató kit
Ricin	
Botulinum toxin	
Saxitoxin	
T2 mikotoxin	

4. Táblázat. ABV AL biológiai toxinokra megállapított alapképessége (STANAG 4632 alapján)

A beérkező környezeti minták jellegüket tekintve talaj, por, folyadék, levegő, illetve mikrobiológiai, állati eredetű, élelmiszer stb. lehetnek.

Az ABV analitikai laboratórium radioanalitikai eljárásainak biztosítani kell a minőségi és mennyiségi nukleáris analízis megvalósulását. A nukleáris analízisre jellemző a detektor válaszjeleinek azonnali feldolgozása, illetve az igény a részecske, vagy energiaszelektív mérésre. Az ABV analitikai laboratórium radioanalitikai követelményeinek meghatározásakor a STANAG 4632 a következő energiaspektrumban határolja be a különböző sugárzástípusok detektálási képességét

Ionizáló sugárzások	
	Energia szint (mev)

[4] Reverz PCR vizsgálat RNS kimutatására

	Min	Max
Alfa	3	8
Béta	0,1	2,5
Gamma	0,05	3
Neutron	2,5e-8	10

5. Táblázat. ABV AL radioanalitikai alapképessége
(STANAG 4632 alapján)

A képességek áttekintését követően, amelyeket az ABV analitikai laboratórium tekintetében határoz meg a STANAG körvonalazható azoknak a veszélyforrásoknak a vegyi, biológiai és radiológiai összetevői, melyek lehetséges elemeit figyelembe kell venni a laboratórium különböző veszélyességi szintű területeire, annak közvetlen környezetére méretezett biztonságtechnikai rendszer tervezését, illetve kialakítását megelőzően. A behatárolt veszélyforrások detektálható paramétereit alapkövetelményként definiálva szükséges tehát meghatározni később azoknak a detektortípusoknak a körét, melyeket rendszerbe integrálva az igényeknek (követelményeknek) megfelelő ABV monitoring hálózathoz történő illesztésük vonatkozásában meg kell vizsgálni, hozzátéve, hogy csupán a sugárvédelmi detektorok vonatkozásában, és a beléptető rendszert állítva a fókuszba kivonatoltan tárgyalom a témát a jelen írásban, tekintve, hogy ez egy, az érintett területet körbejáró sorozat első eleme.

A BELÉPTETETŐ RENDSZERREL SZEMBEN TÁMASZTOTT ÁLTALÁNOS KÖVETELMÉNYEK

Az ABV analitikai laboratórium beléptető rendszerének tervezésekor számos körülményt kell számításba venni, különösen a rendszerrel szemben támasztott követelményeinket illetően. Meg kell vizsgálni egyebek mellett az épület tereinek (zónáinak) sajátosságait, azokba a belépésre jogosultak körét, az ABV védelmi szempontból ellenőrzött terek veszélyforrásait. Meg kell határozni, továbbá a beléptető rendszertől megkívánt funkciókat.

A laborépületbe történő be-, és kiléptetés a rendszer primer funkciója, valamint az objektumon belüli mozgások különböző jogosultsági szintek szerinti szabályozása. Napjainkban a jogosultság megállapíthatóságán kívül elvárható igény a jogosultság időben és térben történő lehatárolhatósága és változtathatósága. A beléptető rendszer személykövetési funkciója is lényeges, hiszen a belépésre jogosult tartózkodását, mozgását a laborban követni képes rendszer, nyílván tudja tartani, hogy az ellenőrzött terekben hányan tartózkodtak az időtartamokkal együtt. Az ideiglenes beléptetést megvalósító vendégkártya kezelési funkciója is lényeges a laborüzemeltetés szempontjából.

Biztonsági szempontból fontos, hogy a beléptető rendszerhez, a behatolásjelző rendszer érzékelői csatlakoztathatók legyenek. A laborüzemeltető szemszögéből elvárható igény a beléptető rendszerrel szemben az épület-felügyeleti funkció, amely lehetővé teszi a szellőztető rendszer ventillátorainak, a hűtőrendszer elemeinek a helységben tartózkodástól, illetve a bent-tartózkodók számától függő automatikus be-, és kikapcsolását. A korszerű szoftverek

manapság lehetővé teszik, hogy meghatározott kimeneteket a beprogramozott bemeneti események bekövetkezéséhez hozzárendelve, feltételes műveleteket végezzen el a központ. Kamerákat kapcsolhat be pl. a méregraktár ajtajának, kinyitása, PLC-t (programozható logikai vezérlő) tartalmazó rendszer esetén a légtechnikai berendezés beindítható vagy leállítható különböző időszakokban, illetve eseményvezérelten.

Természetesen az események archiválása és tárolhatósága kiemelt jelentőségű funkciója a rendszernek, valamint a naplózás. Az ABV analitikai laboratórium esetében a fentieken kívül fontos követelmény a labort felügyelő ABV védelmi monitoring alrendszer ellenőrzött terekben elhelyezett detektorainak beintegrálhatósága a biztonságtechnikai rendszer beléptető rendszerébe.

ABV analitikai laboratórium veszélyforrásait figyelembe véve a beléptető rendszernek képesnek kell lennie on-line üzemmódban működnie. Ez az üzemmód biztosítja számos, üzem-, és munkabiztonsági szempontból lényeges funkció installálását.

A beléptető rendszerek alapvető elemei, az objektumok, helyiségek, területek bejáratainál telepített belépési pontok az on-line rendszereknél helyi kommunikációs hálózaton keresztül számítógépes központhoz kapcsolódnak. [7]

Ez a központ képes kell, hogy legyen több belépési pont üzemeltetése esetén is olyan bonyolult döntések meghozatalára, amely az adott ellenőrzött térben benntartózkodó személyek számának, jogosultságának, a laborban elvégzendő feladatok ellátásához kötött jogok meglétének (a meghatározott személyek előbbi szempont alapján történő minősítésnek), az ABV védelmi monitorhálózat detektorai jelzésének, és egyéb, a létesítmény üzemelésének biztonságát biztosító technikai berendezés (pl. szellőztető motorok) működőképességéről jelentést adó szenzorok jelzéseinek együttes értékelését igényli.

Ez elengedhetetlen, ha olyan biztonsági döntési mechanizmusok elvégzését kívánjuk meg, ami a laboratórium teljes biztonságtechnikai rendszerének állapotát figyelembe veszi. Amennyiben például a radiológiai laborban egyidejűleg munkát végző személyek megengedett száma a biztonságos munkavégzés feltételeként maximum 6 fő, akkor a hetedik belépését már nem engedélyezi a rendszer és nem csak a radiológiai laborba, hanem az oktatási zónától elkülönülő laborterületre sem (kivéve ha oda egyébként van jogosultsága, pl. dolgozó). Vagy egy másik esetben a hallgató, akinek az órarendi adatok birtokában előre meghatározott időben a belépési jogosultsága van (pl. oktatási időben 08.00-15.30-ig), a radiológiai laborba nem tud belépni addig, amíg a foglalkozásvezető, illetve a laboráns nem tartózkodik a laborban. A foglalkozásvezető felügyelete és engedélye nélkül ugyanis munkát végezni mérgező harcanyaggal tilos.

Természetesen ilyen esetben több, más biztonsági elemmel szükséges megtámogatni a beléptető rendszert a kijátszhatóság minimalizálása céljából. Ezek közül – nem részletezve a teljes elgondolást - az egyik a beállítható ajtónyitvatartási idő, mely a beléptető rendszer szintén lényeges funkciója. Amennyiben az engedélyezett ajtónyitvatartási idő lejár, a központi vezérlő utasítására az átaresztő pont olvasóterminálja a szabotázsként értékelt eseményről riasztási jelzést küld a központi egységnek.

A beléptető rendszer on-line működését biztosító központ programja – amely egyébként a már meghatározott jogosultságok alapján a kontrollereket vezérli – esetünkben kell, hogy biztosítsa a következő lehetőségeket:

- Bizonyos terekbe csak kettesével biztosítson belépést, amennyiben a helyiség üres: Biztonsági szempontból kiemelt jelentőségű funkció nem engedi, hogy baleseti veszélyforrásokat rejtő terekbe egyedül ne léphessen be senki. Általános sugárvédelmi rendszabály, hogy sugárveszélyes tevékenység végzéséhez legalább kettő dolgozó jelenléte szükséges. Mérgező harcanyaggal is legalább 2 főnek kell foglalkozni, egyik dolgozik, a másik segít és figyeli a szennyeződést. A kétkártyás

zárvezérlés segítségével ilyen helyiségek zárjának nyitása csak akkor engedélyezett, ha két feljogosított kártyát egymás után olvasnak le.

- Bizonyos helyzetekben oldjon az elektromotoros zár reteszelése: A tűzjelző-riasztó rendszer jelzésére a vészkijárat, és a főbejárat – amely lehet ugyanaz a bejárat is – ajtóinak, vagy védelmi filozófiától függően az összes felügyelt ajtó zárszerkezetének kireteszelését biztosítja a biztonságos kimenekülés érdekében. A védelmi céloktól függően egyébként ez változhat, amennyiben az a cél, hogy a veszélyes anyag még ilyen esetekben se kerülhessen ki, éppen a veszélyes területek nyitását nem engedélyezi a rendszer.
- Zóna-kiürülés esetén automatikus zárás: Biztonsági szempontból rendkívül hasznos funkció, amely alkalmazásával a beléptető rendszer nem engedi, hogy a felügyelt terek véletlenül, vagy szándékosan (szabotázs) nyitva maradjanak.
- Bent lévők listázása: Ezzel nem csak a bent tartózkodók számát, hanem személyét tudjuk nyomon követni a rendszer által felügyelt terekben.

A beléptető rendszer működését lényegesnek tartom tehát kiterjeszteni legalább a labortéren belül elhelyezett radiológiai laboratórium és a vegyi laboratórium belépési pontjaira is. Ezekbe a helyiségekbe az ABV analitikai laboratórium STANAG 4632 által meghatározott képességeinek figyelembe vételével feladatfüggően meghatározott belépési jogosultsági szintek differenciálása szükséges. Amennyiben például a laborvezető által elrendelt, vagy engedélyezett toxikus mérgező harcanyaggal történő munkamenet zajlik a laborban megfelelő algoritmussal (kód beütését követően) a beléptető rendszer az érintett laborhelyiségbe csak az előre meghatározott munkatársak belépését engedélyezi (normál üzemelési feltételek esetén). Ezen speciális esetekben a beléptetésre alkalmasnak látszik valamely biometriai alapú személyazonosítással egybekötött beléptetés közvetlenül az érintett laborhelyiségekbe, ez azonban külön vizsgálatot igényel, hiszen a labormunka egyes sajátosságai kizárhatnak bizonyos eljárásokat. A kézgeometriai vagy ujjnyomat alapú azonosítást például nehezíti az, hogy minden olyan művelethez, ahol a kezek aktív anyaggal szennyeződhetnek, vékony sebészeti gumikesztyűt kell viselni.

A vésznyitás lehetőségének biztosítása ugyanakkor minden rendszernél alapvető követelmény. A rendszer lehetővé kell, hogy tegye rendkívüli esemény bekövetkezésekor az áteresztési pontok azonnali nyitását, a bent tartózkodó személyek kimenekülése érdekében. A laboratóriumban végzett STANAG 4632 szerinti tevékenységek végzésekor azonban megfontolandó a veszélyes anyagok nyitással generált „szellőztetéssel” történő kiáramlásának engedélyezése. Ezen anyagok túlnyomó többségével végzett műveleteknél a kérdés külön vizsgálatot igényel.

A beléptető vezérlők tehát kell, hogy rendelkezzenek olyan bemenettel, amely a tűzjelző rendszer vagy a vésznyitó riasztását érzékelve automatikusan nyitják az áteresztő pontokat. Minden beléptetési ponthoz szükséges tervezni ajtónyitó eszközt (pánik gomb) veszélyhelyzet esetére. A vésznyitók általában beütő-gomb megoldásúak. Veszély (vagy annak érzete esetén) a gombát benyomva a kontroller az elektromos zár áramkörét megszakítva az ajtót nyithatóvá teszi. A vésznyitó gombok elsősorban a beléptető-terminálokkal védett belépési pontokkal határolt helyiségekbe kell, hogy felszerelésre kerüljenek, a vegyi laboratóriumba, illetve a radiológiai laboratóriumba az olvasók mellé.

1. ábra. Vésznyitó gomb
(forrás:Tunyogi-Berek)

Az ideiglenes beléptetés igénye szintén érthető. A megfelelő oktatásban részesített laboratóriumi dolgozókon és az ugyancsak kioktatott takarítószemélyzeten kívül ugyanis idegen (látogató, javítást végző személy stb.) felügyelet nélkül nem tartózkodhat az izotóplaboratóriumban.

Az ABV laboratóriumba az ott dolgozókon kívül, belépő látogatóknak biztosítani kell vendégkártyát, mely korlátozott jogosultságokkal ruházza fel az ideiglenesen belépőt. A vendégkártyák külső megjelenésének biztosítania kell az állandó kártyáktól történő vizuális megkülönböztetés lehetőségét, a rendszernek pedig a belépési idő korlátozását.

A fentieken kívül ABV védelmi laboratórium beléptető rendszerének meg kell felelnie a következőkben részletezett és megfogalmazott igényeknek is az ellenőrzött terület védelme érdekében.

A BELÉPTETŐ-RENDSZER SZEREPE AZ IZOTÓPLABORATÓRIUM BIZTONSÁGÁNAK BIZTOSÍTÁSÁBAN

Az ellenőrzött terület védelme

A 16/2000. (VI. 8.), az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról rendelkező EüM rendelet szerinti ellenőrzött terület az a munkaterület, ahol – a részletes kifejtés igénye nélkül - a tevékenységből adódóan az évi egyéni sugárterhelés meghaladhatja az 1 mSv effektív dózist, illetve a szemlencse, a bőr és a végtagok esetében az *egyenérték dóziskorlátok 1/10*–ét. Az ABV védelmi laboratórium ellenőrzött területe annak izotóp laborja.

A rendelet által előírt szabályok közül néhány a korszerű technikai lehetőségek felhasználásával beépíthető - megfelelő detektor felhasználásával – a rendszer belépési protokolljába.

A munkabiztonság területén

Az ellenőrzött terület határait egyértelműen ki kell jelölni, és az ellenőrzött területre való bejutást ellenőrizni kell, illetve az illetéktelen bejutást meg kell akadályozni, a bejáratot a sugárveszélyre utaló jelzéssel és felirattal, valamint a munkaterület, illetve munkahely

megnevezésével el kell látni, a munkaterület műszeres sugárvédelmi ellenőrzését – a sugárzás típusának, a sugárveszély mértékének megfelelő módon – kell biztosítani. [8]

- Az említett jogszabálynak megfelelően az ellenőrzött területen a sugárterhelés korlátozásának, a sugárterhelés valószínűségének csökkentése érdekében és a radioaktív szennyeződés terjedésének megakadályozása céljából a munkaterület műszeres sugárvédelmi ellenőrzését - a sugárzás típusának, a sugárveszély mértékének megfelelő módon - biztosítani kell.

Az izotóplabor folyamatos üzemű sugárzásmérő detektorral történő felszerelése ezt biztosíthatja, amely beintegrálható a komplex vagyonvédelmi rendszer elektronikai komponensének hálózatába. Ennek megvalósulása esetén már csak egy lépés egy másik lényeges feladat, a laboratórium környezetének sugárvédelmi ellenőrzésének automatizálása.

2. ábra. BNS-97 sugárzásvédelmi monitor [9]

Az izotóp laborban egyedül dolgozni tilos, a beléptető terminálnak biztosítani kell, hogy egyedül belépő egyébként jogosultsággal bíró személy az izotópterzorban tárolt anyagokhoz fizikailag ne férhessen hozzá. Erre lehetséges megoldásnak látszik a trezor kulcsainak biztonságos elhelyezésére szolgáló PIN kódos hozzáférést biztosító kulcsszekrénynek az izotóplabor előkészítőjében történő rögzített elhelyezése, melynek nyitását a rendszer abban az esetben engedélyezi, ha laborban egynél több, megfelelő jogosultsági szinttel bíró személy (vendégkártya nem érvényes) egyidejűleg van jelen.

Fontos biztonsági rendszabály, hogy a meleglaboratóriumba való belépés előtt 4–5 perccel a légelszívót meg kell indítani, hogy a laboratórium esetleg szennyeződött levegőjét frissel kell kicserélni.

A beléptető rendszernek biztosítania kell egyrészt a belépési késleltetést, másrészt a rendszerbe integrált épületautomatikai eszközök segítségével a szellőztető ventillátorok beindítását.

Baleset elhárítás területén

A munkahely, személy vagy környezet törés, technológiai fegyelem megsértése, vagy más hiba következtében sugárzó anyaggal szennyeződik, első teendő a munka azonnali beszüntetése. Az érintett területet el kell határolni és a személyek, illetve a tárgyak további szennyeződésének elkerülése érdekében a szennyeződés továbbterjedését meg kell akadályozni. [10]

A szennyeződés kiszivárgásának megelőzésére a helyiségből kivezető minden nyílást megfelelő módon kell zárni. Ennek a követelménynek a teljesülése érdekében szükséges tehát a laboratórium sugárvédelmi detektorainak, valamint a vagyonvédelmi rendszer beléptető komponensének közös platformon történő elhelyezése. A szennyezett helyiségbe mindaddig tilos belépni, amíg a dekontamináció vezetésére kijelölt személy arra engedélyt nem ad. [11]

Szennyezés bekövetkezése esetén szükséges sugármentesítési tevékenység elvégzése érdekében kijelölt személyeket viszont a rendszernek be kell engednie, akiknek a körét és belépési jogosultságát előzetesen a laborvezető meghatároz és rögzít a rendszerben. A balesetek során bekövetkezett sugárszennyeződés felszámolását ugyanis csak sugárvédelmi szakemberek irányíthatják.

- Zárt radioaktív sugárforrással való munkavégzést követően a sugárforrást állandó tároló helyére kell juttatni. A biztonságba helyezés megtörténtéről a kezelőnek sugárzásméréssel meg kell győződnie. A nyitott radioaktív készítményekkel végzett munkák csak izotóplaboratóriumban végezhetők. [12] Az izotóplaboratóriumból ellenőrizetlenül radioaktív anyag nem kerülhet ki.

Mindez viszonylag egyszerűen megvalósítható a beléptető-rendszerbe integrált detektor (sugárkapu) segítségével.

3. ábra. BNS-94P és PN bejárat fölé telepítve [13]

Személyi dozimetria követelményeinek teljesülése

- A foglalkozási sugárterhelésnek kitett munkavállaló munkavégzés során, az alkalmazott mesterséges és fokozott sugárterhelést eredményező természetes forrásokból származó, külső és belső sugárterhelés együttesen, egymást követő 5 naptári évre összegezve nem haladhatja meg a 100 mSv effektív dóziskorlátot. Az effektív dózis egyetlen naptári évben sem haladhatja meg az 50 mSv értéket. Tekintet nélkül az effektív dózisra megszabott fenti korlátra, a szemlencsére vonatkozó évi egyenérték dóziskorlát 150 mSv. A bőrre – bármely 1 cm^2 területre átlagolva –, továbbá a végtagokra vonatkozó évi egyenérték dóziskorlát 500 mSv.(16/2000 EüM. Rendelet)

RFID dózismérők alkalmazásával ezek a követelmények teljesíthetők, sőt továbblépve, a beléptető rendszer nyilvántartó programjának segítségével a sugárvédelmi szolgálat feladataként meghatározott, személyi sugárterhelés ellenőrzése és eredményének nyilvántartása is automatikusan az ellenőrzött területről történő kilépést megelőzően megvalósul.

- Sugárveszélyes munkahelyeken a sugárzási viszonyokat folyamatosan ellenőrizni kell, sőt, azokon a munkahelyeken, ahol fennáll annak a lehetősége, hogy a külső sugárterhelés az évi 6 mSv effektív dózist meghaladja, az OSSKI5 által beszerzett és

[5] Országos „Frédéric Joliot-Curie” Sugárbiológiai és Sugáregészségügyi Kutató Intézet

kiadott személyi dózismérő mellett, a helyszínen leolvasható személyi dózismérőt vagy hang-, illetve fényjelzést adó egyéni dózisszintjelzőt is használni kell. [14]

Szükséges tehát olyan dózismérő, illetve dozimetriai rendszer alkalmazása, amely a központi egységével és a beléptető rendszer olvasó terminájával RF kommunikációra képes az elektronikus nyilvántartás, valamint az ahhoz kapcsolódó rendszabályok biztosítása érdekében.

- A napi sugárveszélyes tevékenység befejezésével, illetve munkaidőn kívül, a dózismérőt olyan helyen kell tárolni, ahol a természetes háttérsugárzáson felül, járulékos (nem a foglalkozás gyakorlása közben kapott) sugárzás nem érheti. A dózismérő kezelése vagy viselése során nem sérülhet meg, és illetéktelenek nem férhetnek hozzá.

A beléptető rendszer képes ennek a követelménynek a feltételeit is biztosítani olyan módon, hogy a rádiofrekvencián kommunikáló dózismérők a kiértékelő dokkoló-egységének jeleit feldolgozó beléptető szoftver a dózismérők - az érintett személyek adataival együtt történő – nyilvántartásán kívül képes a doziméterek nyomkövetésére, és a laborépületből történő véletlen kivitelének hangjelzéses figyelmeztetéssel megvalósuló „megakadályozására”. A dozimetriai rendszer beintegrálása a beléptetés algoritmusába biztosítja, hogy amennyiben nincs a helyén a dokkoló-egységben a dózismérő figyelmeztető hangjelzést ad a beléptető rendszer, csupán programozás kérdése a kilépési engedélymegvonás hozzárendelése az eseményhez.

Olyan RFID dózismérők alkalmazása indokolt, melynek nyilvántartó szoftvere képes folyamatos statisztika vezetésére és dózis túllépés esetén megvalósítja belépés fizikai korlátozását. A rendszernek képesnek kell lennie hozzárendelni a dózismérőket az egyes dolgozókhoz, vezérelni a beléptető rendszer kapuit, munkavégzést követően kiolvasni és letárolni a dózismérők által mért adatokat, rögzíteni azt ellenőrzött területre történő be- és kilépések adatait. Ezekkel a képességekkel saját adatbázisában tudja összesíteni az aktuális személyi dózisokat, valamint a kártyás azonosítás miatt a tévedés lehetősége kizárható.

Ellenőrzött területről történő kiléptetés

A dózismérők adatainak, és az eszközök letárolásával egybekötött kiléptetési igény mellett más szempontnak is érvényesülnie kell a kiléptetési algoritmus szintjén.

A sugárveszélyes munkahelyen nyílt izotópokkal dolgozó személyeket érhet szennyeződés, elsősorban kezükön vagy cipőjükön, ezért biztonsági szempontból lényeges eleme kell, hogy legyen a kiléptetésnek a szennyezettség ellenőrzése.

A kéz–lábmonitorok alkalmazásával teljesül ez a követelmény, a mérőhelyet a beállított mérési időtartam letelte előtt elhagyó személy távozásakor a rendszer figyelmeztető jelet szolgáltat.

4. ábra. BNS-94PH Hibrid sugárkapu személyek ellenőrzésére
(forrás: BNS-98 Műszaki Dokumentáció, Gamma Műszaki zRt.)

Természetesen a fentiekben felvázolt rendszer egyes moduljai külön-külön és egyes munkaterületeken együtt is számos sugárveszélyes munkahelyen üzemelnek, alkalmazásuk nem új keletű. A beléptető rendszer képességeivel együtt történő bemutatásukkal rá kívántam világítani arra, hogy olyan különleges rendeltetésű objektumok védelmének kialakításakor, mint például egy ABV analitikai laboratórium, a komplex vagyonvédelmi rendszer elektronikai komponense beléptető rendszerének tervezésekor milyen olyan lényeges tényezőket kell figyelembe venni, melyekkel az objektumvédelem általános gyakorlatában ritkán kell számolni.

ÖSSZEFOGLALÁS

Az ABV fenyegetettség napjainkban sem mutat csökkenő tendenciát.

Az ABV analitikai labor a jövőbeni ABV kihívásokkal szemben tett válaszlépés egyik eleme, és a kívánalom az, hogy előremutató jelleggel új és korszerű elvek és metódusok kialakításának színtere legyen. Az ABV védelmi háttér-laboratórium bármely funkciójában – akár oktató,- kiképző-, kutató,- akkreditált analitikai háttér-laboratóriumként – az ott végzett tevékenység veszélyes radioaktív, mérgező, esetleg fertőző anyagok esetenként mérgező harcanyagok szükségszerű felhasználásával történik. A laborkomplexumban kialakított ellenőrzött munkaterületek és munkafolyamatok védelme kiemelt fontosságú. Önmagukban a beléptető rendszerek nem képesek egy objektum megvédésére, csak az áthaladási pontok forgalmát bonyolítják le. A beléptető rendszerek csak részei egy épület biztonsági rendszerének, más biztonsági berendezésekkel együttműködve viszont igen hatékony védelmet tudnak nyújtani.

A biztonsági és beléptető alrendszernek és az ABV védelmi alrendszernek tehát nem egymástól függetlenül kell működnie.

Az ellenőrzött területeken és egyéb terekben felszerelt nukleáris detektorokról, valamint a biztonsági rendszer érzékelőiről érkező jelzéseket olyan rendszernek kell feldolgoznia, amely alkalmas azok együttes kezelésére és vezérelni tudja a jelző-riasztó egységeket a szükséges épület-felügyeleti berendezésekkel együtt.

Irodalomjegyzék

[1] Berek Tamás: ABV (CBRN) analitikai laboratórium, mint művelettámogató speciális vegyivédelmi képesség , 2011. Hadmérnök http://www.hadmernok.hu/2011_1_berek.pdf

[2] STANAG 2112 Nuclear, biological and chemical reconnaissance, 2005.

[3] [15]ATP-3.8.1 Specialist NBC defense cababilities, 2005

[4] AAP 10 NATO kézikönyv a mérgező harcanyagok mintavételéhez és azonosításához

[5] Földi L.- Vágföldi Z.: Korszerű telepíthető laboratóriumok és analitikai módszerek mérgező harcanyagok és veszélyes ipari anyagok azonosítására, http://www.hadmernok.hu/2010_4_vagfoldi_foldi.pdf

[6] László Éva: Polimeráz láncreakció a géntechnológia nélkülözhetetlen eszköze in: Műszaki Szemle 7-8. sz., Babeş-Bolyai Tudományegyetem, Kolozsvár

[7] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Doktori (PhD) értekezés, 2009.

[8][10] A ZMNE sugárvédelmi szabályzata, 2009

[9][13] Komplex CBRN védelmi épületfelügyeleti rendszer, belső műszaki dokumentáció, Gamma Műszaki zRt. 2009

[11][12][14]16/2000. (VI. 8.) EüM rendelet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Dávidovits Zsuzsanna
davizsu@vipmail.hu

A KATONAI MISSZIÓK VÍZELLÁTÁSA, ZENON VÍZTISZTÍTÓ RENDSZER HASZNÁLATA

Absztrakt

Az esettanulmányom célja, hogy a vízről, mint „életet adó elem”-ről írjak. A mindenki által már jól ismert fontosságán – mint a biológiai szükségletként és a további felhasználhatóságain túl, illetve evvel összefüggésben – a célom, hogy szemléltessem a vízellátást, a víz felhasználhatóságát a katonai missziók során. Felmerül ugyanis a kérdés, hogy egy sivatagosabb területen hogy is lehetséges annyi katona és ember napi vízszükségleteit, vízfogyasztását megvalósítani.

The case study is designed to provide water, such as „life-givig element” to write about. The importance of well-known by everyone - as the biological needs, availability and further beyond, or in conjunction with this - my aim to illustrate the water supply, the water's availability for military missions. Indeed the question arises whether it is possible to achieve the daily water needs, and water consumption of so much troops and people on a deserter field.

Kulcsszavak: *víz, katonai misszió, vízfogyasztás, víztisztító berendezés ~ water, military mission, water consumption, water purification equipment*

A VÍZ, MINT ALAPVETŐ SZÜKSÉGLET

"Víz! Se ízed nincs, se zamatod, nem lehet meghatározni téged, megízlelnek anélkül, hogy megismernének. Nem szükséges vagy az életben: maga az élet vagy." (Saint-Exupéry) [1] A víz alapvető alkotórésze az élő és élettelen természetnek. Jelentősége abban rejlik, hogy a Föld felszínét 70,8 százalékban borító víz a legnagyobb tömegben előforduló anyag, mennyisége gyakorlatilag állandó, becslések szerint körülbelül 1,4 milliárd km³. Ennek 97,3 százaléka sós tengervíz, a többi édesvíz, de ebből több, mint 2 százalék jég formájában van jelen. Jelentős vízmennyiség van a légkörben és a talajrétegekben is. Összességében ez azt jelenti, hogy sajnos az úgynevezett iható édesvíz - a folyók és édesvizű tavak vízkészlete és a felszín alatti vízkészlet - csupán mintegy 0,6 százalék, de bolygókon ennek eloszlása sem egyenletes. A víz tehát életet adó elem. Az élet fenntartásához kifogyhatatlan készletekre lenne szükségünk, azonban Földünk édesvízkészlete véges. [2]

A táplálkozásunk legfontosabb eleme is a víz. A megfelelő vízfogyasztás egy átlagos testű ember számára napi 2-3 liter. A nem megfelelő mennyiségű vízfogyasztás pedig a pszichikai tűneteken túl, szervezetünk kiszáradásához vezethet. Az ember élelem nélkül 1-2 hétig kibírhatja, míg iható víz nélkül csak 1 vagy 2 napig. Így nem is csoda, hogy a víz a jól ismert Maslow piramis legalsó, a piramis alapköveit alkotó részében foglal helyet. A piramis legalsó szintjén ugyanis azok a szükségletek helyezkednek el, melyek az életben maradás fiziológiás szükségleteihez tartoznak. Maslow rendszerében tehát ezek a szükségletek hierarchikusan egymásra épülnek, egyik szint kielégítése a következő szint motivátorként való fellépését jelenti. Az egyik szinten lévő szükségleteket legalább részben ki kell elégíteni, mielőtt a felette lévő szint szükségletei a cselekvés jelentős meghatározóivá válnak. A fiziológiás szükségletek után a biztonsági szükségletek, majd a szeretet- és közösséghez való tartozás igénye, erre épülve a tisztelet- és elismerés iránti igény és végül a tudás-és megértés iránti vágy építőkövei kerülnek egymásra. A többi négy szint azonban háttérbe szorulhat, ha a legalapvetőbb fiziológiai szükségletek, úgy, mint az éhség, a szomjúság, és az aluszékonyság nem valósulhat meg megfelelően. A fiziológiai szükségletek ugyanis a legerősebben jelentkező, legdominánsabb szükségletek, és ha akár csak egy közülük nincs kielégítve, mivel ezen szükségletek viszonylag elszigetelhetők, testileg lokalizálhatók – akkor minden egyéb szükséglet háttérbe kerülhet vagy akár meg is szűnhet. [3]

1. ábra. Maslow motivációs piramisa
forrás: http://www.ektf.hu/hefoppalyazat/pszielmal/maslow_motivcis_piramisa.html
(letöltés: 2011. 06. 16.)

A fejlett országokban és hazánkban is teljesen természetes, hogy a lakosok többsége a Maslow piramis tekintetében nem a legalsó szinten állnak, hanem valamely felsőbb szinteken próbálják kielégíteni céljaikat és vágyaikat. Az ember a napi vízfogyasztásán túl az alapvető higiéniás szükségleteinek megoldására is vizet használ. Szükség van a vízre a mosdás, a tisztálkodás, a szennyezések eltávolítása kapcsán is. A víz egészségügyi és szórakozási szempontból az üdülés, a vízi sportok és a gyógyászat jelentős tényezője is. (A szórakozás pedig már a Maslow piramisának magasabb szintjén helyezkedik el.) A víz a közlekedés, az ipar, a mező-, erdő-, és halgazdaság fontos alap- és segédanyaga, szállítóközege, valamint energiaforrás és energiahordozó. Bár a vizet a különböző országok eltérő módon hasznosítják,

a mezőgazdaság igényli a legnagyobb mennyiséget: átlagosan a világon felhasznált víz 73 százalékát. A különböző iparágak, ipartelepek vízfelhasználása is nagyon sok. A vizet hasznosíthatják vegyi folyamatokban nyersanyagként, oldószerként, vagy hőhordozóként, hogy csak a legismertebbeket említsem. [4] [5]

Miközben a Föld lakossága naponta mintegy háromszázezer fővel gyarapodik, víztartalékaink mennyisége hellyel-közzel állandó (sőt: apad); óvatos becslések szerint a világon száz ember közül 42 nem jut annyi vízhez, amennyire egészséges életviteléhez feltétlenül szüksége lenne, s amit szakemberek naponta és fejenként minimum 100 literben állapítottak meg. Továbbá a Földön édesvíz-készletének az eloszlása is változó. Elsősorban a fejlődő országok számára jelent ez gondot. [6]

A víz tehát életet adó elem. Az élet fenntartásához kifogyhatatlan készletekre lenne szükségünk, azonban Földünk édesvízkészlete véges. Sajnos mára már korunk egyik legnagyobb globális problémájává vált az ivóvízhiány. „Egy ENSZ jelentés szerint hat emberből egynek nem jut tiszta víz.”- Jin Zindel szerint. A világszervezet tudósai szerint 2020-ra Dél-Amerikában és Afrikában akkora lesz az ivóvízhiány, hogy annak demográfiai hatásai is várhatóak. A jövőben egyre nagyobb lesz a valószínűsége annak, hogy a vízhiány miatt fegyveres konfliktusok alakulnak ki. És ez sajnos már nem is jövő, hiszen volt már rá példa. 2007-ben katonai összecsapásokhoz vezetett az afrikai Csád-tó száradása, mely Darfuri-konfliktusként ismeretes. Egyiptom pedig még 1991-ben jelentette be, hogy kész katonai beavatkozás árán is megvédeni jogát a Nílus vizére, Szudánnal és Etiópiával szemben. Az Okavango folyó vizén pedig Nabídia, Angola és Botswana vitatkozik. E három ország és a Dél-afrikai Köztársaság a Zambézi folyón is marakodik. Törökország pedig gátakat emel, növelve az ellentéteket Szíriával és Irakkal. Természetesen ilyen jellegű feszültségek nem csak a legszárazabb kontinensen vannak. India és Kína határterületén folyó Brahmaputa folyó elterelése komoly feszültséget okoz Indiának. Jelenleg 5 millió kínai lakos szenved a vízhiány miatt főleg az ország északi területein. Görögország Kimolosz nevű szigetén is kiapadtak mára már a tiszta ivóvízlelőhelyek. A Közel-Kelet térségei is vízhiányos területek közé tartozik. Mivel arrafelé gyakorlatilag a Jordán (és földfelszín feletti, illetve alatti csatolt részei) jelentik az édesvizet, vízgyűjtő területének négy állama: Libanon, Izrael, Jordánia és Szíria időről időre egymásnak feszíti izmait és megpróbálkozik a bibliai folyó felett elérhető maximális ellenőrzés megszerzésével. Biztonságpolitikai szempontból mára már az ivóvízhiány szinte az egész világon kockázati tényezővé vált. A dolgozatom terjedelme miatt azonban nem térek ki bővebben az ivóvízháborúkra.[6] [7]

A VÍZHIÁNY EGÉSZSÉGÜGYI ÉS PSZICHOLÓGIAI HATÁSAI

Éghajlati szempontokat figyelembe véve az édesvíz-készlet aránya a sivatagos területeken a legrosszabb. A szárazabb éghajlati övben élők számára előfordul tehát, hogy napi kihívást jelentsen, hogy vízhez jusson. A szélsőséges időjárási viszonyok, főleg a forró száraz éghajlati körülmények, az emberek szervezetét fokozottabb terhelésnek teszik ki. Az ilyen területeken harcoló és állomásozó katonáknak és misszióknak azon túl, hogy háborús övezetben már eleve nagyobb fizikai és harci veszélynek vannak kitéve, számolniuk kell az extrém éghajlati körülményekkel is. Hazánk is ráadásul egyre nagyobb szerepet vállal ilyen sivatagi hadviselésben és így békefenntartásban is. Az ezeken a területeken szolgálatot teljesítők szervezete tehát még fokozottabb megterhelésnek van kitéve. Ilyen szélsőséges klímaviszonyok mellett nagyobb eséllyel jelentkezhetnek metabolikus, víz-elektrolit és sav-bázis háztartásbeli zavarok, csökken a koncentrációs képesség, és megnő a kardiovaszkuláris események hatása is. Ezek a kórélettani hatások nehezítik és veszélyeztethetik a katonák harci feladatainak a végrehajtását, továbbá egészségi állapotukat. Például folyadék – ivóvíz hiányában ilyen forró éghajlati övű területeken a hőség súlyos víz-elektrolit háztartás

zavarokat okozhat, mely eleinte csak hő-stresszhez, hő-kimerüléshez, alacsony vérnyomáshoz, szinkopéhoz, fájdalmas izomgörcsökhöz, majd hőgutához vezethet. Bár akklimatizálódással ezek a káros hatások csökkenthetőek, mégis a fő szerepe a megelőzésnek van. Ebben az esetben tehát a megszokott, hétköznapi vízfogyasztáson túlmenően, fokozottabban kell figyelni és természetesen biztosítani a szervezet számára szükséges folyadékmennyiséget. A magas hőmérsékletű területeken végzett szolgálatok esetében a katona gyakran teszi ki magát a dehidratáció, azaz a kiszáradás veszélyének. A vízveszteség testének akár 8-10 %-át is elérheti – 25%-os testfolyadék-vesztés pedig már halálos is lehet. Ez az izzadásból, az elégtelen folyadékbevitelből, illetve a csökkent szomjúságérzésből adódik. A vízveszteség hatására megnő a szervezet megterhelése, ami teljesítménycsökkenéshez vezet, további idő elteltével pedig hősérülést is okozhat. A megfelelő mennyiségű folyadékbevitel elengedhetetlen. Ráadásul az ilyen sivatagosabb területeken – több tanulmány szerint – a szomjúságérzet nem biztos jelzője a test kiszáradásának. Szomjúságérzet csak a teljes test vízmennyiségének az 5%-ának elvesztése után jelentkezik. Azonban még ez a kis mennyiség is negatívan befolyásolja az ember teljesítményképességét, reakcióidejét. Ebben az esetben a megoldás egyszerű: meg kell tanítani a katonákat, hogy rendszeres időközönként vegyenek magukhoz folyadékot, ne csak akkor, amikor szomjasnak érzik magukat. A folyadék- és ionpótlás fontosságát már több katonai művelet igazolta: például folyadékhiány hatására kialakult hő-sérülés csaknem 20000 embernyi veszteséget okozott az egyiptomi katonák körében az 1967-es arab-izraeli 6 napos háború során. [8]

A testi – szervi tüneteken túl a vízhiány pszichés tünetekkel is jár. A dehidratáció például a depresszióért és a stresszért is felelős lehet. A vízhiány épp olyan pszichológiai folyamatok elindítására készteti a testünket, mint mikor a stressz ellen küzdünk. A szervezet ugyanis a raktárkészletekhez nyúl, így a víztartalékaink is megcsappannak. A vízhiány ezért a stresszhez, ami pedig további vízhiányhoz vezet. A félelem, az aggódás, a tartós érzelmi bizonytalanság és a düh kialakulása mind-mind az agyszövetek ki nem elégített vízigénye miatt bekövetkező vízhiány eredménye. Az ilyen jellegű tűnetek egy normál körülmények közt élő és dolgozó ember számára is figyelmeztetőek, azon emberek számára, akik pedig eleve stresszes életfeltételek közt élnek és/vagy dolgoznak, még fontosabb ezeknek a tűneteknek a csökkentése és megszűntetése. A katonák számára, akik pedig akár hadműveleti, akár nem hadműveleti feladatokat látnak el a hadműveleti területen, ezért mindenképp komolyan kell venni a szervezet folyadékvesztésének esélyeit.

A vízhiányos területeken, ha van is víz és vagy elő lehet állítani, nagyon fontos a vízmennyiségén túl, annak minősége is. Főleg azokon a területeken, ahol manapság a legtöbb katonai és békefenntartói műveletek zajlanak, jellemző a területekre, hogy nagyon nagy a szárazság, aminek hátrányáról már fentebb írtam. Továbbá ezek a területek nem a fejlett, hanem a fejlődő országok közül kerülnek ki, ahol a szegénység, éhezés vagy a nem megfelelő higiéniás körülmények a jellemzőek. A nem megfelelő higiénia pedig maga után vonja a fertőzések és járványok kialakulását is. Ez a víz szempontjából is így van, a vízszennyezések során fellépő fertőzések jelentős és súlyos megbetegedéseket, akár halált is okozhatnak. Ezek a fertőzések kialakulhatnak szándékos emberi cselekedet vagy emberi mulasztás vagy nem odafigyelés következményeként. A háborús területeken ugyanis jól ismert és alkalmazható tett/hadicsel az ellenség bénítása érdekében a vízlelőhelyek elszennyezése vagy megmérgezése. A víz esetében biológiai -, vegyi és radiológiai szennyezésekről lehet beszélni. A vízbe jutatott biológiai harci anyagok közül főleg a hastífuszt, a kolerát említeném. Ha például vízbe juttatnának például Botulinum toxint, akkor az félmilliárd ember halát okozná. Az emberi mulasztás megakadályozására ezekben az esetekben jó példa lehet, hogy a vízlelőhelyeket, vízelőállító rendszereket megfelelő körültekintéssel kell őrizni és védeni. Továbbá ezért is kell megfelelő szakmai hozzáértéssel azokat a szükségszerű rutin

vizsgálatokat elvégeznie a víztisztító századnak vagy az odavezényelt egészségügyi, vegyvédelmi szakembereknek, hogy az esetleges fertőzéseket megakadályozzák.

KATIONAI MISSZIÓK VÍZELLÁTÁSA

Felmerül ezek után az a kérdés, hogy főleg azokon a területeken, ahol még a helyi lakosság számára sem rendelkeznek elegendő mennyiségű és megfelelő minőségű vízzel, egyáltalán, hogy tud megvalósulni ezekben a térségekben az ott tartózkodó - a háborús (harc, hadművelet) és a nem háborús (válságkezelés, béketámogató) katonai műveletekben részvevő – katonák vízellátása?

Ezt a kérdést pedig két oldalról közelítem meg. Egyrészt, hogy a vízellátás milyen katonai csapatok részvételével és irányításával, hogy is képes megvalósulni. Másrészt pedig vegyészmérnöki nézőpontból vizsgálva a kérdést, milyen kémiai és biológiai és technológiai módszerek szükségeltetnek a háborús és békefenntartói területeken lévők vízigényeinek biztosításához.

Műszaki támogatás

Hazánk politikai és morális kötelességnek tartja, hogy békefenntartó kötelezettségeinket a NATO[1], az ENSZ[2], az OSCE[3] és más nemzetközi szervezetek égisze alatt sikeresen ellássa. Jelenleg békefenntartóink a világ különböző területein jelen vannak, például: Koszovóban, Ciprusok, Irakban, Afganisztánban, mint a KFOR[4], az EUFOR[5], stb. nemzetközi erők részeként. Haderőink feladatai sokrétűek: a legtöbbször katonai békefenntartás, de Tartományi Újjáépítési Csoport részeként is vannak fontosabb szerepvállalásaink, mint például Afganisztánban. Békefenntartásban való hazai csapataink részvétele mára már nem elhanyagolható, ezért módot kell találnunk arra is, hogy csapataink teljesítőképességét milyen módon maximalizálhatnánk a leghatékonyabban.

A katonai műveletek során használt víz kitermelése, előállítása és tisztítása a műszaki támogatás feladatai közé tartozik. Hazánk a NATO-hoz való csatlakozása - az új szövetségi rendszer követelményeinek való megfelelés érdekében - a Magyar Honvédségen belül valamennyi fegyvernem és szakcsapat számára új kihívásokat jelentett és jelent napjainkban is. Az egyes országok műszaki doktrínáinak tanulmányozása során lassan-lassan körvonalazódott a NATO-tagországokban használatos műszaki támogatás cél és feladatrendszere, a műszaki csapatok rendeltetése és alkalmazásuk elvei. A műszaki támogatás a harc-, hadműveleti támogatás része. Magába foglalja mindazokat a speciális rendszabályokat és tevékenységeket, amelyeket a háborús katonai műveletek (harc, hadművelet) valamint a nem háborús katonai műveletek előkészítése és végrehajtása során műszaki feltételként meg kell teremteni a feladatot végrehajtó csapatok tevékenységének sikeres megvalósításához. [9]

[1] North Atlantic Treaty Organisation, mely magyarul az Észak-atlanti Szerződés Szervezetét jelenti.
[2] Egyesült Nemzetek Szervezete
[3] Organization for Security and Co-operation in Europe, mely az Európai Biztonsági és Együttműködési Szervezetet jelenti. A magyar rövidítése az EBESZ.
[4] Kosovo Force
[5] European Union Force

A műszaki támogatás megszervezésének és végrehajtásának célja a rendszeresített vagy a feladatok végrehajtásához biztosított műszaki (hadi-) technikai eszközök, felszerelések és anyagok célirányos alkalmazásával:

- a saját illetve a támogatott erők mozgásának, akadályleküzdő- és túlélőképességének fenntartása, fokozása;
- az ellenség mozgásának, tevékenységének akadályozása;
- részvétel a katonai infrastrukturális, a környezetvédelmi és kárelhárítási feladatok végrehajtásában.

A műszaki támogatás fő feladatai:

- a saját csapatok mozgékonyságát támogató feladatok, mint például a mozgási pályák műszaki felderítése, menetvonalak építése, aknamentesítési műveletek, műszaki zárak leküzdése.
- az ellenség mozgékonyságát akadályozó feladatok közé tartozik például műszaki zárak telepítése.
- a túlélőképesség fenntartását, fokozását biztosító feladatok például: tábori erődítési építmények létesítése, a csapatok által megszállt körletek, vezetési pontok berendezésére, a harci anyagi készletek megóvására, az álcázás műszaki rendszabályainak végrehajtása.
- az egyéb (más vagy általános) műszaki feladatok, mint például: speciális műszaki szakfelderítés végrehajtása, a csapatok ellátását biztosító fő ellátási útvonalak javítása, fenntartása, részvétel fontos vasúti, kikötői létesítmények építésében, javításában, azok működőképességének biztosításában, részvétel az infrastrukturális tevékenységek műszaki támogatásában, a műszaki szakfeladatokhoz szükséges építményelemek, szerkezetek előkészítése. [10]

Az egyéb műszaki feladatok közé tartozik a víz kitermelése és tisztítása. A vízkitermelés és tisztítás végrehajtásának célja a csapatok vízszükségletének biztosítása. A csapatok vízellátása magába foglalja a vízlelőhelyek felderítését, a víz kitermelését és tisztítását valamint tárolását és elosztását. E feladatok közül a vízlelőhely felderítése, a víz kitermelése és a tisztítása képezi a műszaki támogatás részét. A csapatok a vízellátást alkalmasság szempontjából ellenőrzött vízlelőhelyeken — elsősorban a helyszínen vagy annak közelében fellelhető csővezetékes hálózatok, fúrt kutak, tárazók felhasználásával — berendezett vízellátó pontokról saját vízszűrő eszközeikkel önállóan valamint vízellátó alegységek bevonásával — vízközpontok létesítésével — hajtják végre. A vízlelőhelyek felderítését a műszaki alegységek a vegyvédelmi és az egészségügyi szolgálat képviselőivel együttműködve végzik. A vízellátó alegységek feladata az általuk berendezett vízközpontokon a víz kitermelése és tisztítása. A vízellátási feladatok megszervezésében a műszaki szolgálat mellett tevékenyen részt vesz: a hadművelet (G3, S3 törzs), a vízellátás általános irányelveinek és nagyságrendjének kialakításában; az egészségügy a vízvizsgálat és tisztítási eljárások ajánlásában; a műszaki és logisztika szolgálat a vízforrások felhasználásra alkalmassá tételében, a víz kitermelésében, összegyűjtésében, tisztításában, kezelésében, raktározásában valamint a vízellátó pontok működtetésében. [11]

A MAGYAR VÍZTISZTÍTÓSZÁZAD

A Magyar Honvédség a víztisztítás kapcsán komoly fejlesztésbe kezdett, és a nemzetközi katonai műveletek támogatására is ez az egyik felajánlott képességünk. Ennek oka az, hogy amíg a NATO feleslegekkel rendelkezik harci csapatokból, hiányok vannak a harci támogató- és kiszolgáló-képességek területén. Ezt a hiányt a tagországok – elsősorban a kisebb haderővel rendelkező nemzetek – úgy igyekeznek kompenzálni, hogy szakosodnak. Hazánk ilyen specializálódásként tábori víztisztító-képességet épített ki. „A víztisztító- képesség a szövetség területén kívüli, vízszegény területen, befogadó nemzeti támogatás hiányában végrehajtandó műveletek során lesz kiemelkedően értékes hozzájárulás." A Magyar Honvédség 37. II. Rákóczi Ferenc Műszaki Zászlóalj egyik alegysége a víztisztítószázad, melynek rendeltetése, hogy a műveletek teljes skáláján képes legyen ivóvíz biztosítására. [12]

A magyar vízellátó állomás

A 2003-as NATO prágai csúcsértekezletén tett hazai felajánlásainknak megfelelően egyértelműen meghatározta a honvédség jövőjét. Ennek érdekében a Magyar Köztársaság növeli a béketámogató, és egyéb szövetségkötelékben végrehajtandó műveleti képességeit. Gyakorlatban ez azt jelenti, hogy a területvédelmi elv helyett, kis létszámú, önkéntes, mozgékony, professzionálisan felkészített, képességorientált haderőt hozunk létre. Ez okból új elemek is előtérbe kerülnek, ilyen CIMIC, azaz a civil katonai együttműködés szervezeti formái. [13] Erre jó példa azon víztisztító állomás gyártása és kialakítása, melyet egy hazai cég, a Zenon System Kft. gyártott kizárólag a Magyar Honvédség számára a Magyar Honvédelmi Minisztérium megrendelése alapján.

A víztisztító állomás széles körben használható, úgy, mint a harc-hadművelet megvívása estén, a béketámogató műveleteknél, a befogadó nemzeti támogatás feladatai során, továbbá jól alkalmazhatók olyan természeti és civilizációs katasztrófák esetén, ahol elszennyeződnek a kutak és az ivóvízhálózatok. A nagyteljesítményű tábori vízellátó állomás édesvíz, brakkvíz (természetes szennyeződéseket tartalmazó sós vizek), tengervíz és NBC szennyezett vízből egyaránt képes emberi felhasználásra alkalmas ivóvizet előállítani, azaz minden típusú felszín alatti és felszínfeletti vizekből képes ivóvizet előállítani. A berendezést 20 lábas konténerben lehet elhelyezni, mely a NATO és az európai előírásoknak megfelel. A vízellátó állomás szállítása légi,- vízi,- és szárazföldi szállításra alkalmas. A berendezés telepítési és lebontási ideje is: maximum 30 perc két fővel. A rendszer automatikus működtetésű. A rendszer energiaellátását egy 64 KW üzemi teljesítményű aggregátor biztosítja. Az optimális kihasználtsághoz 13,5 m^3/h nyersvíz felhasználása szükséges. Normál üzemeltetéssel óránként 5 m^3 ivóvíz állítható elő. Ez a tábori vízellátó állomás olyan technológiával rendelkezik, amely mind az MSZ 450-1/1989, az MSZ 450-2/1991, az MSZ 450-3/1990 szabványoknak és mind a NATO STAANG2136 számú normatív dokumentumban meghatározott ivóvíz minőségi követelményeknek megfelel. [14]

A vízellátó állmás a víztisztításra ZeeWeed ultraszűrést és fordított ozmózis víztisztítási technológiákat használ. A membránszűrési technika segítségével az oldott anyagokat képes a folyadékokból elválasztani. A nyomás alatt működő membrántechnikai eljárások során, mint például a fordított ozmózis, a nanoszűrés, a mikroszűrés és az ultraszűrés, a vízkezelésben olyan szeparációs technikát jelentenek, mely a sóktól a mikroorganizmusokig terjedő különféle anyagok eltávolítására alkalmas. Az ultraszűrés során a szűrést a szűrendő folyadékba bemerítve telepített membránmodulok és ezeket kiszolgáló gépészet végzi. A modulok kötegekbe vannak rendezve, és ún. kazettákba vannak szerelve, melyek a szűrletgyűjtő vezetékre vannak csatlakoztatva. Az átszívást a membránon keresztül, szivattyú

végzi. Szűréskor tehát a nyersvíz befolyik a folyamati tartályba, ahonnét a memránkazettákon keresztül a szivattyú szívja el a tisztított vizet. (A periodikus visszamosások alatt a víz előre meghatározott százaléka a tartályból túlfolyik, biztosítva így a tartályban feldúsuló lebegőanyag rendszeres dekoncentrálását. A lebegőanyag eltávolítása membránszálakról, a membránkazetták levegőztetésével fúvó segítségével és a kazetták szűrt vízzel történő szivattyús visszamosással lehetséges.) [15]

A rendszer másik fontos technológiája: a fordított ozmózisos technológia (RO, azaz reverz ozmózis), mely a természetes ozmózis folyamat megfordítása nyomás hatására. E folyamat során az oldószer a töményebb oldat felől a hígabb oldat irányába áramlik a féligáteresztő membránon keresztül. A berendezés nagynyomású szivattyúja az előkezelt nyersvizet magas nyomáson szivattyúzza a fordított ozmózisú membránokra. A membránok szétválasztják a folyadék áramot egy tisztított termékvíz áramra és egy koncentrált áramra, mely utóbbiban vannak a nyersvízáramból származó ásványi sók, baktériumok stb. A membránok tisztítása a fúvó bekapcsolásával, a membrán levegőztető elemeken keresztül, vegyszeradagolással történik. A kis vegyszerfelhasználás és a környezetbarát, biológiailag bontható vegyszerek alkalmazásával, az egyes tisztítási fázisoknál, a környezeti terhelés minimális. [16]

Lényegében a víztisztítás tehát egy kétfázisú membrán-technológia alkalmazásával történik: egy fizikai szűrés ultra/nano membránnal (UF) az alakos elemek eltávolítására, majd pedig egy teljes sótalanítás történik reverz ozmózis (RO) membránon az oldott anyagok eltávolítására. Az így megtisztított víz azonban így nem tartalmazza az emberi szervet számára szükséges ásványi anyagokat. A tisztítási folyamatok után így egy visszasózást is kell alkalmazni. Ugyanis nem mindegy, hogy a vízpótlás kapcsán milyen elektrolitokkal, ásványi anyagokkal rendelkezik a fogyasztásra szánt víz. Az elektrolitok pótlása közül nélkülözhetetlen a nátrium, kalcium, kálium, magnézium és a klorid. Fontos tényező, hogy a rehidratáláshoz hasznát folyadék íze is megfelelő legyen. [17]

A vízellátó rendszerhez mobil csomagoló berendezés is csatlakoztatható. A berendezés feladata a kapott nyers ivóvíz adagolása, csomagolása és tartósítása. A berendezés 1500l/h névleges kapacitású, mely így képes naponta 18 000 liter vizet csomagolni műanyag zacskóba. Kompakt konténeres kivitelben készül, a gépkocsira könnyen felszerelhető zártfelépítménybe telepítve. A csomagolással egy időben megtörténik a víz és a csomagoló anyag tartós fertőtlenítése is UV lámpával, illetve NaOCl oldattal. Az ivóvíz légmentes fóliazacskókba kerül és így már fogyasztható az előállított víz. [18]

Ezt a mobil, a honvédség számára legyártott vízellátó és csomagoló rendszert közegészségügyi szempontból az Országos Tisztiorvosi Hivatal engedélyezte az Országos Környezetegészségügyi Intézet szakvéleményezése alapján. A rendszer műszaki szempontú engedélyezésével kapcsolatos vizsgálatokat pedig a VITUKI Kht. végezte el. A vizsgálatok a rendszer üzembe-helyezési, üzemeltetési, visszaöblítési és fertőtlenítési vizsgálataira oszlott. A vizsgálatok természetesen az előállított vizek minőségét voltak hivatottak ellenőrizni. A vizsgálatok a teljes berendezés emberi használatra szánt vízzel érintkező szerkezeti elemeire, a membránokra a visszasózásra használt vegyszerekre irányultak elsősorban. A vízminőségi vizsgálatok a nyersvízből, a közbenső technológiai vízáramokból (az ultraszűrt vízből és a RO-nyersvízből), továbbá a termékvizekből (RO termékvízből, megszakító tartály utáni vízből és a zacskózott vízből) lettek ellenőrizve. Laboratóriumi körülmények között mikrobiológiai szempontból: Heterotróf összcsíraszám meghatározása 22 ºC-on, 37 ºC-on, Coliform szám, Escherichia coli, Pseudomonas aeruginosa és Fekáliás Enterococcus meghatározása történt. A mikroszkópos vizsgálatok elsősorban az üledék mennyiségére, az üledék minőségére, a véglényekre, a férgekre, a gombákra, a vas – mangán baktériumokra, a kénbaktériumokra, az algákra és cianobaktériumokra vonatkoztak. A kémiai vizsgálatok közül pedig főleg a szín, a pH, az elektromos fajlagos vezetőképesség, a lúgosság, az összkeménység és az összes szerves anyagtartalom vizsgálatai voltak a mérvadóak.

Bár a vízellátó rendszer- és a csomagoló berendezés automata-működtetésű, azért az ellenőrzését, kezelését csak betanított, szakképzett emberek használhatják. A tábori vízellátó állomás szakirányú képzettséggel rendelkező műszaki vezető irányításával működtethető. Az üzemeltetőnek ugyanis a termelt víz minőségének ellenőrzésére rendszeres önellenőrző mikrobiológiai, kémiai ill. mikroszkópos vízvizsgálatokat kell végeznie közegészségügyi szempontból, melyet a rendszer működési szabályzata is rögzít. Az ellenőrzéshez elsősorban mobil, könnyen kezelhető műszereket és eszközöket használnak. Az előírt vízminőség ellenőrzésekre azért is szükség van, mert a vízelőállító rendszerek kihasználtsága véges, továbbá a rendszerek tisztítására használatos vegyszerek is okoznak rosszabb vízminőséget. Továbbá a fertőzésveszély megakadályozása végett szükségesek a rutin minőségi ellenőrzések.

A tisztított víz azonban a szállítás során is szennyeződhet. Ennek megakadályozása érdekében pedig a logisztikai parancsnokság egy csoportja koordinálja a vízellátást, amely során mind az előállító, mind a szállító minőségi bevizsgáláson esik át, majd a vízellátó pont csak a bevizsgáláson átesett és ott megfelelt tehergépjárművek részére adhat ki vizet.

A haderőreform, a NATO-hoz való csatlakozás a képességek kialakítása, a létszám, a szervezet és a technikai eszközök korszerűsítése mellett elengedhetetlenné tette az új, korszerű hadviselésnek is megfelelő harcászati, hadműveleti elvek, eljárások kidolgozását is. A vízellátás területén azonban az együttműködésnek még nincs alternatívája. A vízellátás olyan összetett feladat, amely több szolgálati ág összehangolt munkáját jelenti. A magyar felajánlásban szereplő víztisztító kapacitás akkor eredményes és hatékony, ha kiegészül az egészségügy és a logisztika lehetőségeivel. A gyakorlatok azt bizonyították, hogy a feladat végrehajtható a többi érintett összehangolt munkájával (német egészségügyi hozzájárulás, francia vízszállítás és -elosztás), így megteremti a szövetségi rendszer keretén belül — vagy az ENSZ, NATO fennhatósága alatt megvalósuló többnemzetiségű katonai műveletekben — a hatékony együttműködést a katonai missziók vízellátása területén is. [19]

ZÁRSZÓ

A víz és elsősorban a tiszta víz nélkülözhetetlen az emberi élet számára. A száraz éghajlati területeken, ahol nehéz hozzájutni, szinte kincsnek számít. Mint kiderült, ezeken a területeken történő háborúk és harcok során is, komoly felkészülést és jó szervezetét és összehangolt munkát igényel, hogy biztosítsák az ott állomásozó csapatok és missziók vízellátását. A Magyar Honvédség pedig a víztisztító századának létrehozásával és a munkájának a felajánlásával minőségi hozzájárulást képes biztosítani a szövetségi erőknek, hogy az alapvető szükségletek biztosításával és kielégítésével lerakhassák a pszichológiában jól ismert Maslow piramis alapjait.

Irodalomjegyzék:

[1] Víz a bioszférában, a Szegedi Vízmű Zrt honlapjáról
https://www.szegedivizmu.hu/public/hu/vizrol_vizabioszferaban.html
(letöltés: 2011. 04. 07.)

[2] Földünk, a H2O Aqua Life honlapjáról
http://www.vitalhirek.hu/csaktisztaviz/foldunk/ (letöltés: 2011.04. 12.)

[3] A motiváció Maslow – féle szükségletelmélete, a Consultation Magazin honlapjáról
http://www.cons.hu/index.php?menu=cikk&id=20 (letöltés: 2011. 03. 30.)

[4] Nádorné Vörös Ibolya: Vízvédelem 3. modul
http://ittkesz.regiofokusz.hu/tananyagok/telepulesfejl/3_modul.pdf (letöltés: 2011. 04. 13.)

[5] Moser Miklós – Pálmai György: *A környezetvédelem alapjai: 5. Vízminőség – védelem.* Nemzeti Tankönyvkiadó, Budapest, 1999, 223-227.p. ISBN: 963 19 1854 8

[6] Had- és rendvédelem-história, kicsit másképp: A víz háborúja http://tiboru.postr.hu/a-viz-haboruja/ (letöltés: 2011. 03. 20.)

[7] Ivóvízhiány, a Wikipédia, a szabad enciklopédia honlapjáról http://hu.wikipedia.org/wiki/Iv%C3%B3v%C3%ADzhi%C3%A1ny (letöltés: 2011. 04. 01.)

[8] Dr. Kohut László: Extrém fizikai terhelésnek kitett katonai állomány keringési és élettani vizsgálata, Doktori (PhD) értekezés, ZMNE, 2008, Budapest

[9] [10] [11] Szabó Sándor: A műszaki támogatás cél- és feladatrendszerének változása http://193.224.76.4/download/konyvtar/digitgy/20012/eloadas/szabosa.html (letöltés: 2011. 04. 04.)

[12] [19] Jagadics Péter – Kállai Jenő – Padányi József: Magyar katonai víztisztítók a Zöld – foki – szigeteken http://www.regiment.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/magyar_katonai_viztisztitok (letöltés: 2011. 04. 01.)

[13] Mobil védelmi rendszerek, a Callmix Hungary Kft. honlapjáról http://www.callmix.hu/mobil_vedelmi_rendszerek.php (letöltés: 2011. 04. 05.)

[14] [15] [16] [17] [18] GE Water & Process Technologies Zenon Membrane Solutions: *Zenon Water for theword, Megvalósulási tervdokumentáció, Általános rész, Műszaki leírás*, Tatabánya, 2005. 05. 17

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kozák Attila
kozak24@freemail.hu

A HARMADIK VONALAS LÁNGLOVAG

Absztrakt

Publikációm választására azért került sor, mert a tűzoltóság hármas rendszere tűzmegelőzés-tűzoltás-tűzvizsgálat nem érvényesül, vagy alig érezhető. A jelenlegi országos vezetés elkezdte a harmadik vonal a tűzvizsgálat problémáját kezelni. E probléma elméleti és gyakorlati síkon is megoldást követel. A téma fontossága abból is lemérhető, hogy egyre több fórumon lehet aggályokat hallani a tűzvizsgálat alacsony színvonaláról. Publikációmba gondolatokat fogalmaztam a múltról-, jelenről-jövőről, hogy igen is milyen fontos terület a tűzoltóság harmadik területe a tűzvizsgálat. Fontos a tűzmegelőzésnek, melyből új jobb jogszabályokat lehet alkotni a társadalom érdekében, fontos a tűzoltási vonalnak, melyből a szakmai színvonalat lehet emelni és fontos a károsultnak és károsultaknak, hogy jogaikat törvényesen igazságosan érvényesíteni tudják. Remélem témaválasztásom jó gondolat ébresztőül szolgál a tűzvizsgálat szakmai színvonalának emeléséhez, de a megfelelő megoldások kidolgozása a központi szervek feladata.

This article has been written because the triple system of the fire service, in particular, fire prevention, fire extinction and fire investigation cannot or can hardly be observed. The current national leadership has started to deal with the problem of the third line, i.e. fire investigation. This problem needs a solution both in principle and in practice. The importance of this topic is also shown by the fact that anxiety about the low standard of fire investigation is expressed in more and more forums. My article discusses the past, the present and the future, too, stating that the third task of the fire service, i.e. fire investigation is essential. It is important for the fire prevention in order to make better legal provisions for the society; it is important for the fire extinction line in order to improve the professional standards; and it is important for the damaged persons to enforce their rights lawfully and fairly. I hope that my topic selected will be thought-provoking enough to improve the professional standard of fire investigation, but the elaboration of appropriate solutions will be the duty of central organs.

Kulcsszavak: *tűzvizsgálat, tűzvizsgáló, hatósági eljárás, illetékesség, keletkezési ok ~ fire investigation, fire investigator, official procedure, competence, cause of formation*

BEVEZETŐ

A tűzvédelem kezdetben a hagyományokon alapult, melyet felváltott az írásban rögzített tűzi rend.

E szabályzásokat követték a helyhatóságok által alkotott tűzszabály rendeletek, illetve az állami szervek által rögzített tűzrendészeti rendeletek, s végül az állami vezetés szintjén alkotott törvények, kormányrendeletek, miniszteri rendeletek, intézkedések.

Jelenleg hazánkban a tűzvédelmi törvény képzi a tűz elleni védekezés törvényi hátterét. Az intézkedések szükség szerint kötelező magatartásra kényszerítik az állampolgárokat, állami és társadalmi szervezeteket egyaránt.

Magyarországon elméletileg a tűzvédelmi törvényt hármas tagozódás jellemzi. Tűzmegelőzés, tűzoltás-műszakimentés, valamint a tűzvizsgálat.[1] E hármas tagozódás harmadik elemét szeretném írásomban megvizsgálni, rávilágítva arra, hogy miért harmadik vonalas lánglovag a tűzvizsgáló.

A TŰZVIZSGÁLAT, MINT MUNKATEVÉKENYSÉG

A tűzesetek vizsgálatára vonatkozó szabályokat jelenleg a 12/2007.(IV.25.) ÖTM rendelet szabályozza. A rendelet megfogalmazása szerint a tűzvizsgálat célja: „olyan tűzmegelőzési, tűzoltási beavatkozási tapasztalatok megszerzése, következtetések levonása, amelyek alkalmasak a tűzmegelőzési ismeretek bővítésére, a mentési beavatkozási feltételek javítására és hozzájárulnak a jogkövető magatartáshoz.”

A tűzvizsgálat során a tűzvizsgáló, a tűz keletkezésének, terjedésének körülményeit; a tűz keletkezésének helyét, idejét; a tűz keletkezésének ok-okozati összefüggéseit; továbbá a tűzesettel kapcsolatos személyi felelősséget, a tűz keletkezésének megelőzésére, továbbterjedésének megakadályozására vonatkozó tűzvédelmi előírások érvényesülését, a tűzmegelőzésre vonatkozó előírások érvényesülését, a tűzoltás alapvető feltételeinek meglétét vizsgálja.[2]

A területileg illetékes hivatásos önkormányzati tűzoltóság a bejelentett tűzesettel kapcsolatban az ügyfél kérelmére tűzeseti hatósági bizonyítványt ad ki. A tűzeseti hatósági bizonyítvány a tűzvizsgálati eljárás lefolytatásától függetlenül adható ki.

A kérelem tartalmazza: a kérelmező ügyfél vagy képviselőjének adatait, lakcímét/székhelyét, távközlési úton történő elérhetőségét, a tűz keletkezési helyét, idejét, valamint azt az indokot, amely miatt a hatósági bizonyítvány kiadását kezdeményezi.

A tűzeseti hatósági bizonyítvány a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény 83. §-ának (3) bekezdésében foglaltakon túl tartalmazza: a tűzjelzés idejét, a tűzeset helyét és idejét, tűzoltói beavatkozás történt-e, indult-e tűzvizsgálati eljárás, a tűzesetről rendelkezésre álló adatok közül azon adatokat, melyek a tűzeseti hatósági bizonyítvány felhasználása szempontjából szükségesek. A tűzeseti hatósági bizonyítvány kiadása megtagadható, ha a tűzeset megtörténtének ténye a helyszín megtekintése alapján nem állapítható meg.[3]

A TŰZVIZSGÁLÓ, MINT HARMADIK VONALAS LÁNGLOVAG?!

Ma Magyarországon nem érvényesül, vagy csak alig érezhető a tűzmegelőzés - tűzoltás-tűzvizsgálat összefüggő hármas rendszere.

Gyakorlatilag a tűzoltóságok két részre tagozódtak: tűzmegelőzési, valamint a tűzoltási-műszaki mentési szakterületre. A tűzvizsgálatnak jelenleg nincs önálló része a szervezeten belül.

Első lépésként a tűzmegelőzési szakterület szakemberei engedélyezik egy épület, vagy létesítmény használatbavételét. A második lépcsőfokot az jelenti, ha valamilyen oknál fogva tűz keletkezik és a tűzoltási vonal készenléti tűzoltói állománya, elvégzi a mentési, tűzoltási feladatokat.

A harmadik munkafázis során kerül az előtérbe a tűzvizsgáló, mint harmadik vonalas lánglovag. Az ő feladatai közül a legfontosabbakat a tűz keletkezési helyének pontos meghatározása és az ok-okozati összefüggések feltárása jelenti.

A tűzvizsgáló, hogy minél kisebb hibaszázalékkal és eredményesen dolgozzon, nagy felkészültséggel és kellő rutinnal kell (kellene) rendelkeznie.

A TŰZVIZSGÁLAT MÚLTJA

A tűzvizsgálat a rendszerváltás előtt jól működött. Készenléti szolgálati rendszerben látta el feladatait a tűzvizsgálói szolgálat, a vonulós tűzoltókhoz hasonlóan.

Ebben az időszakban az volt az előírás, hogy valamennyi bekövetkezett tűzesetnél el kellett végezni a tűzvizsgálatot, melynek dokumentálását és a statisztika pontos vezetését megkövetelte az akkori országos és megyei szakmai vezetés.

A múlt század utolsó évtizedében az a központi irányelv vált uralkodóvá, hogy a tűzvizsgálatot azok végezzék, akiknek bizonyos érdekei fűződnek hozzá. (pl.: a biztosítók). Ez az elképzelés azonban nem igazolta létjogosultságát, ezért a tűzvizsgálati tevékenység egy 1997-ben kiadott BM rendelettel visszakerült a tűzoltóságokhoz.

A köztes nyolc év alatt azonban megváltozott a tűzoltóságoknál is a szakmai háttér. A nagy gyakorlati tapasztalattal és kiváló szaktudással rendelkező kollégák nyugdíjba vonultak, nem volt meg az átmenetet képező középkorosztály.(Csak megjegyzésként: ez a folyamat súlyosan érintette és érinti ma is, a tűzoltóság másik két szakterületét is)

Így nem csoda, sőt előre prognosztizálható következmény volt, hogy a tűzvizsgálói munka színvonala a mélybe zuhant.

Az akkori szakmai felső vezetés nem gondolkozott azon, hogy a hatósági (tűzvizsgálati) feladatokat újra önálló résszé, harmadik vonallá tegye.

A TŰZVIZSGÁLAT MA MAGYARORSZÁGON

Napjainkban a tűzvizsgálatot végzők száma 700-1000 fő közé tehető. Feltételezem, hogy ennyi hozzáértő nagy tapasztalattal és rutinnal rendelkező kolléga jelenleg nincs a harmadik vonalban.

Ma ugyanúgy, mint régen a tűzvizsgálati tevékenységet bonyolult helyszíneken, alkalmanként társszervekkel közösen, a vonatkozó előírások maradéktalan betartásával kell elvégezni. Saját tapasztalataim szerint a jelenlegi képzés (két hetes tűzvizsgálói tanfolyam) nem teremt biztos alapot a jó munkához, a gyakorlati tapasztalat kevés és sok esetben a kijelölt szakemberek nem dönthetnek önállóan arról, hogy akarnak-e tűzvizsgálatot végezni.

Továbbá kérdéses az is, hogy a jelenlegi törvény (Ket) megfelel-e a tűzvizsgálati tevékenység szabályozására és eléri-e valódi célját.

Mielőtt bárkit megsértenék véleményemmel, tudom, hogy napjainkban is dolgoznak sorainkban nagy tapasztalattal rendelkező, lelkiismeretes munkát végző kollégák, akiknek nagy tapasztalatuk van a helyszínelésben, a szemle lefolytatásában, az ügyfél-tanú meghallgatásban, de nem kevés azon kollégák száma sem, akik a tűzesetek csekély száma miatt kevés tapasztalattal rendelkeznek.

A bizonyító erejű eljáráshoz ma kevés egy nyomtatvány csomag. Szükség lenne a jó technikai háttérre és technikusi tapasztalatra, jó megfigyelő képességre, helyzetfelismerésre is.

Szervezésileg is sok probléma van a jelenkori tűzvizsgálattal. A tűzvizsgálói feladat készenléti megszervezése parancsnokságonként változó. Jelenleg ez a tevékenység a hivatásos önkormányzati tűzoltóparancsnok feladatát képezi.

A legtöbb esetben a tűzmegelőzési osztály hivatásos állományú tagjai, valamint a 24/48 váltásos munkarendben dolgozó szolglatparancsnokok, vagy helyetteseik végzik a tűzvizsgálatot. Ma Magyarországon, egy helyen (Budapesten) végeznek főosztályi szintű tűzvizsgálatot.

Megítélésem szerint, ha a tűzmegelőzési előadó végzi a tűzvizsgálatot, akkor kevesebb szakhatósági munkát tud elvégezni, ha a készenléti szolgálatparancsnok, illetve helyettese feladata a tűzvizsgálat, akkor nem valószínű, hogy adott szolgálati napon le tudja zárni az ügyet. Különösen igaz ez, ha az eset bonyolult, vagy másokat is be kell vonni az eljárásba.

A tűzoltó parancsnokságoknak a jelenlegi normatív finanszírozási rendszerében nincs pénzügyi forrásuk külön ügyeleti osztályt biztosítani a „harmadik vonal" magas színvonalú munkájának biztosításához.

A korábbiakban már említést tettem a tűzvizsgálói szakképzésről. Ma a tűzoltó szakképzés területén a tűzvizsgálati témakörre csak néhány órában kerül sor. Az óraszám még az alapismeretek elsajátításához is kevés.

A BM Katasztrófavédelmi Oktatási Központ 2005-ben 60 órás tanfolyam keretében szervezte újjá a tűzvizsgálói képzést. E tanfolyam már jó kiindulási alapot jelent az elméleti ismeretek elsajátításához, azonban kevés a gyakorlati óraszám, melyet a féléves - saját parancsnokságon eltöltött - felkészülési idő próbál kompenzálni.

Tapasztalataim alapján az otthoni gyakorlati felkészülés a kevés vizsgálati cselekmény miatt nem ad kellő gyakorlati tudást. A záróvizsga egyedisége jó lehetőséget ad a vizsgáztatónak, hogy objektív képet kapjon a tűzvizsgálat jelenlegi helyzetéről.

ÖSSZEGZÉS

Ha hazánkban a tűzvizsgálat, mint harmadik vonal szakmai színvonalát emelni szeretnénk, bizonyos irányba lépéseket kell tenni.

A tűzvizsgálatot végzőkkel szemben támasztott elvárásokat pontosan meg kell határozni. Nem elég, hogy valakinek felsőfokú szakmai végzettsége van, ehhez társítani kellene a megfelelő szakmai szakképzettséget is. Így csökkenhet az általam említett 700-1000 fő vizsgálatot végzők köre.

Azoknak a tűzoltó szakembereknek, akik a tűz keletkezési okát vizsgálják, az eredményes munkavégzéshez szükségük van a tűz tulajdonságainak megismerésére a gyakorlati életben, valamint olyan tűzoltó szakirodalomra, melyben összegezve vannak a műszaki, jogi, eljárás ismeretek. A tűzvizsgálat igényes, sokrétű munkát igényel, melyhez párosulni kell a műszaki, jogi ismeret felhasználásának, s nem utolsó sorban az állandó önképzésnek. Ezen ismeretek birtokában alakulhat ki a sajátos látásmód, amit rutinnak nevezünk.

Amennyiben kisebb létszámmal, magasabb színvonalon végeznék a tűzvizsgálatot, a szakmai tapasztalatokat gyorsabban lehetne összegezni, melyből a tűzvédelem minden területe pozitív tapasztalatot szerezhetne.

A hatályban lévő rendeletek és jogszabályok lényegesen lecsökkentették a tűzvizsgálatok számát (lásd 1. sz. melléklet). Hazánkban országosan éves szinten alig több mint 1000 tűzvizsgálatot végeznek.

A 2. sz. melléklet táblázatából, mely a Szabolcs - Szatmár Bereg megyei adatokat tartalmazza, jól érzékelhető, hogy a vizsgálat lefolytatását a tűzesetek több mint 50%-ában bűncselekmény gyanúja miatt kellett végezni. A gyakorlati tapasztalatok azt mutatják, hogy szakmai okból lényegesen több vizsgálatra lenne szükség, mely a tűzvizsgálatot tökéletesítené.

Megfogalmazódik az a gondolat, hogy szükséges egy tűzvizsgálói osztály, mely megyei szinten vizsgálná tüzeket. A hatékonyság érdekében a tűzvizsgálónak készenlétben kellene lenni, így a hatósági eljárást a tűzoltói beavatkozással szinte egy időben lehetne megkezdeni és az eredményességet javítaná a közvetlen segítség, melyet a beavatkozó tűzoltóktól kaphatna közvetlenül. Ehhez a felálláshoz legalább két fő kell, egy vizsgáló és egy technikus, valamint a beavatkozó egység parancsnoka.

Az ma még kérdés, hogy lesz-e újra önálló harmadik vonalas lánglovag és újjászerveződik-e a tűzvizsgálói osztály, mely képes lenne a magas színvonalon készített vizsgálati anyagokat, tanulmányokat összefogni, hasznosítani.

Felhasznált irodalom

[1] 1996. évi XXXI. Törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról.

[2] 12/2007.(IV.25.) ÖTM rendelet a tűzesetek vizsgálatára vonatkozó szabályokról

[3] Bartha Iván, Fentor László: *A tűzvizsgálat alapjai*

- A tűzvédelmi hatósági feladatokat ellátó szervezetekről és a tűzvédelmi hatósági tevékenység részletes szabályairól szóló 261/2009.(XI.26.) Korm. Rendelet
- Az Országos Tűzvédelmi Szabályzat kiadásáról szóló 9/2008. (II.22.) ÖTM rendelet vonatkozó fejezetei

1. számú melléklet

S.sz.	Megye	Tűzvizsgálatok száma	
		2009. év	2010. év
1.	Bács-Kiskun	105	87
2.	Baranya	51	42
3.	Békés	37	46
4.	Borsod-Abaúj-Zemplén	55	71
5.	Budapest	182	180
6.	Csongrád	56	30
7.	Fejér	17	21
8.	Győr-Moson-Sopron	50	31
9.	Hajdú-Bihar	48	49
10.	Heves	50	39
11.	Jász-Nagykun-Szolnok	50	66
12.	Komárom-Esztergom	38	39
13.	Nógrád	21	15
14.	Pest	148	140
15.	Somogy	35	30
16.	Szabolcs-Szatmár-Bereg	53	42
17.	Tolna	22	21
18.	Vas	29	33
19.	Veszprém	26	36
20.	Zala	50	37
Mindösszesen:		1123	1051

Tűzvizsgálatok száma: 2009. - 2010.
(országos adatok)
forrás: http://kit.katved.gov.hu/kap/

2. számú melléklet

Tűzoltóság (HÖT)	Fehérgyarmat	Mátészalka	Záhony	Kisvárda	Nyíregyháza	Nyírbátor	Vásárosnamény
Bűncselekmény gyanúja miatt:	4	3	2	4	9	4	2
Haláleset miatt:	1	-	-	-	1	-	-
Tűzeset minősített riasztási fokozata miatt:	1	-	-	2	3	4	2
Szakmai vagy egyéb okból:	-	-	-	-	2	1	-
Tűzoltó 8 napon túl gyógyuló sérülést szenvedett:	-	-	-	-	-	-	-
Tömegtartózkodás ú épületben történt a tűzeset:	-	-	-	-	-	-	-
Nem működött tűzvédelmi rendszer, berendezés	-	-	-	-	-	-	-
Becsült kárérték meghaladhatja a 100 millió forintot:	-	-	-	-	-	-	-

2010-ben megindított tűzvizsgálatok okai
(Szabolcs-Szatmár-Bereg megye)
Forrás: http://kit.katved.gov.hu/kap/

3. számú melléklet

Tűzoltóság (HÖT)	Fehérgyarmat	Mátészalka	Záhony	Kisvárda	Nyíregyháza	Nyírbátor	Vásárosnamény
A HÖT illetékességi területén 2010. dec. 03. – 2011 jan. 31. között megindított tűzvizsgálatok száma:	2	1	-	1	4	3	2
Kizárások száma az illetékességi területen 2010. dec. 03. – 2011. jan. 31. között megindított tűzvizsgálatokból:	2	1	-	1	3	2	2

Kizárás vizsgálata
forrás: http://kit.katved.gov.hu/kap/

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Laczik Balázs
balazs.laczik@gmail.com

A KRITIKUS INFRASTRUKTÚRA VÉDELEM ELVEINEK, CÉLJAINAK ÉS A VESZÉLYES IPARI ÜZEMEK BIZTONSÁGÁNAK ÖSSZEFÜGGÉSEI, KAPCSOLATUK

Absztrakt

Napjainkban a védelmi szakemberek egyre nagyobb figyelmet fordítanak a kritikus infrastruktúra rendszerek sérülékenységeinek vizsgálatára és a veszélyes ipari tevékenység környezeti hatásainak elemzésére. Ebben a cikkben arra vállalkozom, hogy rendszerezzem a kritikus infrastruktúra területein és ágazatain belül azok működésére, biztonságára kiható ipari létesítmények helyét és szerepét, továbbá feltárom, hogy az ipari létesítmények biztonságos üzemeltetésének elmulasztása milyen hatással lehet a kritikus infrastruktúra rendszerek működésére. Megvizsgálom a kritikus infrastruktúra védelmének és az ipari biztonság lehetséges kapcsolatait és következtetéseket vonok le ezek összefüggéseire, kölcsönhatásaira.

The defensive specialists translate increasingly bigger attention in our suns for the critical infrastructure onto the examination of the sensibilities of systems and the analysis of the environmental effects of the dangerous industrial activity. I undertake that I should systematize it inside the areas of the critical infrastructure and his sections in this article they his function, the place of industrial establishments influencing his safety and his role. I reveal what kind of effect the critical infrastructure may be the omission of the industrial establishments safe operation furthermore onto the function of systems. I examine it for the protection of the critical infrastructure and the possible contacts of the industrial safety and I draw the conclusions of this contexts, and interactions.

Kulcsszavak: *kritikus infrastruktúra, ipari biztonság, ~ critical infrastructura, dangereous industrial activity*

BEVEZETÉS

A gyakorlatban egyre több olyan baleset történik, melyek hatással vannak a kritikus infrastruktúrákra és kihatnak a káreseménnyel közvetlenül nem érintett területekre is. Veszprém megyében 2010. október 4-én a MAL Zrt. zagytározójának gátja átszakadt, ennek következtében több települést elöntött 700 ezer köbméter vörösiszap. Az iszappal elöntött területekről ki kellett költöztetni a lakosságot, az elektromos ellátás megszűnt, az utak járhatatlanná váltak és hatalmas környezeti károk jelentkeztek. 2009. február 8-án éjszaka Veszprém megyében a rendkívüli viharok és különösen intenzív havazások következtében másnap virradóra 20 ezer háztartás maradt elektromos áram nélkül. Az utak a hó-átfúvások miatt járhatatlanná váltak, több települést nem lehetett megközelíteni, a vasúti közlekedés is akadozott. Mindkét esetben a környékbeli infrastruktúrák (elektromos ellátás, úthálózat stb.) használhatatlanná váltak, az ipari katasztrófa és a szélsőséges időjárás hatásai következtében zavar keletkezett a lakosság ellátásában. Ezek az események felvetették bennem a gondolatot, hogy a kritikus infrastruktúrák védelme és az ipari létesítmények biztonsága áll-e valamilyen kapcsolatban? Egy ipari létesítménynél (ha az kritikus infrastruktúra elem) hogy valósul meg a biztonság, külön választható-e az ipari biztonság és a kritikus infrastruktúra védelme? Az ipari létesítmény biztonsága milyen módon szolgálja a kritikus infrastruktúrák védelmét és az infrastruktúra védelme hatással van-e az egyes üzemek biztonságára? Ezek a kérdések motiváltak, ezekre keresem a választ a cikkben.

AZ INFRASTRUKTÚRA ÉS A KRITIKUS INFRASTRUKTÚRA VÉDELMÉNEK FOGALMA, ALAPVETŐ JELLEMZŐI, VÉDELMÜK ELVEI ÉS MÓDSZEREI

A világban bekövetkezett katasztrófák, terrorista cselekmények, szerencsétlenségek rávilágítottak az infrastruktúrák sérülékenységére. Az Amerikai Egyesült Államokban jelent meg először, hogy az infrastruktúrákat fontosságuk szerint rangsorolták. Egyes területeit kiemelték, ezeket kritikus infrastruktúráknak nevezték. Ezek az infrastruktúrák különösen fontosak az adott ország, nemzet, társadalom működése szempontjából. A kritikus infrastruktúrákat védeni kell a káros hatásoktól, ezért kerültek kidolgozásra a kritikus infrastruktúra védelmi elvei és módszerei. A világon szinte minden állam, vagy államokat tömörítő szövetség kidolgozta a saját kritikus infrastruktúra védelmi elveit.

Az infrastruktúra fogalma, értelmezése, jellemzése

Ha rendszer szempontjából közelítem, az infrastruktúra alaprendszer, ennek része a kritikus infrastruktúra ezért először az infrastruktúra fogalmából kell kiindulni. Kutatásaim során több fogalommal, értelmezéssel találkoztam. Ugyanakkor egy minden területet átölelő és könnyen értelmezhető fogalom szükséges.

- A Magyar Értelmező Kéziszótár az infrastruktúra alatt érti: „a társadalmi, *gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.”*.[1]
- Haig Zsolt és Várhegyi István által készített jegyzet alapján: „egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és

[1] Magyar Értelmező Kéziszótár, Akadémia kiadó Budapest, 1978/2003. 609. p.

berendezések összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és az azokat működtetni tudó szakszemélyzetből áll.”.[2]

A Magyar Értelmező Kéziszótár által megadott definíció lefedi a mindennapi életben használt és értelmezett területet. A fogalomból jól kitűnik, hogy az infrastruktúrák alapvető hatással vannak egy ország életére, jelen vannak a társadalomban és a gazdaságban. A Haig Zsolt és Várhegyi István által alkotott fogalom az emberi tényezőt is figyelembe veszi, ez az értelmezés tágabb, mint a Magyar Értelmező Kéziszótár ad meg. Az infrastruktúrákat sokféleképp lehet csoportosítani, alapvetően azonban elválaszthatóak a lakossági igényeket kiszolgáló és külön az ipari termelést kiszolgáló infrastruktúrák. A lakossági igények szerényebb méreteket öltenek, az ipart kiszolgáló infrastruktúrák szoros kapcsolatban állnak az ipari létesítményekkel, kölcsönhatással vannak egymásra. Azonban, a lakossági és az ipart kiszolgáló infrastruktúrák egymással is kapcsolatban állnak, például az ország gáz-ellátását szolgáló vezetékek egyaránt kiszolgálják a lakosságot és az ipart.

Az infrastruktúrák vizsgálata során jellemzők határozhatóak meg. A tulajdonságok egyaránt érvényesek minden infrastruktúrára. Ezeket az alábbiakban ismertetek:

- összefüggnek a gazdaság fejlődésével, alapvető hatással vannak rá ilyen, például úthálózatok kiépítettsége és minősége (teherbírás, szélesség stb.);
- lassan térülő beruházás, hasznuk más ágazatban jelentkezik és csak tőkeerős cégek képesek kivitelezni, hiszen egy üzemhez vezető elektromos hálózat közvetlenül hasznot nem hajt, azonban az üzem működése számára ez elengedhetetlen;
- az infrastruktúra hálózatok kiépítéséhez, fejlesztéséhez nagy erő és eszközigény szükséges, ezek kivitelezése óriási beruházásokat igényel, például Barátság kőolajvezeték;
- helyhez kötöttek: nem mozdíthatóak, egy úthálózatot nem lehet mobilizálni, mint egy ipari létesítményt;
- csak arra használhatóak, ami az alaprendeltetésük, például vízvezeték hálózaton nem lehet földgázt szállítani;
- magas fenntartási költséggel rendelkeznek: az egyes infrastruktúra hálózatok folyamatos használat miatt állandóan karban kell tartani, erre speciális háttér-szervezetet kell fenntartani (közútkezelők);
- kialakításuk hálózat-szerű, különböző területeket fog össze, ebből adódik, ha egy területen megsérülnek, annak hatása más területeket is érint (ivóvíz-hálózat);
- véges teljesítőképességük van, létesítésük során az adott terület jellemzőihez, igényeihez méretezik őket.

Az infrastruktúrák jellemzőire jó példa a 2003-as Kanadai – Amerikai áramszünet. 2003. augusztus 15-én Kanadában egy villamos erőmű belső informatikai rendszerében hiba keletkezett, ennek következtében az erőmű leállt. Az általa megtermelt teljesítmény kiesést a szomszédos erőműveknek kellett volna pótolni. Azon a területen található villamos hálózat, teljesítőképessége határán volt, a fogyasztói igények nem csökkentek, viszont a területre szánt elektromos áram mennyisége hirtelen lecsökkent. Emiatt, a kanadai erőművel kapcsolatban álló közeli erőművek felé egy olyan plusz teljesítmény-igény jelentkezett, melyet a már

[2] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi kiadó Budapest 2005. ISBN: 963-327-391-9 http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf. 2011.04.22

egyébként is teljesítőképessége határán álló elektromos hálózat nem bírt el. Ezt követően az erőművek egymás után álltak le a hálózat túlterheltsége miatt. Az erőművek leállását követő áramszünet 20 millió embert érintett. A példa jól tükrözi, ha egy infrastruktúra hálózatot teljesítőképessége határán használnak, milyen következményekkel jár. A fentiek alapján érzékelhető még az ipari létesítmények (az erőművek) és az infrastruktúrák kapcsolata is.

A fentiekből látható, léteznek olyan infrastruktúra hálózatok, melyek kiesése komoly gondot okoz a lakosság mindennapi életében (pl.: áramszünet esetén zavar keletkezhet az információs hálózatokban, befolyásolja a kötött pályás közlekedést, üzemekben a termelést stb.) ennek következtében gazdasági következmények is fellépnek (termelési hiány). A védelmi szakemberek összeállították azoknak az infrastruktúráknak a listáját, amelyek kiesése, sérülése komoly gondot okozhat a lakosság mindennapi életében és az ország működésében. Ezeket kritikus infrastruktúraként kezelik. A következőkben megvizsgálom a kritikus infrastruktúra fogalmát és értelmezését.

A kritikus infrastruktúra fogalma, értelmezése

A terrorizmus különös veszéllyel jár, hiszen a világban manapság számos ilyen cselekménnyel találkozhatunk. A terrorista cselekmények mindig jelentős rongálást eredményeznek, például a vonatrobbantások, a World Trade Center elleni támadás stb. Az ilyen esetek miatt az infrastruktúrák közül ki kell emelni azokat, melyek *kiesése esetén az ország működésében vagy a társadalom mindennapi életében jelentős zavar léphet fel*, *ezek kritikus infrastruktúraként* jelennek meg. Az Amerikai – Kanadai áramszünet példájában nem az erőmű saját informatikai hálózatát kell kiemelni az infrastruktúrák közül, hanem az egész villamos-energia ellátást. Gazdasági szempontból nem ideális, ha minden elemet maximális védelemmel látnánk el. A kritikus infrastruktúrák bizonyos elemeit is ellátják a lehető legmagasabb szintű védelemmel, nyilván vannak azonban olyan infrastruktúra elemek, melyek védelme nincs számottevő hatással a teljes rendszer védelmére. Természetesen az is cél, hogy az egyes elemek működése biztosított legyen, azonban mérlegelni kell a védekezés gazdasági vonzatait és az azzal elért előnyök arányát. A cél elsősorban az, hogy a teljes rendszer működőképessége fennálljon akkor is, ha egyes elemei kiesnek.

Az előbbieket szem előtt tartva jelent meg a kritikus infrastruktúra fogalma először 1998-ban az USA-ban. Azóta számos ország és olyan országokat tömörítő szövetség, mint a NATO, az Európai Unió is alkalmazza. Jelen esetben három fogalmat emelek ki, amelyeket fontosnak tartottam. Kiválasztottam az Európai Unió által használtat, illetve két magyarországi értelmezést. Az Uniót és az egyik hazai értelmezést jogszabály rögzítette, a másikat Dr. Kovács Ferenc ny. mk. ezredes definiálta doktori értekezésében.

- Az Európai Unió a kritikus infrastruktúra fogalmát a COM(2006) 786 sz. irányelvében vezette be: „kritikus infrastruktúra mindazon fizikai és információs technikai hálózatok, szolgáltatások, amelyek sérülése vagy elpusztulása esetén komoly gondot okoznak a lakosság közegészségügyi, közbiztonsági, gazdasági jóllétében vagy a kormányzat működésében a tagállamokon belül. A kritikus infrastruktúrák kereszteződnek a gazdaságban, tartalmazzák az anyagi-, pénzügyi ellátást, szállítást, energia-hálózatokat, egészségügyi, élelmezési ellátást, kommunikációs rendszereket és a kormányzati szolgáltatásokat”.[3]

[3] http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf – 2006. 12. 12. Brüsszel, az Európai Tanács ülésén született COM(2006) 768. sz. irányelv 3. pontjában az eredeti angol megfogalmazás: „Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the member states. Critical infrastructures

- A magyarországi fogalom a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) Korm. határozat 1. sz. melléklet 3.2. pontjában került rögzítésre: *„Kritikus infrastruktúrák 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, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.”*.

- A kutatásaim során találtam meg, Dr. Kovács Ferenc ny. mk. ezredes megfogalmazását a kritikus infrastruktúrára vonatkozóan, mely szerint: *”a nemzeti, szövetségi és uniós infrastruktúra azon létfontosságú elemei, melyek jelentős károsodása, üzemzavara vagy megsemmisülése súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére.”*.[4]

A 2080/2008. Korm. határozat mellékletében meghatározott fogalom mindenre kitér, túlságosan hosszú és nehezen értelmezhető. A Dr. Kovács Ferenc ny. mk. ezredes megfogalmazása tömör, lényegre törő, tartalmilag megfelel a jogszabály által használt definíciónak.

Az kritikus infrastruktúrák kiválasztásának oka, hogy az egyes infrastruktúrákat védeni kell annak érdekében, hogy az emberi életben és anyagi javakban súlyos kár ne következzen be. A kiválasztás alapját az infrastruktúra kiesésének következményei adják. Ez az ún. következmény-alapú kiválasztás szempontjai megtalálhatóak a 2080/2008. Korm. határozat 1. sz. melléklet 3.2. pontjában. A következmények az alábbi kategóriák alapján elemezhetőek:

- Egy infrastruktúra kiesése mindig érint egy fizikailag jól definiálható területet. A kiterjedés lehet nemzetközi, nemzeti, regionális szintű.

- A súlyosságot az alapján lehet értékelni, hogy milyen hatással van az adott területre. A hatás mértékét az alábbiakra lehet osztani: nincs hatás, minimális, mérsékelt vagy jelentős. Hatás érheti az alábbi területeket: társadalom, környezet, gazdaság, politika, közegészségügy, pszichológia.

- Az idő fontos tényező egy infrastruktúra kiesésénél, ennek vizsgálata során mérlegelésre kerül, hogy a kiesett infrastruktúra hatása mikor éri el a jelentős súlyosságot. Ezért az időbeli tényezőt is figyelembe kell venni a következmények értékelésénél.

---

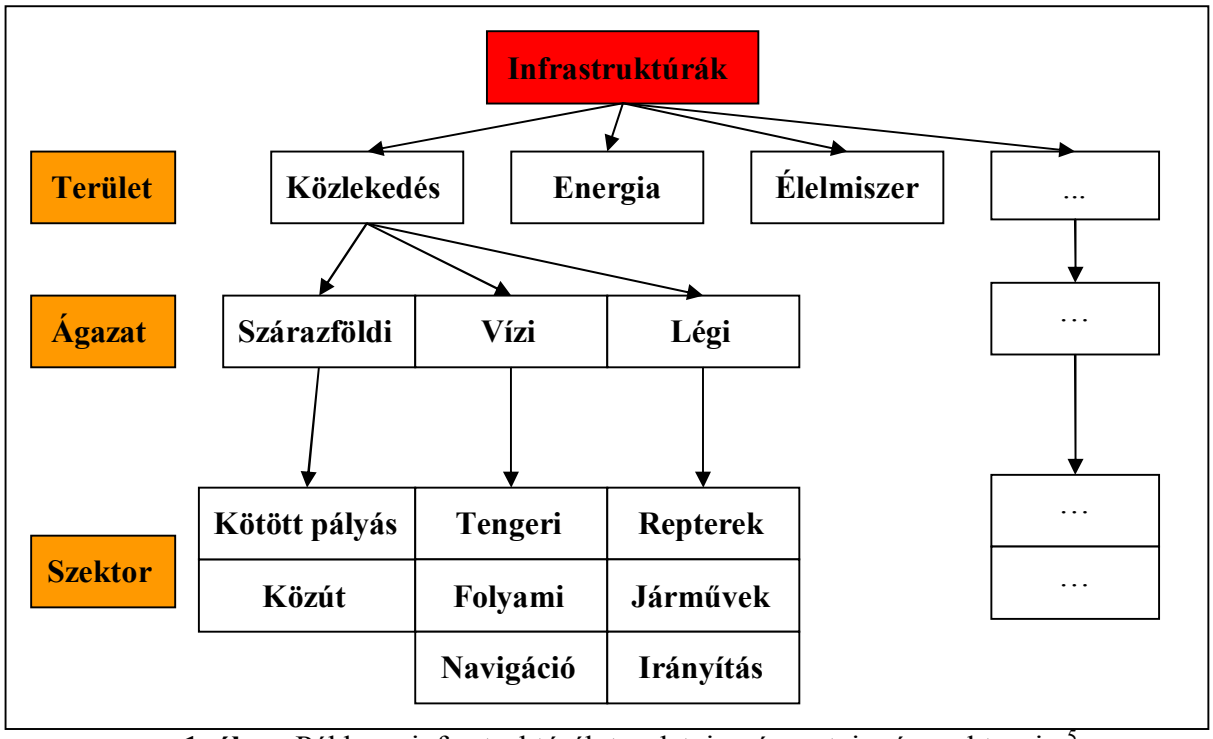
extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.”

[4] Dr. Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. 2005. október. Tanulmány. 7. oldal. GM Könyvtár.

A kritikus infrastruktúrákat kiválasztásukat követően osztályozni és rendszerezni kell. A következmény alapú csoportosításhoz mindenképpen szükséges a rendszer-szemléletű osztályozás, ami alapot nyújt a vizsgálatokhoz. A következőkben megvizsgálom, milyen módon lehet az infrastruktúrákat rendszerezni és felosztani.

A kritikus infrastruktúrák területei, ágazatai, szektorai

Az infrastruktúrákat a könnyebb kezelhetőség miatt részegységekre kell bontani. Az 1. sz. ábrán látható, hogy az infrastruktúrákat milyen egységekre lehet bontani. Az infrastruktúrákat területekre lehet osztani, a területeken belül találhatóak az egyes ágazatok majd az ágazatokon belül a speciális részegységek a szektorok.



1. ábra. Példa az infrastruktúrák területeire, ágazataira és szektoraira[5]

Az Európai Unió iránymutatása alapján minden tagország kidolgozta a saját országában az infrastruktúrák felosztását és elvégezte az előzetes vizsgálatokat, arra vonatkozóan mely infrastruktúrákat kell kiemelni. Magyarországon a 2080/2008. (VI. 30.) Korm. határozat 1. mellékletében előzetes felmérések alapján határozták meg azokat az ágazatokat, melyek kritikus infrastruktúraként lehet figyelembe venni. A jogszabály csak területeket és ágazatokat határoz meg, a szektorokra történő bontás és kidolgozás az ágazati minisztériumok felelőssége. A jogszabály mellékletében meghatározott területek és ágazatok az alábbiak:

- Energia: energia ellátás, elosztás;
- Infokommunikációs rendszerek: vezetékes, mobil hálózatok, internet, műholdas rendszerek, kormányzati információs rendszerek;
- Közlekedés: közúti, vasúti, légi, vízi közlekedés, logisztikai központok;
- Pénzügyi szektor: bank és hitelintézeti biztonság, fizetési, értékpapírklíring rendszerek;

[5] Saját ábra.

- Víz: ivóvíz, szennyvíz, árvízi védművek, felszíni és felszín alatti vizek védelme;
- Élelmiszer: élelmiszer előállítás, élelmiszer biztonság;
- Közegészségügy: kórházi ellátás, mentés irányítás, egészségügyi tartalékok és vérkészletek, biológiai laboratóriumok;
- Ipar: vegyi anyagok tárolása, előállítása, veszélyes hulladék-kezelés, nukleáris anyagok előállítása, tárolása, gyógyszergyártás;
- Jogrend – Kormányzat: közigazgatási szolgáltatások, igazságszolgáltatás, kormányzati létesítmények, eszközök;
- Közbiztonság – védelem: honvédelem, rendvédelmi szervek infrastruktúrái.

Az 1. sz. táblázat szemlélteti a különbségeket az országonként eltérő egyes kritikus infrastruktúra ágazatok, szektorok között. A táblázatban az egyes területeket ágazatokra és szektorokra kellett szétbontani. Ennek célja, a jobb megközelíthetőség és a könnyebb értelmezhetőség. A területeket ágazatokra lehet szétválasztani, az ágazatokon belül pedig szektorokat különböztetünk meg (például: Közbiztonság – védelem *terület*éből a rendvédelem *ágazat*a és a rendvédelem ágazatából külön kiemelhető a katasztrófavédelem *szektor*a).

KI. terület	Ágazat	Szektor	USA	Nagy Britannia	Magyarország
Energia	Energiatermelés Energia elosztás	Közművek			X
		Vízellátás	X	X	X
Élelmiszer	Élelmiszer előállítás Élelmiszer biztonság	Mezőgazdaság	X		
		Élelmiszeripar	X	X	X
		Élelmiszer ellátás	X	X	X
Közlekedés	Szárazföldi Vízi Légi	Közút, vasút		X	X
		Tengeri, Folyami		X	X
		Repterek, navigáció		X	X
Jogrend, gazdaság	Közigazgatás	Hivatalok		X	
	Pénzügy	Bank szektor	X	X	X
	Kormányzat	Kormányzati létesítmények, eszközök	X		
Közbiztonság - védelem	Védelmi szervezetek	Katasztrófavédelem		X	X
		Terror, ABV elleni védelem		X	
		Honvédelem		X	X
	Védelmi ipar	Eszközök, felszerelések	X		
Ipar	Vegyi ipar	Vegyi anyagok előállítása, feldolgozása	X		
	Nukleáris ipar	Radioaktív anyagok előállítása, feldolgozása	X		

Információs rendszerek	Civil információs hálózatok	Telefonhálózatok	X	X	X
		Internet hálózat	X	X	X
		Egyéb (rádió, televízió)	X	X	X
	Kormányzati, védett infokommunikációs rendszerek	Belső informatikai hálózatok, műholdas rendszerek	X	X	X
Víz	Lakossági víz	Ivóvíz	X	X	X
		Szennyvíz	X	X	X
	Természetes vizek	Felszíni vizek	X	X	X
		Felszín alatti vizek	X	X	X
	Ár és belvíz	Passzív árvízvédelmi eszközök (gátak, védművek)	X	X	X
		Aktív árvíz védelem (erők, eszközök)	X	X	X
Egészségügy	Helyhez kötött létesítmények	Kórházi ellátás	X	X	X
		Laboratóriumok	X	X	X
		Egészségügyi készletek	X	X	X
	Mentőerők	Mentőszolgálat	X	X	X
		Mentés irányítás	X	X	X

1. táblázat. A kritikus infrastruktúra ágazatai, szektorai egyes országokban (előzetes felméréseket is felhasználva)[6]

A táblázat és az előzetes felmérések alapján, Magyarországon az ipar teljes területe nem tartozik a kritikus infrastruktúrákhoz, azonban egyes szektorok vagy kapcsolatban állnak a kritikus infrastruktúrákkal vagy kritikus infrastruktúraként tartják számon. Például az ipar kötődhet az energia-termeléshez az erőműveken, illetve a katasztrófavédelemhez a veszélyes üzemeken, az élelmiszer-ellátáshoz az élelmiszeriparon keresztül.

Az infrastruktúrák közül kiemelt kritikus infrastruktúrákat védeni kell az azokat károsító hatásoktól. A következőkben megvizsgálom, a védekezést milyen elvek és módszerek alapján lehet végrehajtani.

A kritikus infrastruktúra védelmének elvei, módszerei

Az állampolgárok mindennapi életét és az ország működését szolgáló infrastruktúrák működésének biztosításához az infrastruktúrákat védeni kell a terrortámadásoktól, a szélsőséges időjárástól, már a létesítésnél komoly figyelmet kell szentelni a tervezésre és az infrastruktúra elem belső működésének stabilitására.

A védelmi elvek kidolgozása is országonként eltérő lehet, az Unió által kiadott alapelvekre építve minden ország kidolgozza a saját elveit. Én csak a magyarországi változatot mutatom be, a vizsgálat alapját a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) Kormány határozat 1. sz. melléklet 3.6. adta meg. A védelem

[6] Felhasználva: Dr. Kovács Ferenc ny. mk. ezredes – A Kritikus Infrastruktúra védelme I. c. tantárgy előadás vázlat 2008.03.04.; 2080/2008. (VI. 30.) Korm. határozat 1. sz. melléklet 3.3. pont.

kidolgozásához illetve a módszerek meghatározásához szükséges lefektetni a pilléreket nyújtó alapelveket. Ezek az alábbiak:

- *Felelősség megosztásának elve (szubszidiaritás):* egy infrastruktúra védelme elsődlegesen üzemeltetői és nemzeti hatáskörbe tartozik. A létesítmények védelme mindig a tulajdonosok illetve az üzemeltetők felelőssége, ők azok, akik a védelmet megszervezik, illetve döntéseket hoznak ennek érdekében. A Kormányzati szereplők elsődlegesen koordinálják az üzemeltetők tevékenységét, valamint lényeges hangsúlyt kell fektetni az ágazatok elemzésére és a szektorok közötti összhangra és kommunikációra.

- *Kiegészítő jelleg:* a védelem célja, nem egy teljesen önálló védelmi rendszer kialakítása, hanem a meglévő rendszerek olyan biztonsági intézkedésekkel történő kiegészítése, amely lehetővé teszi a kritikusinfrastruktúrák veszélyeztető tényezőinek kiküszöbölését.

- *Rugalmasság:* a kritikus infrastruktúrák védelme olyan folyamatos felülvizsgálatot igénylő program, amelyben igen nagy szerepet kap, az időben hosszan elnyúló kihívásokra való megfelelő szintű reagálás.

- *Arányosság:* a védekezési stratégiák, intézkedések minden esetben arányosak a fenyegetettség mértékével, ennek megválasztása különösen nagy odafigyelést igénylő feladat. A magyarországi rendszerek, eljárások nagy hátrányát jelentik az aránytalanul nagymértékű adminisztrációs tevékenységek, ezen eljárások során törekedni kell arra, hogy a lehető leggyorsabb, legegyszerűbb, leghatékonyabb és legkevesebb munkával járó adminisztrációt vezessük be.

- *Fenntarthatóság:* a védelemmel kapcsolatos intézkedések megfinanszírozása a közreműködő személyek felelőségi és érdekeltségi szintjéhez igazodik. Figyelembe kell venni a megállapított kockázati prioritásokat, a mindenkori veszély jellegét és meg kell vizsgálni a szereplők anyagi lehetőségeit. Sokszor felmerülő probléma az anyagi gond, ezek kiküszöböléséhez állami és uniós forrásokat kell biztosítani, illetve olyan partner-kapcsolatokat kiépíteni melyek együttműködésen alapuló védelmi rendszerek kialakítását teszik lehetővé.

- *Titkosság:* átfogó feladathalmaz, amely kihat mindenre. Vannak információk, melyeket védeni kell, ez annyit jelent, hogy ki kell jelölni azokat az információ köröket, csatornákat, amiken megjelennek a kritikus információ halmazok. Ezeknek a kezeléséhez biztosítani kell, egy olyan személyi és technikai, technológiai hátteret – és annak megfelelő kontrollálásához szükséges feltételeket –, melyek az adott információkat bizalmasan és minden gyanún felül állóan kezelik, alkalmazzák.

- *Széles körű védelem, kiemelve a terrorizmus elleni védekezést:* olyan rugalmas megközelítési mód, ami figyelembe vesz minden szándékos, illetve szándékosságból eredő vagy természeti veszélyeztető tényezőt, a szemlélet középpontjában azonban minden esetben a terrorizmus nyújtotta fenyegetettség kap helyet.

- *Horizontálisan egymással összefüggő és ágazati megkülönböztetés:* minden miniszter a saját ágazatáért felelős a kritikus infrastruktúrák védelmi programja által előírtak betartásáért, koordinálásáért. Amennyiben az ágazat állami tulajdonú, azaz a miniszternek az üzemeltetői, tulajdonosi jogviszonya áll fenn, így ebben az esetben ezeket a kötelezettségeket is vállalnia kell.

- *Együttműködés:* az egyes ágazatok közötti és az állami valamint a létesítmények vezetői közötti összehangolt munka a kritikus infrastruktúra védelmének érdekében.

A védelmi elvek összeillesztése és a módszerek összehangolása, hogy azok hatásai ne ütközzenek egymással.

A módszerekre hatással vannak az alapelvek, azoknak tükrözniük kell az elveket. A kritikus infrastruktúrák védelme során a módszereket több csoportra lehet osztani. Ezek az alábbiak:

- Műszaki megoldások, amelyek biztosítják a kifogástalan működést:
  - Hálózatok összekapcsolása: az egyes elemek összekapcsolásának köszönhetően a rendszer stabilitása növekszik, törekedni kell, hogy az egyes rendszerek között az átjárhatóság biztosított legyen, az egyik el tudja látni a másik feladatát és fordítva;
  - Biztonsági berendezések: vagyonvédelmi, biztonságtechnikai berendezések alkalmazása, melyek időben figyelmeztetnek az esetleges veszélyekre és szükség esetén megteszik a megfelelő beavatkozást;
  - Kiszolgáló berendezések működésének folyamatosságát garantáló megoldások: kettős betáplálás, tartalék információs hálózatok.
- Belső szabályzások:
  - Létesítmény belső utasításai, szabályzatai: a létesítmény vezetése által támasztott követelmények, szabályok;
  - Technológiai berendezések utasításai: gyártó által létrehozott szabályozások, melyek a berendezések helyes használatára, karbantartására vonatkoznak;
- Hatósági feladatok, felügyeleti szervek:
  - Jogszabályok: nemzetközi, szövetségi (uniós) vagy nemzeti előírások, melyek egy ország határain belül hatályosak;
  - Irányelvek: országokat tömörítő szervezetek (Unió, NATO) által alkotott szabályok, melyek a szövetségek tagállamaiban érvényesek;
  - Nemzetközi szerződések: országok között létrejött egyezségek.

A kritikus infrastruktúra védelmi elveket felhasználva lehet megvalósítani a konkrét műszaki megoldásokat és a védekezés célját szolgáló szervezeti kialakításokat és a hátteret adó jogszabályi környezetet. A konkrét műszaki megoldások, pedig alapvetően meghatározzák egy adott infrastruktúra védettségét. A következő fejezetben megvizsgálom az ipari biztonságot a kritikus infrastruktúra védelmének elemzése során alkalmazott szempontok alapján.

AZ IPAR, MINT A KRITIKUS INFRASTRUKTÚRA EGYIK ELEME ÉS AZ IPARI BIZTONSÁG FOGALMA, ÉRTELMEZÉSE, VÉDELMI ELVEI ÉS MÓDSZEREI

Az ipari üzemek, létesítmények számos olyan szolgáltatást nyújtanak, melyek kapcsolhatóak az infrastruktúrákhoz. Például egy aszfaltkeverő üzem kapcsolódik az úthálózatokhoz. Másik példa, az elektromos energia előállításához erőműveket kell üzemeltetni, ezek hatalmas ipari létesítmények és az általuk termelt szolgáltatás közvetlenül infrastruktúrához kapcsolható. Az utóbbi példából kiindulva, az energiatermelés és ellátás több országban tartozik a kritikus infrastruktúrákhoz, így Magyarországon is. Tehát az ipar, az ipari létesítményeknek hatása van az infrastruktúrákra. Ezeket a létesítményeket védeni kell, hiszen kiesésük közvetlenül érinti az infrastruktúrákat. Vannak olyan ipari komplexumok, melyek közvetlenül nem köthetőek infrastruktúrákhoz, azonban sérülésük esetén az infrastruktúra hálózatokban kár keletkezhet. Jó példa erre, a veszélyes anyagokat feldolgozó, előállító ipari létesítmények. Az előzőek alapján, az ipar a kritikus infrastruktúra egyik területe ellenben más területekkel és ágazatokkal is kapcsolatban áll. Látszik, hogy az ipari létesítmények működése, alapvető hatással lehet a lakosságra és a környezetre funkciójuktól függően. Az ipari biztonság megjelenik mind a veszélyes anyagokat feldolgozó üzemekben,

mind az egyszerű élelmiszer-ipari gyárakban. A következőkben megvizsgálom az ipari biztonságot.

Az ipari biztonság értelmezése

Az ipar-ágak és az ipari tevékenység védelme (az üzem környezetének védelme is) mindenhol ugyanazt kell, hogy jelentse: az üzem biztonságos működését, a dolgozók biztonságos munkavégzését és a technológia biztonságát. Az ipari üzemek meghibásodása katasztrófahelyzetet okozhat, a katasztrófavédelem Magyarországon kritikus infrastruktúraként szerepel, ez kapcsolati pont az ipari biztonság és a kritikus infrastruktúra között. A továbbiakban ezt veszem alapul az ipari biztonság vizsgálata során. Ebben a fejezetben kitérek az üzem fogalmára és az egyes üzemek csoportosítására, illetve értelmezem az ipari biztonság definícióját.

Az Európai Unió Tanácsának a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről szóló 96/82/EK irányelve szerint az üzem fogalma az alábbi:

> *„az üzemeltető irányítása alatt lévő terület egésze, ahol egy vagy több létesítményben veszélyes anyagok találhatók, beleértve a közös vagy kapcsolódó infrastruktúrát vagy tevékenységeket is;”*[7]

Ez a fogalom azonban szűken csak a veszélyes ipari üzemekre értelmezhető, az irányelv csak a saját céljának megfelelő fogalmat használ, általánosan ez nem alkalmazható, hiszen számos olyan üzem létezik, ahol veszélyes anyag nem található.

Mielőtt rátérek az ipari biztonságra, csoportosítom az üzemeket a könnyebb értelmezhetőség végett. Az üzemeket három nagy csoportra osztom:

- Ipari üzemek: mindaz a tevékenység, amely valamilyen piacképes terméket állít elő (nem szolgáltatást) pl.:
  - Tűz és robbanásveszélyes üzemek (olajfinomítók);
  - Veszélyes üzemek (vegyipar);
  - Fémipari üzemek (kohászat, gépgyártás).
- Mezőgazdasági üzemek azok üzemek, melyeknek köze van az állat és növénytermesztéshez és az ezzel kapcsolatosan előállított termékekhez pl.:
  - Élelmiszeripar;
  - Feldolgozó ipar.
- Egyéb üzemek: ide tartoznak azok az üzemek, melyek valamilyen szolgáltatást nyújtanak (pl. közmű szolgáltatók);
  - Energia-termelő üzemek (pl.: erőművek).

A csoportosításnál nem vettem külön az egyes csoportokhoz kapcsolódó, az azokat kiszolgáló ágazatokat, létesítményeket melyek ellátják nyersanyaggal az adott csoportba tartozó üzemeket (pl.: mezőgazdasági üzem, tejüzemhez tartozó gazdasági társulás).

Az ipari biztonságára fogalmat nem találtam, csak a veszélyes üzemekre. A biztonságot a veszély oldaláról kell megközelíteni, ebből kiindulva az ipari biztonság a saját megfogalmazásom szerint: *mindazon tervezési, szervezési és végrehajtási tevékenységek összességét jelenti, melyek az üzemek biztonságos működését és ezen keresztül az ipar biztonságát szolgálják*. A fogalom alatt értem, azokat a műszaki vagy szervezeti megoldásokat, előírásokat, melyeknek célja nem csak az üzemek termelőképességének megőrzése, hanem a dolgozók, a környékbeli lakosság és a környezet védelme is. Az egyes

[7] http://www.aquadocinter.hu/themes/VKI_hirek/EU_joganyag/31996L0082HU.pdf- – Az Európai Tanács 1996. december 9-i 96/82/EK irányelve a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről. 2011.03.22.

üzemek biztonságos működése pedig kihat az ipar biztonságára is. Az ipar biztonsága pedig kihat az azzal kapcsolatban álló létesítmények, szolgáltatást használók biztonságára is.

Az ipari biztonság kivitelezéséhez olyan alapelveket kell megválasztani, melyek felölelik azokat a módszereket és műszaki megoldásokat, melyek a biztonság javát szolgálják. A következőkben bemutatom ezeket az elveket és módszereket.

Az ipari biztonság megvalósításának elvei, módszerei

Az ipari biztonság védelmi elveinek rögzítése során számos tényezőt kell figyelembe venni. A védelmi elveknek le kell fednie a belső veszélyeztető tényezőkkel (balesetek, tüzek stb.) és a külső veszélyeztető tényezőkkel (szélsőséges időjárás, terror-támadások) szembeni védekezést.

Az ipari biztonság védelmi elvei az alábbiak:

- *Teljes körű védelem megvalósulása:* mindenféle veszéllyel szembeni védekezés, a teljes körű védelembe tartozik a tűzvédelem, vagyonvédelem stb.
- *Nyilvánosság, lakosság tájékoztatásának érvényesülése:* az üzemeknél fontos a korlátozott nyilvánosság biztosítása, a lakosság tájékoztatása a technológiában rejlő veszélyekről és az ezek kiküszöbölésére szolgáló intézkedésekről. Fontos, hogy a lakosság megismerje a környezetében található üzem veszélyeit és azokat az óvintézkedéseket, melyek a védelmüket szolgálják, valamint azokat az eszközöket melyek rendelkezésére állnak számukra egy baleset esetén.
- *Működőképesség megőrzése és fenntartása:* a profit-orientáltság miatt az ipari létesítmények vezetőségének fontos, hogy az üzem a termelőképességét megőrizze, és ne következzen be kiesés, ezért a teljes védelem e köré az alapelv köré csoportosul.
- *Biztonságos működés:* az üzem működése közben a működési hibák kockázatának csökkentése, a bekövetkezett hibák következményeinek minimalizálása, olyan technológiák alkalmazása melyek a lehető legstabilabbak és legveszélytelenebbek.

A fenti alapelveket figyelembe véve kell a módszereket kidolgozni és megvalósítani. A módszereknek markánsan tükrözniük kell az alapelveket. Ezek az alábbiak lehetnek:

- Az üzem biztonságos működésére vonatkozó konkrét műszaki megoldások:
  - Technológiai elemek duplikálása;
  - Működéshez szükséges feltételek biztosítása: raktár-készletek biztosítása, szünetmentes tápok stb.;
  - Biztonsági berendezések: tűzjelzők, vagyonvédelmi rendszerek.
- Üzemeltető által meghatározott előírások:
  - Minőségirányítási, minőségbiztosítási rendszerek;
  - Technológiai előírások;
  - Jogszabályi keretek között kiadott utasítások például munkavédelmi szabályzat, tűzvédelmi szabályzat.
- Egyéb előírások:
  - Nemzetközi és állami felügyeleti szervek által meghatározott követelmények, előírások stb.;
  - Gépek, berendezések üzemeltetési, karbantartási előírásai.

Az alapelvek és módszerek megismerését követően a lehetőség nyílik a pontos műszaki megoldások és előírások kidolgozására. Az előzőekben értelmeztem az ipari biztonságot, bemutattam az ipari biztonság alapelveit és módszereit. A következő fejezetben összegzem azokat a pontokat melyek jellemezhetik az ipar és a kritikus infrastruktúrák között kapcsolatot.

AZ IPARI TEVÉKENYSÉG ÉS A KRITIKUS INFRASTRUKTÚRA KÖZTI KAPCSOLAT FELTÁRÁSA, KÖVETKEZTETÉSEK LEVONÁSA

Magyarországon az ipar a kritikus infrastruktúrák között szerepel, de az ágazatain belül is megjelenik, mint például az energia-ellátás. A kritikus infrastruktúra ágazatok között is megjelennek az ipar egyes területei például az energia szektor. Vannak az ipari tevékenységnek olyan területei melyek veszélyességüknél fogva szerepelniük kellene a kritikus infrastruktúra elemek között mert azok sérülései hatással lehetnek a környezetre és a lakosság ellátására. Ilyenek például a veszélyes ipari üzemek melyek önmagukban nem kritikus infrastruktúra elemek, de sérülésük előidézhet katasztrófákat. A katasztrófavédelem a hazai szempont-rendszerben pedig kritikus infrastruktúra ágazatként szerepel. Ebben az esetben nem csak a Seveso hatálya alá tartozó üzemeket és létesítményeket kell érteni, hanem minden olyan mennyiségű veszélyes anyagot felhasználó, feldolgozó üzemet, mely sérülése kiválthat katasztrófa-helyzetet.

Az energia-ellátás, mint a kritikus infrastruktúra ágazatának egy eleme több olyan létesítményt foglal magába, ahol kiemelkedő szerep jut az ipari biztonságnak. Ilyenek például a hőerőművek, mint ipari létesítmények, ezekre nem csak a kritikus infrastruktúra elemekre vonatkozó szabályok, hanem az ipari biztonság szabályai is érvényesek. Egy ilyen ipari létesítmény sérülése nem csak az adott területre jelent katasztrófát, hanem kihat az energiaellátásra, ami a kritikus elemek közé tartozik. Ezért az ipari biztonság egyik elsődleges feladata az ilyen üzemek zavartalan működésének biztosítása. Különösen fontos, hogy ezek az energiaellátás rendszerét képező létesítmények működése biztosítva legyen, mert ezek egymással hálózatot alkotnak és ilyenkor több országot összekötő infrastruktúráról beszélünk. A cikkben megállapítottam a kritikus infrastruktúrák és az ipari biztonság védelmi elvei hasonló területeket fednek le, egymással szorosan összefüggnek, annak ellenére, hogy belső tartalmuk bizonyos eltérést mutat. A vizsgálat alapján megállapítható, hogy az ipari létesítményekre vonatkozó biztonsági előírások, követelmények betartása elősegíti a kritikus infrastruktúra védelmi elveinek megvalósulását ugyanúgy, mint ahogy a kritikus infrastruktúra elemek védelmi elvei is visszahatnak az ipari létesítmények biztonságos üzemeltetésére. Ez az állítás jól igazolható a halmaz-elmélettel, mely kimondja, ha egy halmazt speciális tulajdonságokkal ruházok fel, az kihat a halmaz elemeire, ha a halmaz elemei rendelkeznek speciális tulajdonságokkal, az kihat a halmaz tulajdonságaira. Ha az ipari létesítmények működési oldaláról vizsgáljuk a kérdést a következők tapasztalhatók, egy ipari elem kiesése nem biztos, hogy gondot okoz a kritikus infrastruktúra teljes rendszerére vonatkozóan, de a helyi környezetre negatív hatással lehet. Ha viszont a teljes kritikus infrastruktúra rendszere sérül (pl.: Nyugat-európai áramkimaradás) nem csak helyi problémát okoz, hanem országrészek, régiók működését is befolyásolhatja. Ezért a kettőt együtt kell kezelni, egymástól nem célszerű őket elválasztani, de elsődleges és meghatározó szerepe a kritikus infrastruktúra hálózat működésének a védelme. A fentiek alapján megállapítható, hogy az ipari létesítmények biztonságos működése és a kritikus infrastruktúra rendszerek között szoros kapcsolat van, amelyet minden esetben az üzemeltetőnek és a védelmi szakembereknek is figyelembe kell venni.

Ebben a cikkben nem vizsgáltam meg teljes körűen, hogy az ipari tevékenység mely ágazatai azok, amelyek hatással vannak a kritikus infrastruktúra rendszerekre és milyen ipari biztonsági szabályzókkal lehetne ezek kapcsolatát hatékonyabbá tenni. Ezen vizsgálatok elvégzése után az összefüggések feltárását követően célszerű a védekezés megvalósításának rendjét kidolgozni. Véleményem szerint erre figyelemmel kell lenni, hiszen az ipari balesetek hatással vannak az infrastruktúrákra, illetve olyan hatásaik lehetnek, melyek egyeznek a kritikus infrastruktúrák sérülésének hatásaival. Célszerű lenne megvizsgálni azokat az ágazatokat, melyek hatással vannak a kritikus infrastruktúrákra, illetve kapcsolatban állnak

azokkal. Az ágazatok meghatározását követően, fontosnak tartom az összefüggések tükrében, megvizsgálni a védekezés gyakorlati megvalósításának rendjét. A biztonság és a védekezés hatékonyságának növelése érdekében nagyobb hangsúlyt kell fektetni a gyakorlatban mind az elvekre mind a konkrét megoldásokra az egymással való kölcsönhatások figyelembe vételével.

Irodalom jegyzék

http://www.aquadocinter.hu/themes/VKI_hirek/EU_joganyag/31996L0082HU.pdf – Az Európai Tanács 1996. december 9-i 96/82/EK irányelve a veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyeinek ellenőrzéséről.

Dr. Kovács Ferenc ny. mk. ezredes: A Kritikus Infrastruktúra védelme I. c. tantárgy előadás vázlat. 2008.03.04.

Dr. Kovács Ferenc: Az infrastruktúra kritikus elemeinek felmérése, védelmének és helyreállításának megszervezésére vonatkozó intézkedési javaslatok kidolgozása. 2005. október. Tanulmány. 7. oldal. GM Könyvtár.

http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf – 2006. 12. 12. Brüsszel, az Európai Tanács ülésén született COM(2006) 768. sz. irányelv.

Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi kiadó Budapest 2005. ISBN: 963-327-391-9 – http://www.cert-hungary.hu/sites/default/ files/news/ a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf.

Magyar Értelmező Kéziszótár, Akadémia kiadó Budapest, 1978/2003. 609. p.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Béres Deák Endre
bdendre@gmail.com

Szakál Béla
szakal.bela@ybl.szie.hu

MONITORING RENDSZER KIÉPÍTÉSE A KOCKÁZATOK CSÖKKENTÉSE ÉRDEKÉBEN SZÉNHIDROGÉN-TÁROLÓ TELEPHELYEKEN

Absztrakt

Rendszeresen előfordulnak olyan rendkívüli események, vagy technológiai üzemzavarok, amelyek akár súlyos balesetekké eszkalálódhatnak, és amelyek következményei a lakosságot súlyosan érintik. Van, amikor a számított kockázatok e kritériumok közelében vannak, vagy esetleg némileg meg is haladták azokat. Ekkor kockázatcsökkentő intézkedésekre van szükség. Ennek egyik legkézenfekvőbb megoldása a megfelelő vegyi monitoring és tájékozató rendszer kialakítása a veszélyes tevékenységet folytató vállalatok körül. A szerzők a cikkben a kőolaj- és földgázszármazékokat tároló objektumok területén kiépítendő Monitoring és tájékoztató rendszerek kiépítésre vonatkozó elvi elképzelést fejtenek ki.

In the meantime, technological breakdowns and serious accidents do happen regularly and their consequences can seriously affect civilians. In cases when the estimated risks grow near these criteria or slightly go beyond them, measures have to be taken to reduce these risks. Possibly the most obvious solution for meeting societal expectations are the creation of safety zones around these industrial sites. In this article the authors present the actual legal regulations and conceptual methods of establishing monitoring and information systems on territories where oil and gas products are stored
Kulcsszavak: veszélyes ipari üzemek, monitoring-tervezés, kockázatelemzés, lakosságvédelem ~ dangerous industrial companies, monitoring planning, population protection, risk analysis

Kulcsszavak: *kockázat, kockézat kezelés, szénhidrogén ~ risk, risk management, hydrocarbon*

BEVEZETŐ

A veszélyes anyagok előállítása, tárolása, felhasználása és forgalmazása szigorú jogi szabályokhoz kötött tevékenység, amely normák betartása nagymértékben hozzájárul veszélyes voltukból eredő kockázatok csökkentéséhez. A veszélyes tevékenységet folytató vállalkozásokkal szembeni minimális társadalmi elvárás az, hogy tevékenységükkel ne veszélyeztessék a lakosságot és a természeti környezetet. Ugyanakkor rendszeresen előfordulnak olyan rendkívüli események, vagy technológiai üzemzavarok, amelyek akár súlyos balesetekké eszkalálódhatnak, és amelyek következményei a lakosságot súlyosan érintik. A jelzett társadalmi elvárásnak való megfelelést szolgálja a vonatkozó jogi szabályozás, a Katasztrófa törvény és annak végrehajtási rendelete [1][2]. Itt az üzemeltető bizonyítja azt, hogy az általa folytatott tevékenység kockázatai kisebbek, mint a jelzett jogszabály engedélyezési kritériumai. Van, amikor a számított kockázatok e kritériumok közelében vannak, vagy esetleg némileg meg is haladták azokat. Ekkor kockázatcsökkentő intézkedésekre van szükség. Ennek egyik legkézenfekvőbb megoldása a megfelelő vegyi monitoring és tájékozató rendszer kialakítása a veszélyes tevékenységet folytató vállalatok körül. A szerzők a cikkben a kőolaj- és földgázszármazékokat tároló objektumok (a továbbiakban együtt: CH tárolóterek) területén kiépítendő Monitoring és tájékoztató rendszerek kiépítésre vonatkozó elvi elképzelést fejtenek ki. Bár e rendszert az iparág egyik legjelentősebb vállalata építi ki, a szerzők úgy gondolják, hogy a tervezési és kialakítási megoldások általánosíthatóak. Ezért a céget meg sem nevezve, általános tervezési-telepítési megoldásokról írják cikküket.

1. ábra. CH tárolótér súlyos balesete, (London, 2005. december 11.) [3]

CÉLOK

A jelzett monitoring és tájékoztató rendszer (a továbbiakban: SEVESO RENDSZER) egy komplex monitoring-tájékoztató-informatikai megoldás, amelynek fő feladata, hogy a CH tárolótereken magas szintű támogatást biztosítson a döntéshozóknak a katasztrófa megelőzés és elhárítás területén. Tehát az, hogy mérési adatokkal és információkkal segítse a döntéshozókat, felelős vezetőket. Tegye lehetővé a potenciális veszélyhelyzetek minél korábbi érzékelését, tényleges vészhelyzetben pedig az érintett lakosság és a területen dolgozó személyek informálását, riasztását. [4]

A fenti feladatok ellátásának érdekében véleményünk szerint a SEVESO RENDSZER -nek a következő funkcionális feladatokat kell ellátnia:

- Monitoring rendszer működtetése területén:
  - Gázkoncentráció mérése
  - Meteorológiai információk meghatározása
- Területi tájékoztatórendszer működtetése területén:
  - Hangosító rendszer működtetése
  - Figyelemfelhívó rendszer működtetése
- Informatikai rendszer működtetése területén:
  - Adat és információ feldolgozás
  - Megjelenítés, riasztások kezelése
  - Adat és információ megosztás felettes és esetleg a felügyeleti szervezetekkel

A feladat ellátáshoz részletesen megtervezett informatikai rendszert kell létrehozni, amely kiszolgálja a katasztrófa megelőzés és elhárítás igényeit.

A SEVESO RENDSZER MŰSZAKI TARTALMA

Monitoring-rendszer

Monitoring-rendszer célja

A *monitoring-rendszer célja* a levegőben terjedő szénhidrogén gőzök és gázok detektálása, töménységének mérése, amely lehetővé teszi a baleseti szintű kibocsátások érzékelését, és a vegyi helyzetre vonatkozó információk gyűjtését. Jelen rendszerrel az üzemeltető olyan érzékelő–riasztási rendszert tud létrehozni, amellyel a lehetséges eseménysorokat már kezdeti fázisban lehet detektálni, azaz a technológiai eszközök, berendezések meghibásodásakor, vagyis közvetlenül a veszélyes anyag szabadba kerülésekor.

A monitoring rendszernek ugyanakkor *nem célja*, a normál technológiai körülmények közötti kibocsátások jelzése, illetve a környezetvédelmi jogszabályokban foglaltaknak való megfelelőség (pontszerű kibocsátások mérése) igazolása. [5]

A Monitoring rendszer felépítésének alapgondolata

A kijelölt CH tárolótereken a veszélyforrás a *cseppfolyósított gáz és folyékony halmazállapotú szén-hidrogének* jelenléte.

Az üzemanyag szabadba kerülésekor tócsa alakul ki, amely párologni kezd, míg a cseppfolyósított gáz halmazállapotú szén-hidrogének esetében azonnali elforrással kell számolni. A keletkező tócsa, illetve a kialakult gőzfelhő akkor válik veszélyessé, ha megfelelő energiájú gyújtóforrással érintkezik. Ezért a monitoring-rendszer elhelyezésénél az egyik legfontosabb figyelembe vett szempont, hogy a rendszer a gőzfelhőt akkor detektálja, amikor az olyan környezetben tartózkodik, ahol normál állapotban a gyújtóforrások jelenléte kizárható (robbanásveszélyes térben). [5]

A robbanásveszélyes terek kijelölése jogszabályi kötelezettség. A robbanásveszélyes terek kijelölésére „Az Országos Tűzvédelmi Szabályzat kiadásáról" szóló 9/2008. (II.22.) ÖTM rendelet 4. rész (Tűzvédelmi műszaki követelmények éghető folyadékok és gázok tárolására), illetve „a potenciálisan robbanásveszélyes környezetben levő munkahelyek minimális munkavédelmi követelményeiről" szóló 3/2003. (III. 11.) FMM-ESzCsM együttes rendelet nyújt iránymutatást. A robbanásveszélyes terekben (a kijelölt zónától függően – 0-as zóna, 1-es zóna, 2-es zóna) csak olyan eszközök, berendezések helyezhetők el, melyek normál üzemben nem képeznek gyújtóforrást.[5]

Amennyiben egy esemény esetleges bekövetkezésekor a szabadba kerülő gőzfelhőt már a robbanásveszélyes terekben sikerül időben detektálni, akkor lehetőség van arra, hogy különböző védelmi intézkedésekkel – pl. áramtalanítás, a gőzfelhő vízzel való hígítása – a késleltetett gyújtás bekövetkezési valószínűsége minimalizálható.

A gázérzékelő típusának megválasztása [5]

Tekintettel arra, hogy a CH tárolótereken többféle szén-hidrogén fajta detektálása szükséges, ezért *javasolt C_1 – C_8 érzékelő típus telepítése*, ami az iparban elterjedten használatos**.** A rendszer telepítésénél fontos szempont, hogy a mérendő gáz (gőz) nehezebb, mint a levegő, így földfelszínen való terjedése várható.

Jelenleg a piacon több különböző mérési elven alapuló gázérzékelő műszer szerezhető be, ezért az 1. számú táblázatban összehasonlítottuk őket. [5]

	Katalitikus elégetés	Hő-vezetés	NDIR (infravörös)	MOS (félvezető)	Elektro-kémiai (O2)	Elektrokémiai (mérgező)	Foto-ionizációs
Méréshatár[2]	ARH%	0...100 V/V%	0...100 V/V%	10000 ppm-től	0...30 V/V%	ppb...ppm	ppb...ppm
Élettartam[3]	●●●●	●●●●	●●●●●	●●●●●	●●●	●●●●	●●
Üresjárási időtartam[4]	●●●●●	●●●●●	●●●●●●	●●●●●	●●●	●●●	●●●●●●
Meghatározott gázok[5]	●●●	●	●●●●	●●	●●●●●●	●●●●	●
Megszólalási idő[6]	●●●●	●●●●	●●●	●●●●	●●●●	●●●●	●●●●●
Energia felhasználás[7]	●●●	●●●	●●●	●	●●●●●	●●●●●	●●●●
Ismétlőképes-ség[8]	●●●●	●●●	●●●●●	●●	●●●●	●●●●	●●●
Stabilitás/null-	●●●●	●●●	●●●●●	●●	●●●●	●●●●	●●

ponteltolódás[9]							
Kalibráció időközök[10]	havonta	havonta	évente	havonta	havonta	havonta	havonta
Hőmérsékleti tartomány[11]	●●●●●	●●●●	●●●●	●●●●	●●●●	●●●●	●●

1. táblázat.

- A érzékelők sajátosságai, rangsorolva a következő besorolások szerint: gyenge ●, megfelelő ●●, jó ●●●, nagyon jó ●●●●●, kiváló ●●●●●
- Mérési tartomány, ppb/ppm szint a mérgező gázokra, ARH % tartomány az éghető gázokra, térf % tartomány az oxigén mérésénél
- A érzékelők várható élettartama: < 3 hónap ●, < 1 év ●●, < 2 év ●●●, < 5 év ●●●●, > 5 év ●●●●●
- "Üres járási" élettartam; néhány érzékelő esetében megfelelő száraz, hűvös helyen történő tárolás esetében lényegében korlátlan ●●●●●, de pl. az elektrokémiai cellás érzékelők esetében 6 hónap ●●●.
- A érzékelőket besorolhatjuk meghatározott gázokra történő kalibrálhatóságuk szerint: ●-●●●●●.
- Megszólalási idő, amíg az üzemkész állapotban lévő érzékelő eléri a mért érték 90 %-át.
- Teljesítményfelvételi igény, különösen fontos a hordozható műszerek esetében a korlátozott akkumulátorteljesítmény miatt.
- A mérés ismétlőképessége az egymást követő kalibrálások között.
- Néhány érzékelő esetében lassú nullponteltolódás észlelhető. Ez az ún. drift meghatározza a nulla és érzékenység kalibrálás gyakoriságát.
- A kalibrálás gyakorisága (tájékoztató jellegű érték, ugyanazon mérési elven működő érzékelők esetében a különböző anyagok szerint is lehet eltérés). Megjegyzés: A kalibrálás összehasonlítás egy hiteles anyagmintával, amely rögzíti a talált meteorológiai jellemzőket. Nem azonos a beszabályozással.
- A legtöbb érzékelő megbízhatóan működik 40...50 °C-ig. Alacsonyabb hőmérsékleti tartományban, mialatt néhány típus -40 °C alatt is működőképes ●●●●●., mások csak 0°C fölött képesek megfelelően működni ●.

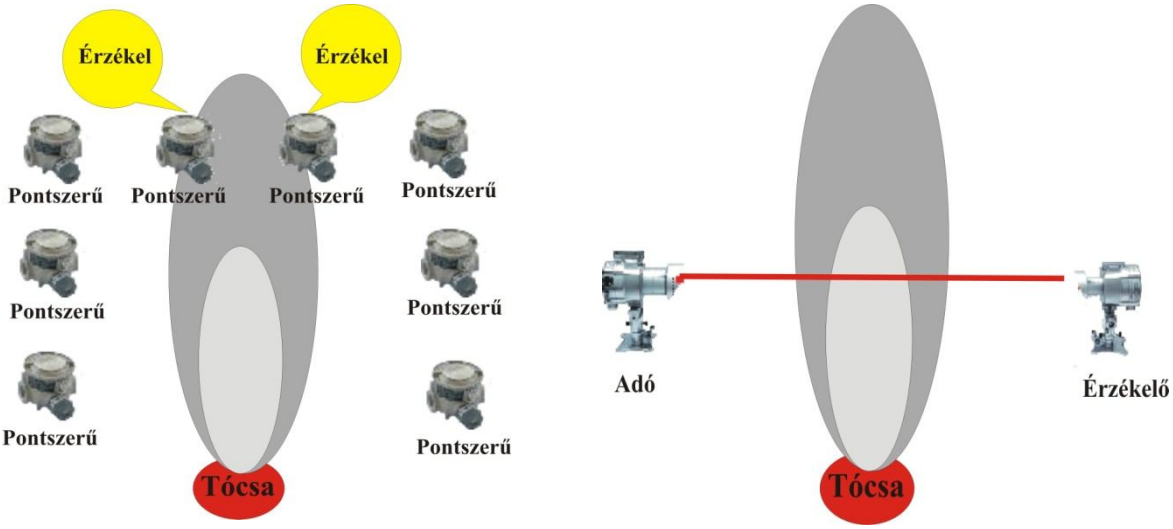
A fenti összehasonlító táblázat szerint a legkedvezőbb üzemeltetési feltételekkel – preferáltan figyelembe véve a karbantartást (kalibrálását) – az infravörös gázérzékelő rendelkezik.

Jelenleg a világon, CH tárolóterekben a normálüzemi (és egyben baleseti célú) monitoringozáskor az érzékelékeléshez kizárólag infraspektrometriás vonali módszerek használatosak (és ilyen elven működő eszközök kaphatók), ezért eltekintünk a más detektálási elven alapuló vonali monitoring eszközök bemutatásától.

A monitoring rendszernek nagy területen kell az éghető gázt (gőzt) detektálni. A szabad téren a gőzfelhő észlelése pontszerű érzékelőkkel igen komoly hibákhoz vezethet, hiszen az érzékelők csak a közvetlen környezetükben levő gázt képesek jelezni. (A MOLARI rendszer

kapcsán végzett számításaink szerint hatékony – közel teljes hatékonyságú - kimutatás csak akkor lehetséges, ha kb. 10 -15 méterenként telepítjük a pontszerű gázérzékelőket). Ennek egyik alternatívája a vonali érzékelés, amely során a felhőt infravörös sugárral „szúrjuk" át, és az elnyelési mutatókból következtetünk arra, hogy a nyaláb mennyi molekulával találkozott. Tehát a vonali érzékelés sokkal hatékonyabb a pontszerűnél. A vonali érzékelő telepítését indokolja továbbá, hogy

- bizonyos időjárási helyzetben a gáz még a sűrűn, 10 – 15 méterenként telepített pontérzékelőt is megkerülheti,
- a 10 – 15 méterenként telepített pontérzékelő üzemviteli – például fűnyírás, folyamatos hó-eltakarítás stb. – szempontból is kellemetlenségeket okozhat.



2. ábra. A pontszerű és a vonali érzékelők működésének összevetése (saját készítés)

Amennyiben a terepviszonyok, illetve a védendő távolságok mégsem teszik lehetővé a vonalérzékelő alkalmazását, a detektálást *javasolt pontszerű érzőkkel* kiegészíteni. Ezeket oly módon kell telepíteni, hogy a terjedő felhő nem kerüli meg az érzékelőket.

Meteorológiai állomás

A mikro-meteorológiai információk gyűjtéséhez az érintett CH tárolótér területén legalább 2 db meteorológiai mérőállomást kell működtetni. A minimum kettő elhelyezését a következők indokolják:

- Egy telephelyre vonatkozó redundáns mérés biztosítása (pl: egy mérőműszer kiesése nem jelenti a mérési adat teljes elvesztését a telephelyre vonatkozóan)
- A telepítés helyére vonatkozó káros és zavaró tényezők kiküszöbölése (pl: szélárnyék, turbulenciák hatása)
- A mérési eredmények megfelelő algoritmus szerinti feldolgozásával kompenzálhatók egyes mérési hibák (pl: átlagolás, változásmeredekség ellenőrzés, stb)

A meteorológiai mérési adatok alapvetően befolyásolják a vegyi helyzetet. Ez kihat a helyzetértékelésből fakadó feladatokra, tehát alapvető az életmentés és kárelhárítás tervezéséhez. A gőz/gázfelhő terjedésében a szélnek van alapvető szerepe, de más mutatók is

fontosak a terjedésben. Ezek meghatározásához az alábbiakban javaslunk mérési elveket és eszközöket.

Szélirány

A levegő mozgásállapotát adott pillanatban és adott helyen egy **vektor** jellemzi, amely a mozgás irányával azonos irányba mutat, és amelynek nagysága arányos a légmozgás sebességével.

A vertikális légáramlatok, vagy azok hiánya jelentősen befolyásolhatják a légtérbe jutott elegyek koncentrációját. Tekintve, hogy egyes veszélyes gázok nehezebbek a levegőnél, ezért azok horizontális és vertikális terjedését a földhöz közelebb mozgó szelek, légáramlatok, valamint a légkör stabilitási viszonyai fogják elsősorban befolyásolni.

Véleményünk szerint a szél méréséhez célszerű alkatrész nélküli mérés ultrahangos szélmérőt alkalmazni. A korszerű szélmérők intelligens parancskészlete az alábbi paraméterek lekérdezését teszi lehetővé:

- átlagsebesség
- lökés
- átlag irány
- irány extrémumok
- lökés iránya
- lökés ideje
- virtuális hőmérséklet

Az ultrahang terjedési sebességének mérésén alapuló mérőeszköz mozgó alkatrészt nem tartalmaz, nincs indulási küszöbsebessége, a legkisebb légmozgást is megbízhatóan méri.

Léghőmérséklet és páratartalom

A léghőmérséklet és páratartalom mérésére kombinált műszer alkalmazható, amelyek egy közös árnyékoló kalap alatt kerüljenek elhelyezésre. Az árnyékoló kalap funkciója, hogy az érzékelő szondákat védje a közvetlen napsugárzástól, csapadéktól és biztosítsa a levegő szabad áramlását.

Ultrahangos csapadékmérő

A csapadékmérők új családtagja a „distrometer”, egy olyan meteorológiai mérőműszer, amelyik lézersugarak segítségével komplex mérést végez. Kalkulálja az intenzitást, mennyiséget (víz egyenérték) és a csapadék spektrumát (csep/szemcse mérete, sebessége) méri a meteorológiai láthatóságot és a visszaverődési tényezőt.

Terepi adatgyűjtés

A monitoring rendszerben a terepi adatgyűjtést, vezérlést és kommunikációs megoldást, valamint az egész rendszer energiaellátását integrált RTU (Remote Terninal Unit) berendezések biztosítják. Mivel az RTU-k közvetlenül a veszélyeztetett területen, a mérőműszerek közelében kerülnek elhelyezésre, ezért a műszerszekrényének alkalmasnak kell lennie Ex Zóna-2 övezethatáron belül történő működésre.

Az RTU biztosítja a következő funkcionális feladatokat, vagyis:

- Fogadja a primer műszerek köreit az ipari szabványoknak megfelelő I/O felületeken
- Biztosítja a primer műszerekkel a soros vonali kapcsolatot, ha szükséges
- Biztosítja a kétállapotú vezérlő jeleket (24VDC, dry contact, stb)
- Biztosítja a külső, belső kommunikációs felületeket (LAN, RS 232, RS 485)
- Biztosítja a leggyakoribb ipari protokollokat a soros felületeken (TCP/IP, MODBUS RTU, HART, stb)
- Biztosítja a primer műszerezés és az összes rendszerelem számára a szünetmentes energiaellátást.
- Biztosítja az eszközökre vonatkozó önteszt funkciókat (akkumulátor kapocsfeszültségének állapota, tápfeszültség megléte, ajtónyitás állapota, gázérzékelő üzemképességének állapota)

Az RTU-k redundáns optikai körgyűrűs hálózaton csatlakoznak a Helyi Informatikai Központ rendszeréhez.

A monitoring RTU-k 4-4 db gázérzékelő pár felügyeletét látják el egyidejűleg, hogy 1 db RTU egység meghibásodása ne jelentse a teljes monitoring rendszer megbénulását.

A mérésadatgyűjtést végző RTU-k a primer műszerek mérési adatait a következőképpen kezelik:

- Az RTU-hoz tartozó memóriában hosszútávon őrzi az időbélyeggel ellátott és dimenzionált mérési adatokat (ez azt jelenti, hogy a központi rendszertől függetlenül is bármikor, utólag kinyerhető a terepi mérési adat)
- Nagysebességű optikai hálózaton a központi adatgyűjtőhöz továbbítja a mérési adatokat.

Ez a megoldás nagy biztonsággal, két egymástól független rendszerben őrzi üzemi szinten az adatokat, így nagy valószínűséggel elkerülhető az adatvesztés. (nem beszélve a külső informatikai rendszerek adatgyűjtéséről és archiválásáról)

A terepi RTU-k és a központi adatgyűjtő között redundáns optikai hálózat biztosítja az adatáramlást. A hardveres felületet optikai médiakonverterek adják. Az optikai hálózat klasszikus körgyűrűs elrendezést mutat. A megoldás lényege, hogy a gyűrűn belül bekövetkező szakadás után a másik ágon bármelyik RTU továbbra is képes kommunikálni. Az optikai rendszer működőképességét folyamatosan felügyeli a központi rendszer.

Az RTU rendszer elsődleges energiaellátása az üzemi 230VAC hálózatról történik. Ez a hálózat tölti a beépített 24VDC akkumulátort, ami puffer üzemmódban működik. Gyakorlatilag szünetmentes energiaellátást biztosít az RTU berendezés összes aktív eleme számára. A rendelkezésre állás időtartamát úgy kell méretezni, hogy akár hálózat-kimaradás esetén, akár katasztrófahelyzetben kellő ideig (legalább 6 órán keresztül) működőképes legyen a rendszer.

Tájékoztatórendszer

A tájékoztatórendszer felépítésének alapgondolata

A tájékoztatórendszer egyik alapvető feladata az adott telephelyek kültéri területein, illetve a területen található épületekben tartózkodó személyzet, valamint a telephely határvonalával szomszédos területeken elhelyezkedő polgári lakosság tájékoztatása a veszélyes üzemek baleseteiről és a bekövetkező események káros hatásának elhárítását vagy csökkentését célzó intézkedésekről a létesítmény telekhatárától mért 300 méteres távolságon belül lévő

tartózkodási helyeken. A működési folyamatábrát tekintve a tájékoztató rendszer legvégső részei a kihangosítási végpontok, amelyek segítségével vészjel hangok és szöveges információ továbbítható a lakosság felé. A kihangosítók felépítésénél a MSZ EN 60849:2000 „Hangrendszerek veszélyhelyzetekhez" című magyar szabvány előírásai az irányadók.

A nagy besugárzott terület (több négyzetkilométer), a ritka megszólalási alkalmak (évente legfeljebb néhány eset), a viszonylag egyenletes megoszlású és kis alapzaj (45-60 dB(A)) miatt jelen esetben kisebb számú, egymástól nagyobb távolságban elhelyezett, nagyobb egység teljesítményű hangforrásokból felépülő kihangosító rendszer kialakítása gazdaságos. Az üzemi területen történő elhelyezés miatt a kihangosítási végpontok áramellátása a CH tárolóterek belső elektromos hálózatról oldható meg, de áramkimaradás esetére a folyamatos üzemet szünetmentes tápegység beépítésével kell biztosítani a rendszer egészére.

A besugárzott terület nagysága, illetve az egyes sugárzási végpontok és a központ közötti nagy távolság miatt, valamint a rendszerfelügyelet és a továbbítandó adat mennyiségét figyelembe véve a IP alapú, zárt-gyűrűs optikai hálózat kiépítésével (összhangban a monitoring rendszerrel) kell megvalósítani. A zárt-gyűrűs optikai hálózat, valamint az IP kompatibilis eszközök alkalmazásával lehetőség nyílik a rendszer további fejlesztésére, bővítésére, valamint a tereptárgyak módosítása, változása során akusztikai szempontból szükséges módosítások elvégzésére. Az IP alapú végberendezések tesztelése, felügyelete, vezérlése hálózaton keresztül távoli hozzáférést biztosít, rendszer-integrációja könnyen megvalósíthatóvá válik.

Kültéri végberendezések szolgáltatásaival szemben támasztott követelmények

- Egyértelmű, jól áttekinthető kezelőfelület.
- Alkalmas legyen a rendszeresített riasztási jelzések memóriából történő kisugárzására.
- Alkalmas legyen a helyi és a távvezérelt üzemmódban egyaránt az előbeszédes tájékoztatást kisugározni.
- Alkalmas legyen a végpontokon tárolt rögzített szöveg kisugárzására.
- A végpont vészhelyzeti kommunikációs (beszédátviteli) állomásként is használható legyen akár távolról akár helyben.
- A berendezés tárolja a végponti események minimum utolsó 200 bejegyzését dátumhoz, időponthoz társítva.
- Távoli szerviz hozzáférés lehetősége.
- Szervizcsatlakozó kialakítása a berendezés paramétereinek helyszínen elvégezhető beállításához.
- A berendezések paramétereinek ellenőrzését, módosítását, illetve beállítását hordozható PC kompatibilis egységgel megvalósítható legyen.
- Moduláris berendezés kialakítása a gyors szervízelhetőség érdekében.
- A berendezésnek alkalmasnak kell lennie az úgynevezett „hangtalan" próbára.
- Beépített önteszt funkciókkal kell rendelkezni az eszköznek, mely a következő paramétereket kell tartalmaznia (akkumulátor kapocsfeszültségének állapota, tápfeszültség megléte, ajtónyitás állapota, hangfrekvenciás erősítő üzemképességének állapota, hangsugárzók üzemképességének állapota)

- Az ajánlott eszköz rendelkezzen magyarországi javítóanyag bázissal és szakképzett javító személyzettel.

Beltéri végberendezésekkel szemben támasztott követelmények

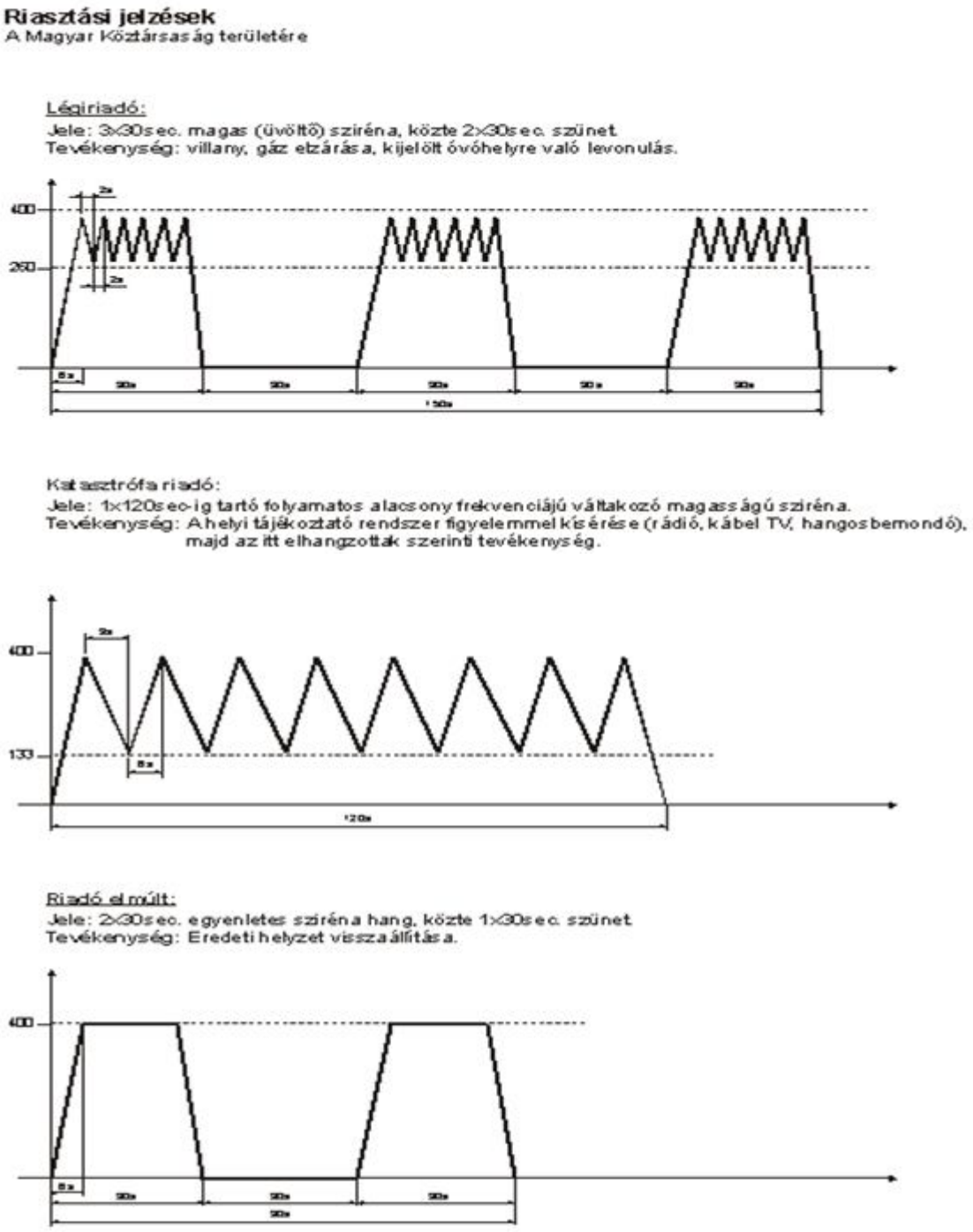
- Alkalmas legyen a rendszeresített riasztási jelzések memóriából történő kisugárzására.
- Alkalmas legyen távvezérelt üzemmódban az előbeszédes tájékoztatást kisugározni.
- Alkalmas legyen objektumonként más-más előre rögzített szöveg kisugárzására.
- A berendezés tárolja a végponti események minimum utolsó 200 bejegyzését dátumhoz, időponthoz társítva.
- Távoli szerviz hozzáférés lehetősége.
- Szervizcsatlakozó kialakítása a berendezés paramétereinek helyszínen elvégezhető beállításához.
- A berendezések paramétereinek ellenőrzését, módosítását, illetve beállítását hordozható PC kompatibilis egységgel megvalósítható legyen.
- Moduláris berendezés kialakítása a gyors szervízelhetőség érdekében.
- A berendezésnek alkalmasnak kell lennie az úgynevezett „hangtalan” próbára.
- Beépített önteszt funkciókkal kell rendelkezni az eszköznek, mely a következő paramétereket kell tartalmaznia (tápfeszültség megléte, hangfrekvenciás erősítő üzemképességének állapota, hangsugárzók üzemképességének állapota)
- Az ajánlott eszköz rendelkezzen magyarországi javítóanyag bázissal és szakképzett javító személyzettel.

Kisugározandó jelzések szövegek

Előre rögzített szövegek

Az eszközök képesek legyenek legalább 10 db 0,5 perc hosszú előre rögzített szöveg tárolására és esetleges megszólaltatására.

Kisugározandó jelzések



3. ábra. A légi és a katasztrófariasztás sziréna jelzései [4]

Informatikai rendszer

Rendszer elemek

Az Informatikai rendszer rendeltetése a SEVESO RENDSZER adatainak feldolgozása, kiértékelése, tárolása, felügyelete és vezérlése.

Helyi Informatikai Központ: Az objektumon belül működő, a SEVESO RENDSZER által szolgáltatott jelek, mérési adatok feldolgozására, információk előállítására, riasztási jelek generálására és akusztikai vezérlésekre alkalmas rendszer. Támogatja az elhárítási

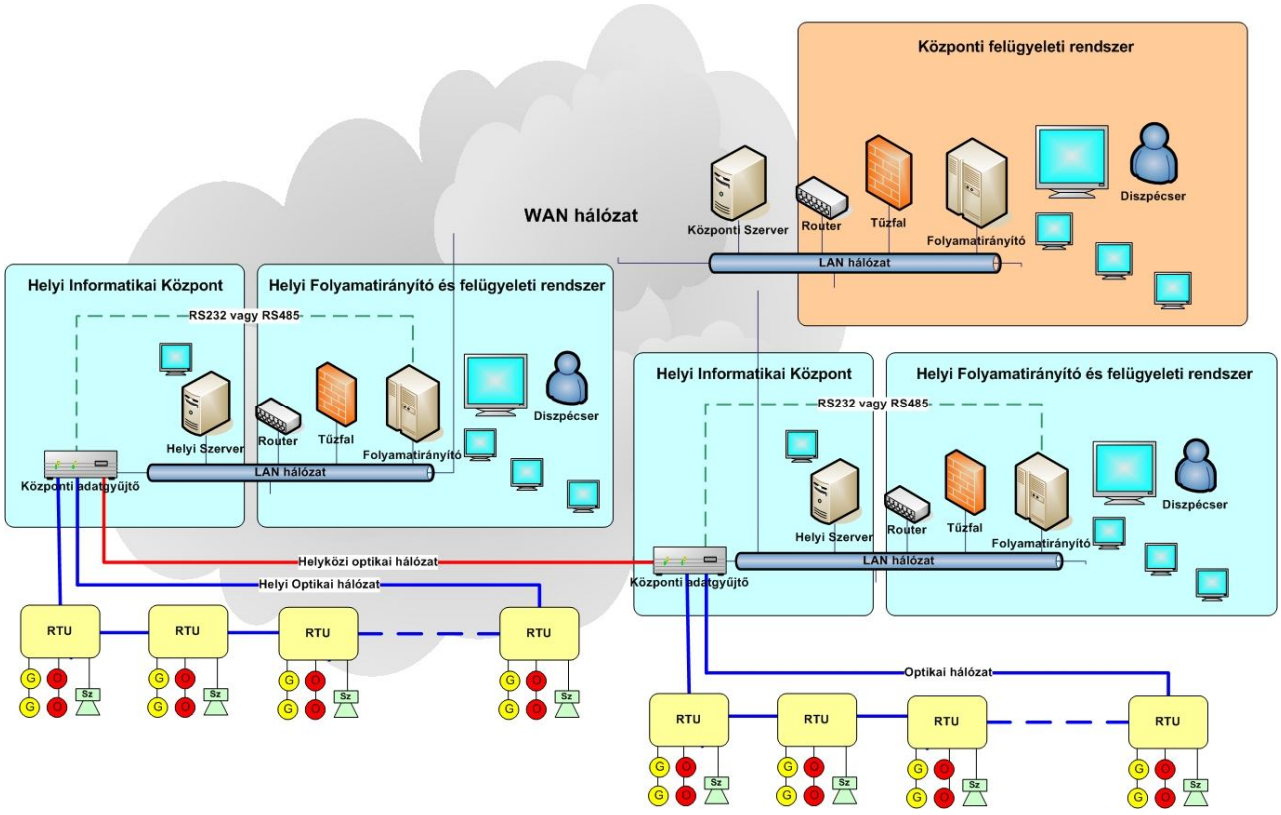
tevékenységet, adatot és információt szolgáltat minden érintett munkaszervezet és döntéshozó személy számára. A Helyi Informatikai Központ adatátviteli kapcsolatban állhat más helyi (pl: folyamatirányító) és távoli (pl: HAVARIA központ) rendszerrel, de azoktól függetlenül, szigetszerűen is működőképesnek kell lennie.

Az informatikai központ egy duplikált szerveren gyűjti az adatokat, amit elér a helyi felügyeleti megjelenítő egység és a távoli központ duplikált szervere is. A távoli központ szervere és a helyi szerverek folyamatos kapcsolatban állnak, hogy az adatok, mind a két helyen egyidejűleg tárolásra kerüljenek.

Helyi adatátvitel, helyi alhálózaton (LAN): Az objektum telephelyén belüli adatátviteli kapcsolat rendszere, amely alkalmas arra, hogy információval lássa el az üzemeltetésben, felügyeletben érintett telephelyi munkaszervezeteket. Gyakorlati megvalósulása egy optikai , „gyűrűbe zárt" gerinchálózaton alapuló TC/IP hálózat.

Távoli adatátvitel, távoli hálózatokon (WAN): Az objektumban keletkezett információkat, riasztási státuszokat adott esetben meg kell osztani távoli felügyeletet, vagy operatív beavatkozást biztosító távoli munkaszervezetekkel (pl: HAVARIA központ, Létesítményi Tűzoltóság). Az ehhez szükséges adatátvitel az üzemeltető által üzemeltett belső ipari hálózaton valósul meg és tartalék adatátviteli útként pedig a ipari GPRS hálózatot célszerű felhasználni.

Távoli Informatikai Központ (..ok): Az objektumok lokális felügyeletén túl távoli helyeken levő munkaszervezetek (pl: HAVARIA központ, Létesítményi Tűzoltóság) is gyakorolhatnak felügyeletet, ellenőrzést. Ez az informatikai rendszer működőképességének, a riasztási státuszok ellenőrzésére is kiterjed, akár egy, akár több távoli helyről is



4. ábra. Informatikai rendszer [5]

Helyi Informatikai Központ rendszere

Minden CH tárolóteren ki kell alakítani azt a központi rendszert, ami biztosítja a működtetéshez, feladatellátáshoz szükséges informatikai megoldást.

A Helyi Informatikai Központ legfontosabb fizikai rendszerelemei:

- *Média konverter,* az optikai adatátvitelt biztosítja az RTU berendezésekkel
- *Központi adatgyűjtő* és vezérlő, kommunikációs csomópont a terep és a központ között
- *Helyi duplikált szerver rendszer,* biztosítja az összes klasszikus informatikai funkciót
- *Kiegészítő informatikai rendszer,* folyamatirányító, router, tűzfal.

A Helyi Informatikai Központ rendszere a következő főbb funkciókat kell, hogy biztosítsa a veszélyelhárításban érintett helyi szakemberek számára:

- Objektum szintű központi adatgyűjtés
- Jelfeldolgozás
- Adatbázis kezelés
- HMI felületek biztosítása
- Mérési adatok és információk megjelenítése
- Mérési határértékek átlépésére keletkező riasztások kezelése
- Akusztikai jelzések vezérlése
- Rendszerelemek paraméterezése
- Rendszerelemek informatikai menedzselése, felügyelete
- Helyi jogosultsági szintek, engedélyezett felhasználók paraméterezése
- Naplózás
- Adatmentés, archiválás
- Hangosító rendszer menedzselése
- Adat és információ megosztás más engedélyezett felhasználók részére

Távoli Informatikai Központ rendszere

Célja a katasztrófa elhárításhoz kapcsolódó tevékenységek támogatása és ellenőrzése, illetve az informatikai rendszer felső szintű üzemeltetéséhez kapcsolódó ellenőrzési, távmenedzselési funkciók biztosítása.

A Távoli Informatikai Központ legfontosabb fizikai rendszerelemei:

- Router, A WAN hálózati adatátvitelt biztosító csomóponti rendszerelem
- Tűzfal, a biztonságos adatátvitel rendszereleme
- Központi Szerver rendszer, biztosítja az összes klasszikus informatikai funkciót

A Távoli Informatikai Központ rendszere a következő főbb funkciókat biztosítja az érintett szakemberek számára:

- Központi szintű adatgyűjtés

- Adatbázis kezelés
- HMI felületek biztosítása
- Mérési adatok és információk megjelenítése
- A terepi rendszerben keletkezett riasztások kezelése, ellenőrzése
- Informatikai rendszer távmenedzselése, felügyelete
- Felsőszintű jogosultsági szintek, engedélyezett felhasználók paraméterezése
- Naplózás
- Adatmentés, archiválás
- Adat és információ megosztás más engedélyezett felhasználók részére

Riasztási szintek

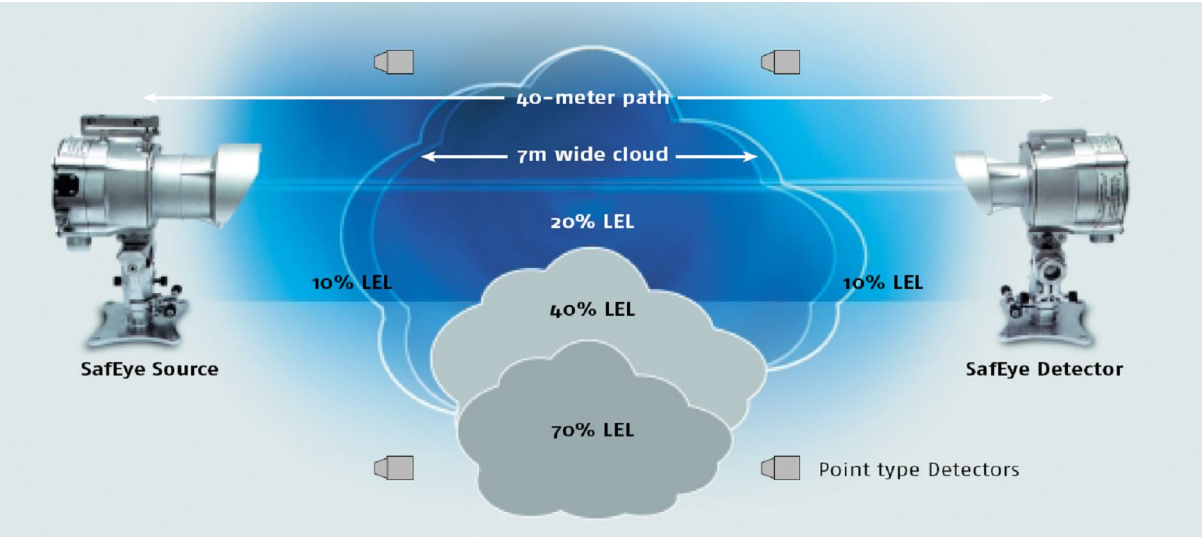
Vonali gázérzékelés elvi alapjai

A SEVESO RENDSZER a CH tároló terek technológiai tevékenységétől független működésű. A rendszer szakszerű működtetését csak abban az esetben lehet biztosítani, ha értjük annak működési elvét. Magyarországon az olaj és gáziparban általános mérési gyakorlatként pontszerű mérőműszereket használták eddig, ahol a mérési eredmény dimenziója az „ARH”, azaz alsórobbanási határérték volt.

A SEVESO RENDSZERekben használatra javasolt „open path” (vonali) mérési elv új távlatot nyit a biztonságos gázkoncentráció mérés, érzékelés területén, új dimenzióként az „ARH.m” használata szükséges.

A pontszerű érzékelők a térben csak egyetlen pontban képesek mérni a gázkoncentrációt. Ezért könnyen előfordulhat, hogy a gázfelhő éppen kikerüli a pontszerű gázérzékelőt és így nem lehet időben észlelni a veszélyes eseményt.

Az „open path” (vonali) mérőműszer viszont két pont közötti szakaszban méri a gáz előfordulását, tehát lényegesen nagyobb az esélye a veszélyes esemény észlelésének. A mérés elvét az alábbi ábra mutatja be: (LEL = ARH)



5. ábra. A vonali érzékelés elve [6]

Nem minden gázfelhő végzetesen veszélyes, – egy gyúlékony gáz, vagy gőzfelhő csak akkor válik jelentős veszéllyé, ha elég széles ahhoz, hogy abban a láng gyorsulása meghaladja a 100 m/sec értéket.

- Ugyanúgy, ahogy egy távolugró sportolónak is szüksége van nekifutási távolságra, a lángnak is szüksége van távolságra, hogy elérje azt a sebességet, amely az égés során a túlnyomás, nyomásimpulzus és szélnyomás káros hatásait okozza.
- Az általánosan elfogadott gázmennyiség, amelynek megvan az a potenciálja, hogy gyulladás esetén kárt okozzon, egy 5 m átmérőjű felhő, sztoichiometrikus koncentrációban. (körülbelül 200% ARH).
- Hogy legyen biztonsági ráhagyás, ezt a koncentrációt felezik 100% ARH-ra. Így a méréshez használt infrasugár, ami áthatol ezen a felhőn, 5 ARH.m értéket mutat.
- A vonali gázérzékelő elhelyezése kevésbé kényes, mint egy pontszerűen mérő érzékelő esetében, mivel a felhígult gázfelhőről is ad mérési jelet és nem kell közel lennie a szivárgási forráshoz.
- A pontszerűen mérő érzékelők egy adott pontban, % ARH értékben mérik a gázt, viszont az „open path” gázérzékelők a gáz mennyiségét az infra-fény szakasz mentén bárhol mérik, a koncentráció és hosszúság szorzatának értékében.

ARH.méter

Érzékelő kimenet:	gázfelhő koncentrációja (ARH) x gázfelhő hossza (m)
A mérési egység:	ARH.méter:
A gáz 100% ARH-ja:	1 ARH
1 ARH.méter:	1 ARH x 1 méter

A fentiek értelmében érthető, hogy az egységnyi gázkoncentráció különböző szakasz hosszúságok esetén csak úgy alakulhat ki, ha a levegőben levő gáz mennyisége növekszik. Például:

1 m x 100% ARH = 1 ARH.méter

10m x 10% ARH = 1 ARH.méter

20 m x 5% ARH = 1 ARH.méter

Magyarázat: Az 1 ARH.m azt jelenti, hogy a sugár útjában van egy 1 m széles 100%-os ARH koncentrációjú gázfelhő, vagy egy 10 m széles 10%-os ARH koncentrációjú felhő. Tehát az ARH.m = % ARH x m.

A fentiek tükrében kijelenthető, hogy szakaszra vonatkozó átlag koncentráció mérés történik.

A valóságban a robbanási határ 10 ARH.m, tehát ez az a gázkoncentráció, amely gyújtóforrás esetén belobban. A biztonság kedvéért az elvi robbanási határ az 5 ARH.m értéknél határozták meg a vészriasztási szintet.

Ez az érték a mérőműszerben gyárilag beállított érték, amelyet felhasználói szinten nem lehet változtatni. *Az érzékenység növelését csak speciális műszer és programozói ismeretekkel rendelkező szakcég végezheti 2 ARH.m értékre.*

Jelenleg a mérőműszer 0 és 5 ARH.m érték tartományban felelteti meg az analóg 4-20mA jel tartománynak. (megjegyzés: a rendszer digitális jelként dolgozza fel a mérési értékeket, nem analóg mérésként). A mérőműszer ezen tartomány felett is mér, amely mérési adatok továbbításra kerülnek a SEVESO PC felé. Tehát akár az 5 ARH.m feletti értékeket is méri a rendszer.

A terepen levő „open path” mérőműszer folyamatosan biztosítja a mérési adatokat, amelyeket 3 másodpercenként frissít.

6. ábra. Vonali érzékelési szakasz (saját felvétel)

Figyelmeztetés és riasztás

A rendszerben két egymástól független riasztás történhet a következők szerint:

- *Terepen:* Az érintett objektum elhelyezett, oszlopokra szerelt berendezéseknél a terepi riasztási határérték átlépés esetén hang és fényjelzés keletkezik, amelyet maga a mérőműszer generál, teljesen függetlenül minden más rendszerelemtől. Az egyik szakaszon keletkezett riasztási parancs átterjed az összes oszlop összes hang és fényjelző berendezésére, hiszen a gázfelhő is bármilyen irányba terjedhet, amivel nem csak egy mérési szakasz környezetét veszélyezteti, hanem az egész objektum környezetét is.

- *Helyi Informatikai Központ:* a SEVESO PC számítógépes kezelői felületeken (dinamikus grafikai felületen látható jelzés, hangjelzés). A biztonság kedvéért két külön metódus alapján logikai „vagy” kapcsolat szerint generálódik az ügyeleti riasztás:

    - *A mérőműszer által folyamatosan mért értéke alapján:* ennek értéke a számítógépes rendszerben konfigurálásra került.
    - *A mérőműszer által kapcsolt kétállapotú terepi riasztási jel alapján:* Ennek értéke azonos a terepi riasztás határértékével, nem paraméterezhető a számítógépes rendszerben!

A terepi riasztás már az objektumon kívül is látható, hallható. Ezért nagyon fontos, hogy a felelős személyzet már a terepi riasztás *előtt* tájékozódjon a várható veszélyes esemény bekövetkeztéről. Ennek módja a *többszintű figyelmeztetés*, amely csak a SEVESO PC kezelői felületén kerül kijelzésre, tehát a terepen nem érzékelhető !!!

Az elvi robbanási határ értéke 5 ARH.m, amelynek 60%-nál (3 ARH.m) következik be a terepi mérőműszer által kezdeményezett riasztás jelzés.

A terepi riasztás jelzés bekövetkezte előtt a SEVESO PC-ben előre konfigurált határérték átlépés esetén figyelmeztetés történik. Ennek értékei:

Jelzési szint:	Magyarázat:	ARH.m érték:
Figyelmeztetési szint	elvi robbanási határérték 20%-a	1 ARH.m
1. riasztási jelzés	elvi robbanási határérték 40%-a	2 ARH.m
3. kiemelt riasztási jelzés	elvi robbanási határérték 60%-a	3 ARH.m
Terepi riasztás jelzés	elvi robbanási határérték 100%-a	5 ARH.m

- Figyelmeztetési szint (20%, 1ARHm) – Figyelmezteti a felügyeleti szerveket, hogy az adott érzékelő viszonylatban indokolatlan CH gázszint van jelen. Az érintett területen lévő technológiai egységek felügyeleti rendszerein keresztül meg kell vizsgálni, hogy nem sérült-e meg a technológia.
- Első riasztási szint (40%, 2ARHm) – Ennél a szintnél a helyi és a távoli diszpécserek egyeztetniük kell, hogy szükséges-e kármentesítő egység indítása (pl: Létesítményi Tűzoltóság)
- Második (gázérzékelő) riasztási szint (60%, 3ARHm) – A szabályzatban kijelölt diszpécsernek mérlegelés nélkül értesítenie kell a kármentesítő egységeket, hogy vonuljanak ki és kezdjék meg a terület biztosítását.
- Terepi riasztási szint (100%, 5ARHm) (100%, 5ARHm) – erre akkor kerül sor, amennyiben a terepi eszköz illetve eszközök és a központ között nincs kapcsolat, hogy a helyben tartózkodók vonuljanak a mentési tervben szereplő gyülekezőhelyekre.

A SEVESO PC rendszerben keletkezett figyelmeztetések és riasztások, valamint ezen jelzések kezelése kerüljön naplózásra.

ÖSSZEFOGLALÁS

A veszélyes anyagok felhasználásával üzemelő vállalkozásokkal szembeni minimálisan elvárható társadalmi kritérium, hogy a tevékenységből származó lakosságra gyakorolt kockázata minimális, gyakorlatilag nulla legyen.

A fentiekben felvázolt SEVESO RENDSZER biztosítja, hogy az esetleges HAVARIA eseményeket, még a kialakulás fázisában detektáljunk és megelőzzük a nagyobb mérvű anyagi és személyi sérüléseket.

Irodalomjegyzék:

[1]18/2006. (I. 26.) Korm. rendelet A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

[2]253/1997. (XII. 20.) Korm. rendelet Az országos településrendezési és építési követelményekről

[3]Még mindig oltják Európa legnagyobb tüzét, sg.hu Internetes folyóirat, 2005. dec. 13.

[4]Szakál Béla Veszélyes anyagok és vegyipari katasztrófák III. SZIE YMÉK jegyzet, Budapest, 2008.

[5]Szakál Béla: A társadalmi kockázatok csökkentése a MOL Nyrt. bázistelepein szénhidrogén monitorigozással, előadás a tanszéki konferencián, SZIE YMÉK TÜBI honlapján, Budapest, 2010.

[6]Open-Path Gas Detection System Spectrex Inc. Termékismertető, Houston, 2004.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Schmidt Petra
schmidt.petra.88@gmail.com

A SZÉN-DIOXID KLÍMA ALAKÍTÓ HATÁSA, CSÖKKENTÉSI LEHETŐSÉGEI, KÜLÖNÖS TEKINTETTEL A KIOTÓI EGYEZMÉNY MAGYARORSZÁGI VONATKOZÁSAIRA[1]

Absztrakt

A Föld benépesedése egyre sűrűbben lakott területek kialakulását vonja maga után, melynek hatására exponenciális mértékben a megnő a gazdasági (ipari) teljesítmény, mely felerősítve az üvegházhatást közvetetten felelős korunk legnagyobb környezeti problémája, a globális klímaváltozás kialakulásáért. A klímaváltozás csökkentése globális szintű, rendkívüli jelentőségű feladattá vált. Célom dolgozatommal egy olyan pártatlan állásfoglalás kialakítása, mely vizsgálja a Kiotói egyezmény pozitív és negatív hatásait, a minisztériumi (Környezetvédelmi és Vízügyi Minisztérium) és az úgynevezett „Zöld szervezetek" legjelentősebbikének, a Greenpeace (Hungary) álláspontjának ismeretében.

The population of Earth involves the constitution of more and more densely inhabitated territories as a result of which the economic (industrial) yield increases exponentially. This performance increase results in a more and more aggressive emission, that intensifying the greenhouse effect is indirectly responsible for the biggest environmental problem of our age, the global climate change.. The reduction of climate change became a global and most significant task. The aim of my work is to present such an impartial standpoint that examines the positive and negative effects of the Kyoto Agreement, knowing the position of the Ministry of Environmental Protection and Water Resources and that of the Greenpeace (Hungary), the most significant of the so-called „green organizations".

***Kulcsszavak**: klímaváltozás, szén-dioxid, emisszió, környezetpolitika, Kiotói egyezmény ~ climate change, carbon-dioxide, emission, environment politics, Kyoto convention*

[1] A Bolyai János Hadmérnöki Díj pályázatán 1. helyezést elért pályamunka, 2011.

BEVEZETŐ

Korunk természeti csapásai különösen megviselhetik a lakosságot, tekintve, hogy a világ lakosságának száma évről-évre növekszik. A Föld benépesedése egyre sűrűbben lakott területek kialakulását vonja maga után, melynek hatására exponenciális mértékben a megnő a gazdasági (ipari) teljesítmény. E teljesítménynövekedés, felerősítve az üvegházhatást közvetetten felelős korunk legnagyobb környezeti problémája, a globális klímaváltozás ütemgyorsulásának kialakulásáért.

A klímaváltozás nem katasztrófa, hanem katasztrofális eredmény, mely kísérőjelenségei rendkívüli természeti csapásokat eredményeznek és melyek elsősorban a meteorológiai, hidrometeorológia események gyakoriság és mérték növekedésében tapasztalhatóak (extrém időjárás, árvizek).

Megváltozik az élettér, eltolódnak az éghajlati övek. Ezen szélsőséges éghajlati események hatására biodiverzitás csökkenés, átalakulás várható.

Különös jelentőséggel és felelősséggel bír a feladat, ha azt vesszük figyelembe, hogy a katasztrófa sújtotta területek újra helyreállíthatók, a fizikai kár helyrehozható, de a környezet károsodási folyamatának visszafordítása jelenleg irreális feladatnak minősül.

Cikkemben igyekszem reálisan, a mai nemzetközi - magyarországi viszonyoknak megfelelően bemutatni, hogy miként hat a levegő szennyezése, a káros anyag kibocsátása a környezetünkre illetve milyen nívójú megoldást jelenthet erre a Kiotói egyezmény, különös tekintettel hazánkra nézve.

Célom dolgozatommal továbbá egy olyan pártatlan állásfoglalás kialakítása, mely vizsgálja a Kiotói egyezmény pozitív és negatív hatásait, a minisztériumi (Környezetvédelmi és Vízügyi Minisztérium ,később Vidékfejlesztési Minisztérium) és az úgynevezett „Zöld szervezetek" legjelentősebbikével a Greenpeace (Hungary) álláspontjának ismeretében.

A napjainkat fenyegető klímaváltózás nem új keletű kifejezés, klímaváltozás már az őstörténet óta folyamatosan alakítja Földünk felszínét, éghajlatát, de sosem volt még ilyen gyors ez a folyamat. Az emberek számára éppen ezért nem vált közvetlenül érzékelhetővé - egészen napjainkig. Ez mára megváltozott. Gondoljunk csak az utóbbi idők hazai szélsőséges időjárási anomáliáira.

Ma már emberi léptékkel halad a klímaváltozás, így a felgyorsult folyamatok, azok kísérőjelenségei számunkra is érzékelhetővé váltak. Tudományos kutatási eredmények bizonyítják, hogy elsődlegesen az emberi tevékenység a kiváltó oka a folyamat felgyorsulásának.

A szén-dioxid csökkentése globális szintű, rendkívüli jelentőségű feladattá vált, mely csökkentés mára már nem csak egy lehetőség, időközben szükségszerű tevékenységgé nőtte ki magát. Nemzetközi összefogás, koordinációs megoldás vált szükségessé. Amennyiben nem születik globális megoldás a klímaváltozást előidéző üvegházhatású gázok csökkentése érdekében, az esetben ez a folyamat ellenőrizhetetlenül felgyorsul majd.

Számtalan emberi áldozat és környezeti érték menthető meg a káros anyag kibocsátás csökkentésével, energia hatékony technológiák alkalmazásával, progresszív nemzeti stratégia létrehozásával, egy környezet tudatosabb életmód kialakításával.

A klímaváltozás csökkentése globális szintű, rendkívüli jelentőségű feladattá vált. Nemzetközi összefogás, koordinációs megoldás vált szükségessé.

Legfőbb célként, a kormányzati szervek, illetve az önkéntes társadalmi csoportok között egy konszenzusra, véleményütköztetésre lehetőséget adó fórum megteremtését látom.

A KLÍMAVÁLTOZÁS

Mostanában sokat olvashatunk, hallhatunk a globális klímaváltozásról, a globális felmelegedésről, a szélsőséges, extrém időjárási események gyakoriságának növekedéséről, a gleccserek elolvadásáról, tavak kiszáradásáról, az évszakok eltolódásáról, egyre gyakoribbá és hevesebbé váló természeti katasztrófákról.

Mit is jelent a klímaváltozás? A klímaváltozás tulajdonképpen egy ál fogalom, mert klímaváltozás mindig is volt, van és a jövőben is lesz. Ma már nem csak természeti, hanem egyben társadalmi jelenséggé is vált. A klímaváltozás tehát a Föld éghajlatának nagymértékű megváltozása, melyben az emberi tevékenység jelentős és egyre növekvő tényező.

Ez a változás a Föld életében nem ismeretlen jelenség. Ciklikusan ismételte önmagát.

A kutatási eredmények azt bizonyítják, hogy az elmúlt 400.000 évben szabályszerű ciklusok voltak. Két ciklus csúcs között körülbelül 80.000 év telt el, melyek folyamatosan ismételték egymást. Ebből a bizonyos 80.000 évből kb.30 ezer év a lassú lehűlés időszaka volt, ezt követte a kb. 20.000 éves úgynevezett jégkorszak és végül egy kb. 30 ezer éves lassú hőmérséklet emelkedés, azaz felmelegedés indult meg.

Felmerül a kérdés, vajon hol tart a világ jelenleg ebben a bizonyos éghajlat változásban? Mely szakaszban lehetünk most?

A kutatók azt valószínűsítik, hogy jelenleg a már előbb említett úgynevezett melegedési szakaszban vagyunk, (a jégkorszak után eltelt kb. 18-20 ezer év), melyből maradt kb. 10-12 ezer évünk a lassú felmelegedésre. Utána ismét újra fordul ez a folyamat.

A kérdés azonban a következő. Vajon mennyire sikerült az úgynevezett emberi tényezőnek ezt a folyamatot felgyorsítania? Vajon mennyivel rövidül ez a hátralévő 10-12.000 év? Mit tehetünk ellene?

Ahhoz, azonban, hogy egy problémát meg lehessen oldani, ismerni kell az azt kiváltó okokat. Természetesen, mint mindennek a klímaváltozásnak is van oka. Mi ez az ok?

Az ok az üvegházhatású gázok dúsulása a légkörben (melyért a leginkább a szán-dioxid kibocsátás a felelős). Ennek okozataként jelentős felmelegedés indul meg, melynek következményei a szélsőséges meteorológiai, hidrometeorológiai események gyarapodása.

Az emberiség az ipari forradalom óta (150-200 éve) hatalmas mennyiségben éget el fosszilis energiahordozókat (szén, kőolaj), és ezzel üvegházhatású gázokat, főként szén-dioxidot juttat a levegőbe. Ennek eredménye, hogy az utóbbi száz évben a globális átlaghőmérséklet már 0,74 Celsius fokkal megemelkedett, és ha a jelenlegi ütemben folytatódik a felmelegedés, akkor a század végéig várhatóan 2 fokkal lesz magasabb a globális átlaghőmérséklet.

A kutatók az Antarktisz jégtömbjeiből vettek furatmintákat, azokban helyenként levegő buborékok találhatók, melyekből egy úgynevezett kémiai analízis segítségével megállapítható, hogy a furatban található jég keletkezésének idejében mekkora volt a Földön a széndioxid tartalom, valamint a hőmérséklet.

A kutatási eredményekből kiderült, hogy az elmúlt 400.000 évben a levegő szén-dioxid tartalma sohasem haladta meg a 280ppm-et, azonban a mai eredmények azt mutatják, hogy jelenleg a levegő szén-dioxid tartalma már a 380ppm feletti.

Ebből is látható, hogy a széndioxid csökkentés mára már nem csak egy lehetőség, hanem egy szükségszerű tevékenység. Hiszen ha nincs utánpótlás, ha ma megszüntetnénk minden kibocsátó forrást, a szén-dioxid molekula még akkor is minimum 45-50 évig benne marad a légkörben.

(Prof. Dr. Láng István előadásanyagából dolgozva- Klíma és Biztonság Konferencia I. 2009)

A CSÖKKENTÉS ÉRDEKÉBEN TETT LÉPÉSEK

A tudósok véleménye szerint, ha a globális klímaváltozás ilyen ütemben folytatódik, abban az esetben a következő események várhatóak hazánkban:

Magyarország a „nedves óceáni, a mediterrán és a száraz kontinentális éghajlati régiók határterületén helyezkedik el", és ezért már a kismértékű zónák eltolódásában testet öltő éghajlatváltozás is a globálist meghaladó mértékű hatást eredményezne.

Az ENSZ Fenntartható Fejlődés Bizottságának jelentése alapján hazánk az egyik legsérülékenyebb ország a klímaváltozás- valamint annak a természeti sokszínűségre gyakorolt hatása szempontjából. Meteorológiai számítások alapján hazánk átlaghőmérsékletének emelkedése csaknem másfélszer nagyobb a globális felmelegedés üteménél.

Az előrejelzések azt sejtetik, hogy 20-30 év múlva, körülbelül 2030-ra számottevő változások várhatók az évszakok hosszát, lefolyását valamint fázisát illetően: rövid, valószínűleg igen változékony tavaszt, a mai állapotnál lényegesen hosszabb, de annál nem sokkal melegebb, csapadékban szegény nyár követ. Az ősz későbbre tolódik és tovább tart, így a mai indián nyárra emlékeztet majd, míg a januártól márciusig tartó telet a mai szóhasználattal nagyon enyhének neveznénk, de rendkívül sok csapadékkal érkezik.

Magyarországon várhatóan az északnyugati szelek egyre gyakrabban fordulnak déliesre, ezek pedig a csapadékos óceáni levegő helyett száraz mediterrán, szubtrópusi meleget hoznak, időnként irgalmatlan viharokkal. Hosszú távon fokozatos felmelegedés, a nyári csapadék mennyiségének csökkenése várható, mely az alföldi részek teljes elsivatagosodásához vezetnek majd.

A korábban ismertetett tények élesen rávilágítottak arra, hogy a károsanyag, azon belül a szén-dioxid kibocsátását mindenképpen csökkenteni kell, nem csak világviszonylatban, de nemzeti szinten is, még hozzá záros határidőn belül.

Ez a csökkentés, több féle képen is lehetséges. Beszélhetünk aktív és passzív csökkentésről.

A passzív csökkentés nem jelent tényleges csökkentést. Passzív csökkentéskor tulajdonképpen nem avatkozunk bele a kibocsátásba, nem redukáljuk azt. Itt a hatásokat próbáljuk mérsékelni. Ilyen mérséklési mód többek között a magasabb kémények építése-ezáltal elősegítik a szén-dioxid jobb és gyorsabb felhígulását a levegőben. De ide sorolható még a kibocsátó kéményekben alkalmazott megkötő szűrők alkalmazása is.

Az aktív csökkentés a tényleges kibocsátás mérséklés, annak elvezetése, kivonása a légkörből, illetve megkötése.

Ma már olyan fejlett technológiák álnak rendelkezésünkre, melyekkel optimálisan megoldható a szén-dioxid föld alá, óceán alá juttatása lekötése, sőt a szén-dioxid kémiai átalakítása-karbamiddá képzése is.

A napi adatokból kiolvasható tendenciák sokszor ijesztőek, ráadásul a globális jelenségek igen összetettek. Mivel az éghajlat kérdése az egész világot befolyásolja, ezért csak és kizárólag nemzetközi összefogással orvosolható.

Olyan konszenzus létrehozásával, mely politikai és gazdasági érdekektől mentes, radikális változásokat eredményezne, és kötelező jelleggel bírna a Föld valamennyi országa számára.

Fő célként az üvegházhatású gázok kibocsátásának csökkentését kell kitűzni, mely elsősorban a szén-dioxid és a metán kibocsátására vonatkozna.

Ez a csökkentés ez emberiség hosszú távú érdekeit szolgálja valamint a fenntartható fejlődést is elősegíti. Ellenben a nemzetközi jogilag kötelező kibocsátás csökkentési megállapodások csak akkor köthetőek és érvényesíthetők, ha a döntéshozók az

elővigyázatosság elvének megfelelően elfogadják azt, hogy a jelenlegi éghajlatváltozás az emberi tevékenységnek tudható be első sorban.

KIOTÓI EGYEZMÉNY

A világon egyre sokasodnak a klímaváltozással foglalkozó kutatások, konferenciák, földcsúcsok, egyezmények. Egyre több ország érzi fontosnak az ezeken való részvételt, illetve az egyezményekhez való csatlakozást.

Az utóbbi idők legjelentősebb ilyen egyezménye az úgynevezett Kiotói Egyezmény, egy 1997-ben aláírt, a fejlett országokat tömörítő, nemzetközi egyezmény, amelyben a résztvevő, iparosodott államok kötelezik magukat arra, hogy széndioxid-kibocsátásukat az aláírást követő évtizedben 5,2 százalékkal az 1990-es szint alá szorítják vissza.

Az egyezmény 1997-es kidolgozása az ENSZ Klímaváltozási Konvenciójának (United Nations Framework Convention on Climate Change (UNFCCC)) keretében történt, célja pedig a légkör üvegházhatású gázkoncentrációjának stabilizálása volt, hogy a klímaváltozás és a globális felmelegedés előrelátható hatásait enyhíteni tudják. Az egyezmény nem léphetett addig életbe, amíg az üvegházhatású gázok kibocsátásának minimum 55%-áért felelős országok nem ratifikálták a szerződést. Az 55%-os küszöböt 2004 őszén sikerült átlépni (Oroszország csatlakozásával) így az egyezmény jogilag 2005. február 16-án lépett életbe.

A kiotói jegyzőkönyv a fejlett országok számára jogi értelemben kötelező célokat határoz meg, és megállapítja emisszió csökkentésük határidejét. Míg a keretegyezményben előírt nem kötelező jellegű vállalás csak stabilizálásra ösztönzi a fejlett országokat, addig a jegyzőkönyv kötelezi őket a csökkentésre.

Ezen csökkentési kötelezettségek mellett más feladatokat is ró a kiotói jegyzőkönyv az államokra. Ezen feladatok a következők (Kiotói jegyzőkönyv 4.1. cikkelyében foglaltak alapján):

- A keretegyezmény szerint mind a fejlődő, mind a fejlett országok elfogadták, hogy lépéseket tesznek az emisszió korlátozására, illetve előmozdítják az éghajlatváltozáshoz való alkalmazkodást;
- Létrehoznak egy nemzeti tervet az üvegházhatású gázok kibocsátásának csökkentésére, és évente készítenek jelentést a végrehajtásról;
- Tájékoztatást adnak nemzeti éghajlatvédelmi programjukról és kibocsátás adatairól, előmozdítják a technológiák átadását, együttműködnek a tudományos és technológiai kutatásban, és támogatják az éghajlatváltozással foglalkozó oktatást, illetve a közvélemény hozzáférését az éghajlatváltozásról szóló információkhoz.

Magyarország 2002 júliusában csatlakozott ehhez az ENSZ által kezdeményezett nemzetközi klímavédő egyezményhez. Hazánk számára a Kiotói Egyezmény de nem az 1990-es hanem az 1985-1987-es bázisidőszakhoz képest 6 százalékos kibocsátás-csökkentést tesz kötelezővé az üvegházhatást okozó gázokra vonatkozóan, a 2008-2012-es évek átlagában. [1]

Ez a lehetőség tulajdonképpen rendkívül kedvező hazánkra nézve, hiszen a rendszerváltást követően összeomlott a tervgazdaság, átalakult a gazdasági szerkezet így tulajdonképpen nagyobb anyagi ráfordítás nélkül sikerül ezt a csökkentési értéket teljesítenünk. Nem kellett gyárakat, üzemeket bezárnunk, fejlett technológiákat vásárolnunk, alkalmaznunk a csökkentés megvalósításának érdekében.

A Környezetvédelmi és Vízügyi Minisztérium (KVM) adatai szerint Magyarország a bázisidőszakban szén-dioxid-egyenértékben kifejezve átlagosan 111 millió tonnát bocsátott ki évente. 2002-ben 75,6 millió tonna volt az emisszió, ami 30 százalékkal kisebb a viszonyítási szintnél.[2] A KVVM prognózisa szerint az elmúlt és az elkövetkező évek gazdasági fejlődése

miatt a kibocsátás folyamatos növekedésére lehet számítani, amelynek nyomán 2010-ben Magyarországról 97,2 millió tonna szén-dioxid kerül majd a légkörbe, azaz még mindig 6,92 százalékkal kevesebb a bázisértéknél.[3]

Ez azt jelenti, hogy jóval a kiszabott csökkentési határ alatt teljest hazánk, így tulajdonképpen hátraléka keletkezik. Felmerül a kérdés, vajon mi lesz a fel nem használt szén-dioxid egységekkel?

EMISSZIÓ KERESKEDELEM

Az éghajlatváltozás kérdése mára nemcsak a környezetvédelem, hanem a gazdaság egésze, a mindennapi élet egyik fő témájává vált. Ugyan még sokan vitatják az emberi tevékenységekre visszavezethető éghajlatváltozás létét (USA egyes kormánykörei), azonban a tudományos bizonyítékok egyre nőnek. Véleményem szerint, a gazdasági eszközök már rendelkezésre állnak, így ha azt vesszük figyelembe, hogy a globális felmelegedés már tényként említhető folyamat, úgy azt a piacgazdaság eszközeinek alkalmazásával kordában kell tartani, illetve amennyiben még lehetséges, meg kell előzni.

A Kiotói egyezmény azt is lehetővé teszi, hogy egy fejlett ország, ha gázkibocsátását (a jobb gazdasági eredmények érdekében) növelni szeretné, akkor egy fejlődő országnak fizessen, hogy tovább csökkentse a gázemissziót.

Azaz a csökkentésre kötelezett ország kibocsátását egy adott évben meghatározzák, és az emisszió csökkentési célt százalékban adják meg. Így az adott ország tudja, hogy milyen nagyságú szennyezési kvótával rendelkezik. Ha az adott ország az előírt kvótánál kisebb mennyiséget bocsát ki, akkor az előírt és ténylegesen magvalósuló kvóta közötti különbséget értékesítheti egy olyan országnak, amely előre tudja, hogy nem lesz képes teljesíteni kötelezettségét.

A fejlett országok így viszonylag könnyedén hozzájuthatnak a "gyengék", a fejlődő országok kibocsátási lehetőségeihez ahelyett, hogy fejlesztéseket eszközölnének, s megszűntetnek pazarló kibocsátásukat. Ezáltal egyre inkább háttérbe szorulnak a technológiafejlesztések és beruházások.

Az ETS-sel (Emission Trading Scheme) az Unió elindította a világ eddigi legtöbb szereplőt magába foglaló kereskedelmi rendszerét. Ezen belül folynak az emissziós tranzakciók. A résztvevő létesítmények száma ma közel 12000. [4]

A direktíva nyomán 2005-től megindult a tagországokban az üvegházhatású gázok kereskedelmének első szakasza, majd 2008-tól a tényleges kereskedés. A direktíva célja az üvegházhatású gázok kibocsátásának költséghatékony és gazdaságilag hatásos módon történő csökkentése. A direktíva két szakaszt különböztet meg:

- Az első szakasz 2005. január 1-től 2007. december 31-ig tartott. Ez az úgynevezett tanulási szakasz, amikor még a feltételek sokkal kevésbé voltak szigorúak.
- A második szakasz 2008. január 1-től kezdődött, és 2012. december 31-ig tart.

Itt már a tényleges feltételek érvényesek. 2012-től várhatóan ötéves időszakokban fog a kereskedés bonyolódni.

Magyarország szinte az elsők között kezdte meg a kereskedelmet, (összesen 15-25 millió tonna szén-dioxid kvóta értékesítésére kapott engedélyt) melyben első partner országunk Belgium volt. Megközelítőleg 2 millió tonna került eladásra.

A mai napig (2009.10.24.) Magyarország Belgium mellett csak Spanyolországnak értékesített kvótát, 2008 novemberében, több mint 6 milliót. A Point Carbon legfrissebb értesülései szerint azonban a Spanyolországnak eladott pontos mennyiség 6,6 millió tonna.

A fenti adatok és a tranzakciók lebonyolításakor aktuális árfolyamok alapján tehát valószínű, hogy egy tonna szén-dioxid-kvótát átlagosan 13,5-14,5 eurós áron tudtunk értékesíteni. Eddig a legmagasabb ár, amit kiotói kvótáért egy kormány ki tudott alkudni, 10 euró volt.

A felek érdekeire hivatkozva eleinte az adásvétel részleteit, annak pontos összegét nem hozták nyilvánosságra, ellenben elmondták, hogy az így befolyt összeget lakóépületek és középületek energiahatékonyságának javítására fogják használni. Ezt nevezzük ZBR rendszernek.

(Azóta nyilvánosságra került a kereskedelmünkből befolyt összeg értéke, mely megközelítőleg 28,2 milliárd forint.)

VÉLEMÉNYKÜLÖNBSÉGEK

Tanulmányom egyik nem titkolt célja, az volt hogy felderítsem az önkormányzati illetve az önkéntes társadalmi csoportok, szervezetek véleményét a globális klímaváltozásért vívott harcban, az emisszió csökkentés érdekében végzett törekvéseik tükrében.

Ennek érdekében két rendkívül jelentős, de eltérő álláspontot kívánok ütköztetni egymással, melynek célja az ellentétek feloldása egy pártatlan állásfoglalás kialakításával.

Elsőként a Greenpeace Hungary-t kerestem fel, majd a Környezetvédelmi és Vízügyi Minisztérium (később Vidékfejlesztési Minisztérium) válaszreakcióira valamint véleményére voltam kíváncsi.

Mind két szervezetnél ugyanazokat a kérdéseket tettem fel, mindamellett természetesen a Környezetvédelmi és Vízügyi Minisztériumtól, a Greenpeace feltevéseinek, kérdéseinek megválaszolását is reméltem.

(A kérdések 2009.07.01. és 2009.09.03. között kerültek megválaszolásra így előfordul, hogy jövő időben említek olyan eseményeket, amelyek 2009.október 31. óta már bekövetkeztek, eredményeik, hatásaik ismeretesek. A cikk végén kitérek ezen változásokra.)

Greenpeace

Elsőként a Greenpeace szervezetét látogattam meg ez ügyben.

A szervezet kiemelten foglalkozik az üvegházhatást elősegítő gázok csökkentésével valamint, az ebből adódó globális éghajlatváltozás problémájával. A téma élharcosaként, néha drasztikusabb, figyelemfelkeltő módszerekkel, demonstrációkkal igyekszik felhívni a lakosság illetve a mindenkori kormány figyelmét erre a sürgető globális problémára.

Soron követi Magyarország szerepvállalását a Kiotói egyezményben, annak teljesítési feltételeinek betartását, betartatását, a kvótakereskedelmet, a kereskedelemben részt vevőket, az emisszió kereskedelem címén befolyt összegeket, azok további sorsát.

Mint azt már az előbbiekben említettem, aktivistái többször demonstráltak már ez ügyben. Legutoljára 2009.06.17-én, amikor Greenpeace aktivisták (20fő) sátrakat állítva tábort ütöttek a Minisztériumi Hivatal bejárata előtt. Céljuk az volt, hogy hírt kapjanak végre, megvárják, amíg a kvótakereskedelemből származó 28,2 milliárd forintra kiírják a zöld pályázatokat.

Szerettem volna többet megtudni a demonstráció okairól, eredményeiről, de legfőképpen a Greenpeace véleményét a Kiotói egyezményről, kvótakereskedelmünkről ezért felkerestem a Greenpeace Hungary Klíma és Energiakampány Koordinátorát, Stoll Barbarát.

Elmondása szerint a demonstráció egy jelképes/szimbolikus csendes figyelemfelkeltés volt. Még a demonstrációt megelőzően a szervet többször küldött hivatalos levelet előbb Gyurcsány Ferenc miniszterelnök Úrnak, majd később Bajnai Gordonnak. A levél tartalma a

ZBR rendszer késlekedéséről kérdezte a miniszter Urakat. Stoll Barbara elmondása alapján a válasz a mai napig nem érkezett meg, egyik kormányfő részéről sem.

Egy másik demonstrációt kiváltó okként említette, hogy Szabó Imre Környezetvédelmi miniszter bejelentését miszerint, a gazdasági világválságra való tekintettel a 2009-es kereskedelmi pénz, azaz a 28,2 milliárd egy részét visszatartják.

Nem kiváltó okként, de okot erősítő hatásként említethető, a Japánnal való kvótatranzakció elbukását, melyet nem hivatalos források szerint, azért nem tudott hazánk tető alá hozni, mert a Japán vezetése nem bízott, az ahogy ők nevezték „hiteltelenné vált Magyarországban", féltek, hogy nem tudjuk majd teljesíteni a szükséges csökkentést, illetve véleményük szerint Magyarország túl sokszor módosította a szerződési feltételeket.

Természetesen mondanom sem kell, hogy egy olyan „gazdaságilag fejlett" fejlődő ország, mint Japán további fejlődése érdekében jelentős összegű bevételt áldozott volna a tranzakció megvalósulása érdekében.

Természetesen a ZBR rendszer elindulása mellett, az addíciós bevételek holléte is foglalkoztatta az aktivistákat, hiszen a Kiotói egyezményben foglaltatik, hogy az így beszedett összegeket az országoknak saját környezetük védelmére illetve a globális klímaváltozás megakadályozására kell felhasználni, és mivel Magyarország kvótatöbblete a rendszerváltás következtében, mondhatni erőfeszítés, anyagi ráfordítás nélkül keletkezett nincs szükség arra, hogy ezt a pénzt a csökkentési munkálatok utólagos kifizetésére bocsássák.

Mivel mindezidáig semmit sem lehet tudni a 28.2 milliárd hollétéről, féltek attól, hogy a bevétel teljes egészében már nem is áll rendelkezésre. „Mint hogy ez egy komoly összeg, félő, hogy a kormány bizonyos költségvetési lyukak betömésére használja."Barbara elmondása szerint elsősorban ezek az okok vezettek az aktivisták demonstrációjához, melynek véleménye szerint részben meg is lett az eredménye, hiszen 2009 augusztusában megindult a ZBR rendszer.

(A Greenpeace az elszámolási kötelezettséget nem a Környezetvédelmi és Minisztériumi Hivataltól, hanem a mindenkori kormánytól, annak miniszterelnökétől várja. Véleménye szerint a leginkább „érdekelt" a kvótakereskedelem akadálytalan haladásának vontatottá tételében Szabó Imre Környezetvédelmi Miniszter. A Környezetvédelmi minisztériumot csak az érdekütköztetések elszenvedőjének tartja.)

Kíváncsi voltam a szervezet véleményére a Kiotói jegyzőkönyvről, Magyarország jelenlegi klímaváltozásra való reagálásáról, természetesen a jegyzőkönyv tükrében.

Barbara első mondatára szinte számítani lehetett. Véleménye szerint ez a jelenleg agregált 5,2%-os kibocsátás csökkentés semmire sem elég.

„Ez az 5.2%-os csökkentés nem szignifikáns, hiszen ma már tudományos kutatások bizonyítják, hogy ahhoz, hogy egyáltalán szinten lehessen tartani az üvegházhatású gázok kibocsátását legalább 40-50%-os csökkentésre volna szükség és itt csak szinten tartásról beszélünk". Mindamellett hozzátette: „A pozitívum a negatívumok mellett, hogy a jelenlegi feltételek mellett a Kiotói egyezmény teljesíthetőnek látszik".

A másik nagy problémának, (vagy nevezhetjük a Kiotói egyezmény gyenge pontjának) az úgynevezett klímaigazságosságot tartja. Pontosabban annak hiányát a fejlődő és fejlett nemzetek tekintetében.

Véleményük szerint a fejlődő országokat teljesen más aspektusból kellene megközelíteni. Jelenleg senkinek sem áll jogában a fejlődő országoknak, fejlődésük rovására, jelentős káros anyag kibocsátás csökkentésre kötelezni őket. Főként nem akkor, ha tudatában vagyunk annak, hogy a jelenlegi hatalmas emissziós növekedés egy jelentős részét tulajdonképpen mi magunk (fejlődő országok) generáltuk, hiszen az ipari forradalom után megindult hihetetlen

gazdasági fejlődésből csak „mi” profitáltunk, ellenben a környezetre káros hatásokat a fejődő országok is érzékelik.

Álláspontjuk szerint sem a Kiotói egyezmény, sem a kvótakereskedelem, sem pedig a magyarországi úgynevezett „helyzetkezelés” nem elég hatásos, nem elég eredményes, célravezető.

A Kiotói jegyzőkönyvben rengeteg jogi kiskaput, kibúvót hagytak a jegyzőkönyv szerkesztői, melyet a benne szereplő országok jócskán ki is használnak. Leginkább érzékelhető ez a flexibilis mechanizmusokban.

És természetesen itt van még a már említett klímaigazságosság kérdése.

Véleményük szerint a gazdasági érdekek függvényében, különböző vonatkozási rendszert kell kiépíteni az országoknak aszerint, hogy a fejlett vagy fejlődőek csoportjába tartoznak.

A fejlett országoktól jelentősen nagyobb százalékos csökkentést jogi úton kellene kötelezővé tenni, míg a fejlődő országoktól az úgynevezett BAU állapottól (a mindenkori normális, optimális állapot) egy minimum 20%-os eltérést, változást remélnek.

A szervezet szerint azonban mindez, minden csökkentési – klímaváltozást megelőző feladat, nem ér el jelentős eredményeket, ha a Föld két legnagyobb kibocsátó nagyhatalma (USA, Kína) nem írja alá az egyezményt.

Végül, de nem utolsósorban beszélnünk kell az egyre agresszívebb mértékű erdőirtásokról. Napjainkban rengeteg erdőt, erdőséget irtanak ki szüntelenül. Gondoljunk csak az indonéziai térségre vagy a Kongó-medence területeire.

Ma már szintén jelentős tudományos kutatási eredmények bizonyítják azt a tényt, miszerint ha nem irtottunk volna ki ilyen hatalmas mennyiségű fát, ez esetben ez a bizonyos mennyiségű növényzet a jelenlegi káros anyag kibocsátás körülbelül 20%-át elnyelte volna.

Környezetvédelmi és Vízügyi Minisztérium (később Vidékfejlesztési Minisztérium)

Természetesen a Greenpeace-nél tett látogatásom után mindenképpen szerettem volna megtudni a Minisztérium véleményét is, szerettem volna válaszokat kapni a kérdéseimre, ezért felkerestem a Környezetvédelmi és Vízügyi Minisztérium Nemzetközi Kapcsolatok és Klímapolitikai Főosztályának munkatársát Szabó Kingát.

Kérdéseimre nagyon szűkszavúan, vagy egyáltalán nem válaszolt. Elmondása szerint szinte minden pont tartalma, melyre választ szerettem volna kapni, titkosított információ, mely csak szakállamtitkári engedéllyel adható ki, különös tekintettel a kvótakereskedelemre.

Néhányat közülük még titoktartási nyilatkozat ellenében sem ismertethetett velem.

Kíváncsi voltam, miért ez a nagy titoktartás és hol van az egyének az információhoz való joga.

Elismerte, hogy a rendszerrel maga sem ért egyet, mint állampolgár, de mint minisztériumi dolgozó kötelessége betartani a szerződésében foglaltakat.

Mint, ahogy azt megtudtam a titkosítások elsődleges oka a versenyrendszer fenntartása, valamint a Belgiummal és Spanyolországgal kötött kvótaeladási szerződésbe iktatásra került egy titoktartási záradék, mely értelmében a résztvevő felek nem adhatnak ki semmilyen információt az adás-vétel részleteiről.

Megkérdeztem, hogy akkor az általam korábbiakban említett (5.3 fejezet: Magyarország kvótakereskedelem) kereskedelmi adatok, hitelesek-e. Valóban igaz-e az, hogy Belgiumnak megközelítőleg 2 millió tonnát, míg Spanyolországnak 6,6 millió tonnát adtunk el?

„Az adatok körülbelüli értékek, nagyon közel állnak az igazsághoz. Szabó Imre Környezetvédelmi Miniszter Úr egyik sajtótájékoztatón történt „elszólása” szolgáltatott ennek alapot- mondja Kinga.

Néhány kérdésemre azonban, ha nem is részletesen, de megadta a választ (természetesen rendkívül óvatosan fogalmazva).

Elsőként a Kiotói egyezményről, annak gyenge pontjairól beszéltünk. Mint ahogyan az kiderült, a minisztérium gyengepontnak tekinti, hogy USA nincs a tagországok között, illetőleg, hogy nem működik optimálisan az ellenőrző rendszer, túl sok a jogszabályi hézag, nem elég szabályozottak a lehetőségek.

A kvótakereskedelmi rendszer kérdésköréből annyit sikerült megtudnom, hogy az eladásokból beérkezett, befolyt összeg ,állításuk szerint teljes egészében rendelkezésre áll, és igaz ugyan hogy egy ideig a gazdasági világválságra való tekintettel a Környezetvédelmi Miniszterelnök zároltatta az összeg egy részét, de azóta az is feloldásra került.

„Ezen bevételt teljes egészében a ZBR rendszer beindítására költik majd"- állítja Szabó Kinga. [5]

Szerettem volna választ kapni arra a kérdésemre is, miszerint a Japánnal való tárgyalások Magyarország hiteltelenné válása, a szerződési feltételek folyamatos módosítása miatt nem jött-e létre.

Sajnos ezt az információt sem adhatta ki részemre, ahogyan azt sem, hogy jelenleg folynak-e tárgyalások más országokkal kvótakereskedelmi ügyben.

Arra a kérdésre azonban készséggel válaszolt, hogy „Vajon mi várható a jövőben?".

A várható emissziós csökkentési érték növekedést hazánk elfogadja, és betartja majd, amely mintegy 30%-os csökkentést eredményez. Ez az érték 2020-ra 50%-ra nő majd.

Magyarország támogatni fogja azt a kezdeményezést miszerint a légi, illetve tengeri közlekedést is be kell vonni az emissziós kibocsátási értékek alá, ennek vonzataként, ezen a területen is visszaszorítások szükségesek.

Záró témaként USA szerepéről, annak a klímaváltozásban való szerepvállalásáról esett szó.

„Reményeink szerint, és mivel Obama elnök első három legfontosabb feladata közt tartja számon a klímaváltozás elleni védekezést, USA részt vesz majd, részt vállal a Koppenhágai egyezményben.

A beszélgetés végén még egy utolsó kérdést intéztem Szabó Kingához, még pedig az idei júniusi Greenpeace demonstrációról való álláspontját szerettem volna megtudni.

„Véleményem szerint a demonstráció külső szemmel nézve jogosnak mondható, hiszen az információ hiány a (sokszor alaptalan) találgatások melegágya. Érthető a nyugtalanság, de eredményre nem vezet."

A két szervezet álláspontját megismerve, véleményütköztetést szerettem volna végezni.

Sajnos a Minisztériumtól kapott információ elenyészően kevésnek bizonyult ehhez így a konzekvencia levonását az olvasóra bízom.

Azonban egyet kell értenem a Greenpeace nézőpontjával, abból a szempontból, miszerint az egyénnek joga van az információkhoz. A Minisztérium titoktartási politikája alapot adhat azon félelmek beigazolódására, miszerint a kereskedelemből származó bevételek nem állnak teljes egészében rendelkezésre.

Legnagyobb problémaként az információk visszatartását látom.

Ellenben nem szabad elfelejteni, hogy a hazánkat érintő összes környezetvédelmi, környezetbiztonsági kérdésben nem a különböző társadalmi, önkéntes szervezetek, hanem a Környezetvédelmi és Vízügyi Minisztérium dönt. És hazánk részvétele a különböző klímapolitikai konferenciákon, egyezményekben rendkívül kielégítő.

ÖSSZEGZÉS

Pályaművem fő kérdésköre a Kiotói egyezmény és annak utóélete volt. Ez időszak alatt e kérdéskörben lényegi változás nem történt.

Ugyanez a Koppenhágai Klímacsúcsra már nem mondható el. A konferencia végkimenetelét illető jóslataim beigazolódtak. A konferencia jelentős eredmény nélkül zárult, USA és Kína kihátrálásával.

Azóta a Mexikói konferencián is túljutottunk ahol áttörésről ugyan nem beszélhetünk, de mindenképpen pozitív eredménnyel zárult ez a klímacsúcs, hiszen végül megegyezés született. Több kulcskérdésben is előrelépés történt, azonban a mostani egyezség csak egy kiindulási alap, amire építve a jövő évi dél-afrikai konferencián egy megfelelő, jogilag kötelező megállapodás születhet.

Az eredmény: 25-40 százalékos kibocsátás-csökkentés, két fok alatt tartott globális felmelegedés (természetesen még nem megvalósítva, de legalább közös célként kijelölve).

Japán és az Amerikai Egyesült Államok most sem vállalt szerepet az egyezményben, hiszen az elviekben a klímaharc mellett elkötelezett Obama-kormányzat a 2005-ös évhez viszonyítva 17 százalékkal szorítaná le kibocsátását, (ami az 1990-es szinthez képest mindössze 4-5 százalékos csökkenést jelent) továbbá egyértelműen nem támogatják még a megállapodást Oroszország és a fejlődő országok, mint például Kína vagy India.

Kvótaeladás ügyben sem történt előrelépés. A hazai kvótabotrány bírság nélkül zárult. Új kvótafelvásárló partnert nem szerzett hazánk, azonban Japánt további egységeket vásárolt. Így összességében Magyarország eddig Spanyolországnak, Belgiumnak és egy japán cégnek adott el összesen 11,6 millió tonna szén-dioxid-kvótát 31,2 milliárd forintért.

Pályamunkám lezárásakor a hazai klímatörvény általános vitára alkalmas állapotban volt. Az Egyesült Királyság után másodikként Magyarországnak lehetett volna klímatörvénye. Ez a lehetőség azonban most egy időre elúszott. (Bár a környezetvédelmi bizottság 2010. február 15.-én általános vitára alkalmasnak találta az éghajlatvédelmi kerettörvényt, február 22.-én az MTI már arról számolt be, hogy az MSZP frakcióülésén 30:28 arányban elutasította, hogy kezdeményezzék a kerettörvény-tervezet tárgyalásának folytatását. A döntés hónapokra elhalasztja a kerettörvény elfogadását, mivel az Országgyűlés legközelebb csak az áprilisi választások után, immáron új felállásban ül össze.)

Magyarország korábbi „titkolózó" klímapolitikájával kapcsolatban mi sem bizonyítja jobban pályaművem aktualitását, időszerűségét, mint hogy megírását követően néhány hónappal az Energia Klub Környezetvédelmi Egyesület a kiotói egységek értékesítéséből befolyt bevételeknek a Zöld Beruházási Rendszer (a továbbiakban: ZBR) keretében történő felhasználásának vizsgálatát kérte a Jövő Nemzedékek Országgyűlési Biztosától.

És míg az én válaszaimra nem, addig ennek eredményeképpen sok számomra ismeretlen információra derült fény. Ennek eredményei a:

http://www.kvvm.hu/cimg/documents/Reszletes_eszrevetelek_.pdf-es internetes oldalon olvashatók. Azóta a minisztérium, mely ma (2011.01.03.) a Vidékfejlesztési Minisztérium nevet viseli, már nyitott környezet-klímapolitikát folytat. Honlapján nem csak a kvótakereskedelemi partnereink, de a kvótaárak[2] – bevételek - kiadások is helyet kapnak, azonban mindez kódszámot visel, mely sajnos a laikus lakosság számára egyenlőre még érthetetlen.

Ennek eredménye talán a Greenpeace Hungary és a minisztérium, továbbra is negatív kapcsolata. Míg előbbi radikális nézeteivel, addig a másik (állításuk szerint) lekövethetetlen politikájával váltja ki a másik szervezet ellenszenvét.

[2] Magyar CER kvóták listája letölthető: http://www.kvvm.hu/index.php?pid=1&sid=1&hid=2581

Természetesen a legoptimálisabb az lenne, ha a minisztériumi és az úgynevezett „zöld szervezetek” kompromisszumra jutnának, de az eredményes hazai klímapolitika talán a jelenleg is meglévő negatív kapcsolattal jár a legjobban, (mert mint azt korábban említettem) még akkor is, ha e két szervezet ellentétes nézőpontjaival, egymást szemmel tartva, felülvizsgálva, motivációs jelenségként hat egymásra.

Ezen eredmények tudatában, továbbra is fenntartom minden következtetésem, javaslatom, főként a legutolsó pont tartalmát, miszerint szükséges hazánkban egy független információs szervezet, fórum létrehozása (mely nem egyezik meg a lakossági fórummal.) Egy olyan információs szervezet, iroda megléte szükséges mely független kapcsolatként szolgálna a zöld szervezetek és a minisztérium között, és melynek célja nem az érdekütköztetés, hanem az érdekegyeztetés-érvényesítés.

BEFEJEZÉS

Egyre több tényt ismer meg a közvélemény az éghajlatváltozásról. A Kilimandzsáró havának elolvadása, a turistaszezonok több hetes eltolódása, a tengerparti települések elsüllyedése, a szélsőséges időjárás, vagy „válaszlépésként” a síparadicsomokban egyre divatosabb hóágyúk, mind kedvelt témái a napi sajtónak.

Arról azonban lényegesen kevesebb szó esik, hogy az érintettek mit tehetnének az éghajlatvédelemért. Az emisszió jelentős csökkentésére, miért nincs a szektoroknak világos stratégiája, miért nem adaptálják a nemzetek lakosaikba a környezettudatosabb életmód jótékony, megelőző hatásait?

Környezetünk minden része egy örök körforgási folyamat eleme, melyben elég egy apró eltérés ahhoz, hogy az visszafordíthatatlan károsodást eredményezzen.

Irodalomjegyzék

[1] Láng István: KvVM-MTA-„VAHAVA” Projekt összefoglalása: A magyarországi klímapolitika alapjai, Budapest, 2006. (27.oldal)

[2] „Klíma-21” Füzetek, Klímaváltozás – Hatások – Válaszok 2008. 52.szám: Magyarország szén-dioxid mérlege BIOME-BGC modellel (83.oldal)

[3] KvVM-MTA-„VAHAVA” Projekt összefoglalása: A magyarországi klímapolitika alapjai, Budapest,2006. (32.oldal)

[4] Nemzeti Kiosztási Terv http://www.kvvm.hu/cimg/documents/NKT2_061020tars_vit.pdf

[5] A magyar kormány 2206/2000. (IX.13.) számú határozata, http://www.greenfo.hu/hirek/hirek_item.php?hir=197

Készült a Somos Alapítvány támogatásával.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Juhász Zsolt
juhaszzsolt@gmail.hu

COMPARISON OF QUALIFICATIONS AND CONSTITUTIONAL INDEXES OF CATEGORIES T3 AND T4 IN THE CIRCLE OF THE HUNGARIAN ARMY'S STAFF APPLYING FOR FOREIGN SERVICE
(01.01.2007 – 31.12.2010.)

Absztrakt

A fizikai erőnléti állapot következetes és rendszeres vizsgálata a különböző külföldi beosztások eltérő sajátosságai, valamint az emberi szervezetre gyakorolt eltérő jellegű és mértékű negatív hatásai miatt, egyre nagyobb jelentőséggel bír. Írásomban mindezek tükrében a külszolgálatokra jelentkező személyi állomány négy év alatt mért minősítései és alkati mutatói közötti összefüggéseket kerestem. és azok segítségével, a teljesség igénye nélkül igyekeztem egy átfogó képet adni a magyar haderő 2007 és 2010 között megvizsgált külszolgálatra jelentkező állományának fizikai erőnléti állapotáról.

A consistent and regular test of physical condition owing to the different characteristics of diverse foreign military posts, as well as to their negative effects of different kinds and grade taken on human body is being of more and more importance. In my study reflecting all these I looked for a connection between the qualifications and constitutional indexes of the staff applying for foreign service measured during four years. By dint of all these figures I tried to give a comprehensive picture of the physical condition of the Hungarian Army's staff applying for foreign service in the period of 2007-2010, without aiming at completeness.

Kulcsszavak: *alkati tényezők, fizikailag alkalmas, fizikailag alkalmatlan, külszolgálat ~ constitutional indexes, physically fit, physically unfit, foreign service*

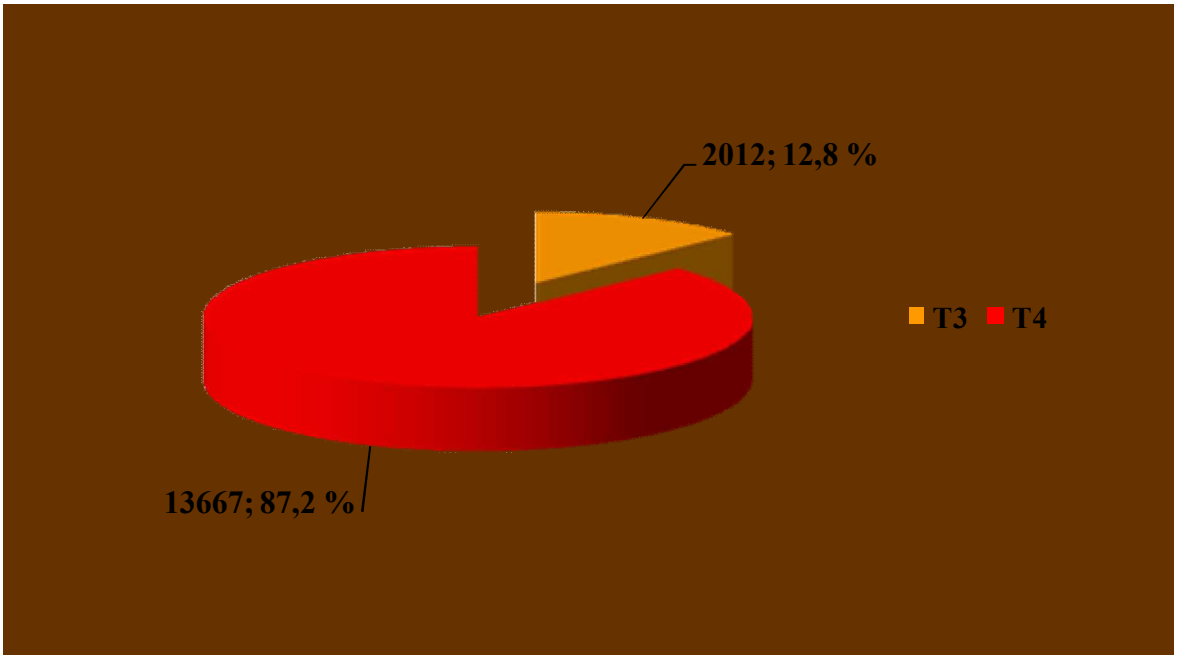
INTRODUCTION

The physical aptitude test inside the three-way medical check-up system represents an extremely important field similarly to other medical and psychological ones. Namely it is indispensable for carrying out foreign tasks successfully to have a number of such basic and specific physical motor faculties, the improper development of which can endanger the health condition of the soldiers, and thus of course it may even risk the successfulness of the military mission, as well.

So must be both psychological and physical capacities of the body developed, and then they have to be kept on the same level, too. In fact the aim is not else but to create harmony in body and spirit, and afterwards its continuous maintenance. Therefore the physical aptitude test is making its way more and more to the direction that beyond measuring the basic conditioning faculties (strength, speed and stamina) also other specific abilities characterstic mostly of missionary activities and closely tied to those ones should be scrutinized. Should we keep in view the principle of progressivity and should be the above-mentioned motor capacities developed also under extreme wheather conditions, so may the chance increase, according to which the performance of our soldiers also in foreign service remains undiminished or decreases slightly.

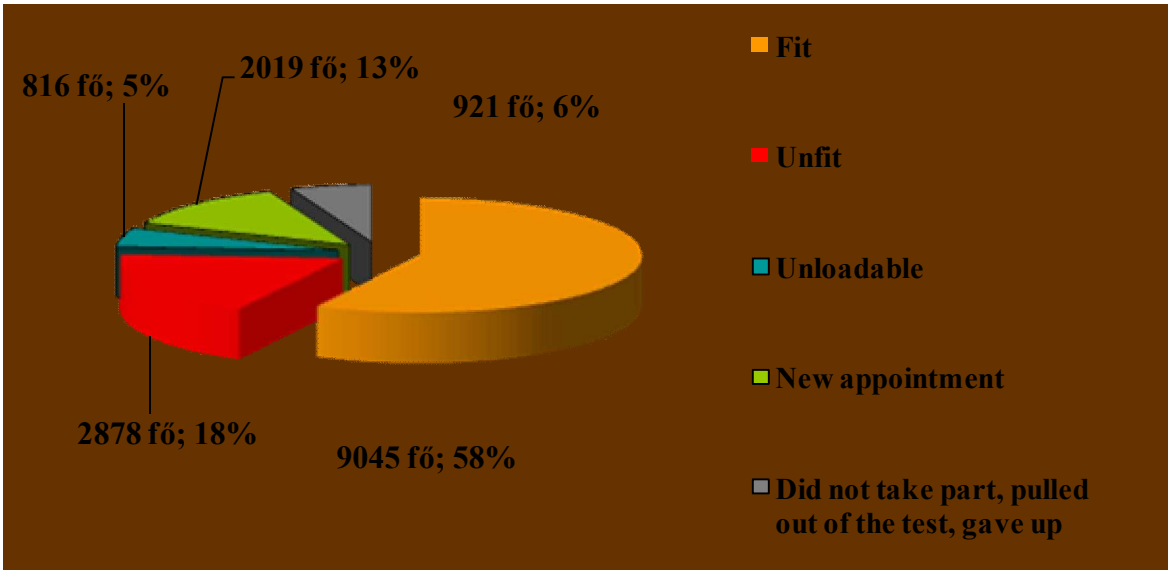
COMPARISON OF QUALIFICATIONS AND CONSTITUTIONAL INDEXES OF CATEGORIES T3 AND T4

Between 01.01.2007. and 31.12.2010. there were *15.679 professional and contractual* male soldiers ordered in by the Military Physical Aptitude Testing Department and by the Medical Physiological Department to the physical aptitude test required to their missionary service.



1. figure. Distribution of military male staff into T3-T4 ordered in to missionary medical tests; (n=15.679 persons) [1]

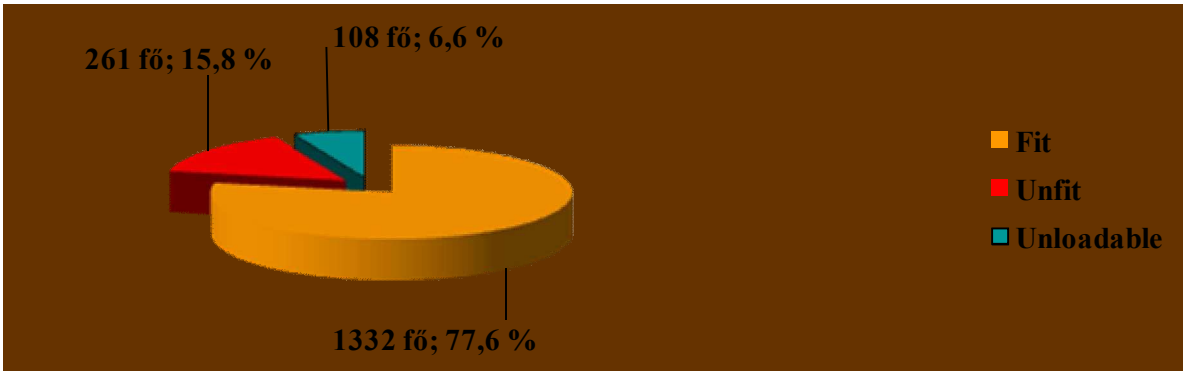
A considerable part of the staff, nearly *90%* - in accordance with the Military Order 7/2006 (III.21.) applied for military posts required extended tough condition, marked „T4". A minor part of them applied for posts required increased tough condition marked „T3". (Figure 1.)



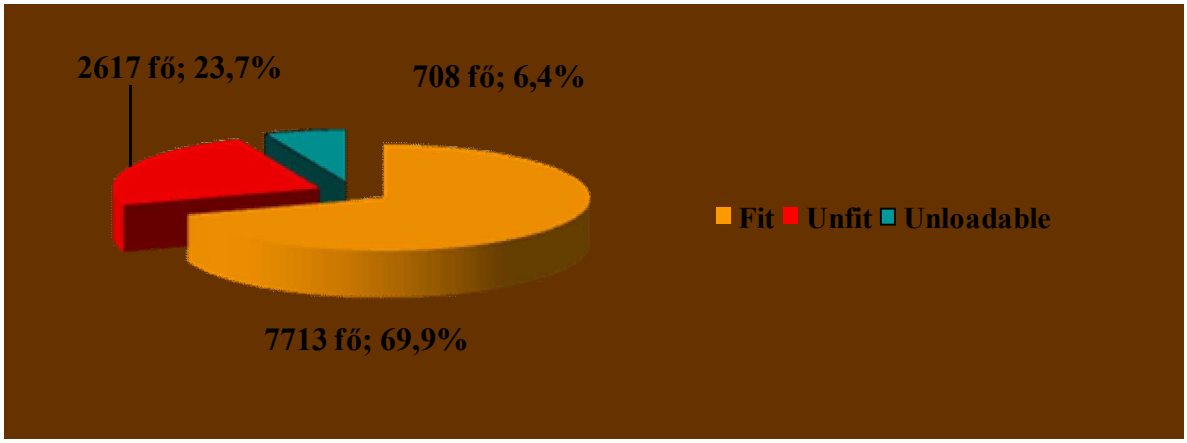
2. figure. Distribution of the military male staff „T3"-„T4" ordered in to missionary medical tests according to the qualifications between 01.01.2007-31.12.2010. (n=15.679 persons) [2]

As regards qualifications *58%* of the staff were declared *„Physically fit"***,** and *18%* were qualified *„Physically unfit"*. For health reasons *5%* of the persons ordered in *was not to be loaded.* (Figure 2.)

Alltogether *11.923 persons* took part in the tests in fact, which meant *75%* of the staff *ordered in* at the period of reference, and only *24,1%* of that got the qualification *„Physically unfit"*.



3. figure. Distribution of the military male staff „T3" appeared on the missionary medical tests on the basis of the qualifications between 01.01.2007–31.12.2010. (n=1.701 persons) [3]



4. figure. Distribution of the military male staff „T4" appeared on the missionary medical tests on the basis of the qualifications between 01.01.2007-31.12.2010. (n=11.038 persons) [4]

Average age of the staff marked „T4" with the requirement „extended tough condition" [5] was *30,3* +/-5,3 years, *that* of the staff of *„T3"* was *34* +/- 6,0 years (p<0,001). Body-mass and Body-mass Index of *„T3"* was significantly higher (p<0,001) than those of *„T4"* (*85,5*+/-12,5; *82,0* +/-12,2 kg, or rather *26,7* +/- 3,5; *26,0* +/- 3,4 kg/m^2), their body height was 178,8 +/- 0,6 and 177,5 +/- 6,9 cm alike.

77,6% of the *staff „T3"* required „increased tough condition" [6] was *„Physically fit"*, while in case of *„T4"* it was only *69,9%.* Distribution of the staff of not to be loaded was in both categories alike, but of the *„T4"* the number of the *„Physically unfit"* was *(23,7%)* was higher compared to that of *„T3" (15,8%)*. (Figures 3-4.)

On the basis of the data and figures obtained it is alltogether to be ascertained that only 58% of *the total staff „T3-T4" ordered in (15.679 persons)*, and 70% of the staff appeared and tested in fact was *„Physically fit"*.

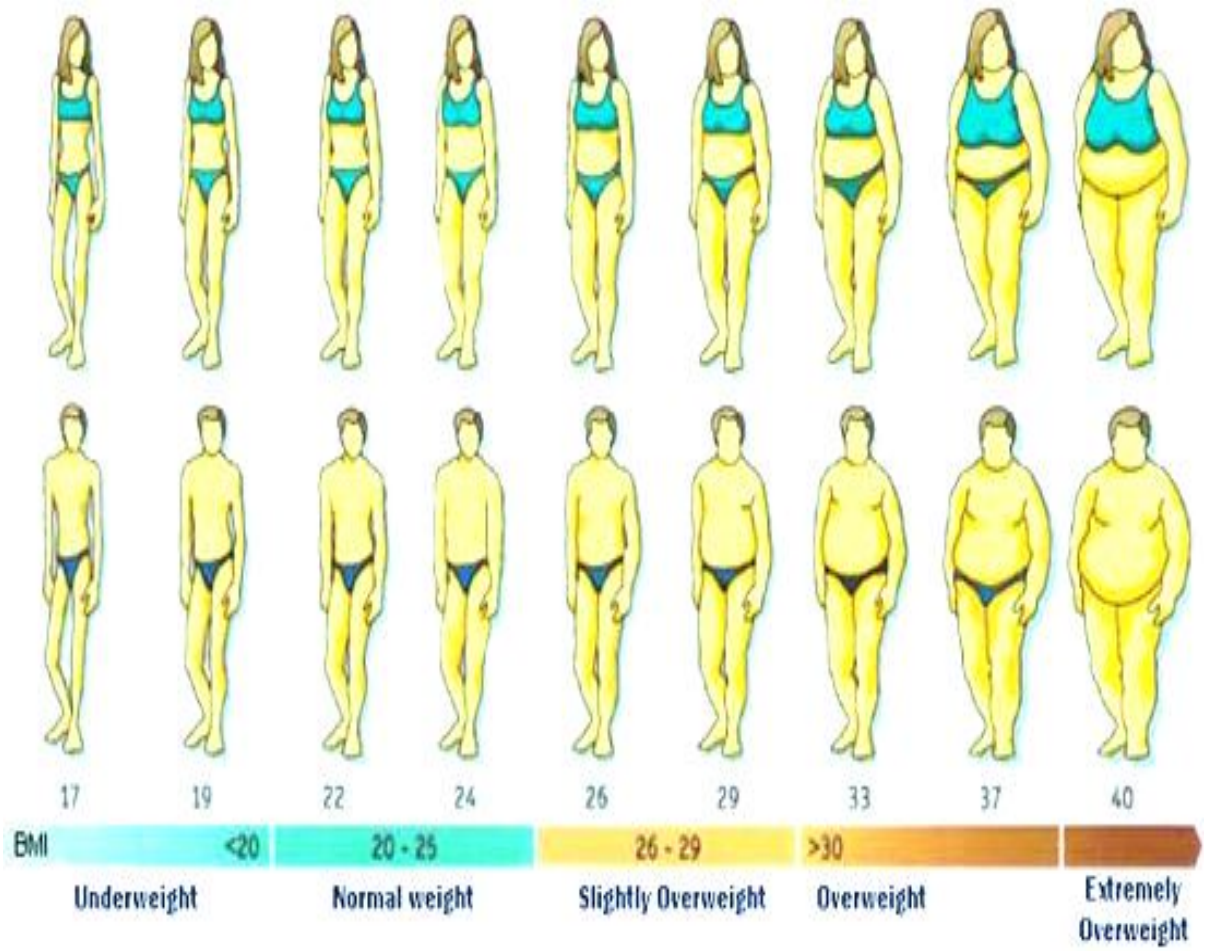
Testing anthropometrical indexes

„b) For a more precise quantity determination of obesity degree it is Body-mass Index (BMI) used. By Body-mass Index (BMI) fat excess is more accurately reflected. BMI is so calculated that body weight measured in kg is divided by the square of the body height measured in meter. „Normal" BMI is, as follows: 18,5-24,9 kg/m^2.

Degree of overweight and obesity:

BMI	WHO
• <18,5	lean
• 18,5-24,9	normal
• 25,0-29,9	overweight
• 30,0-34,9	Obesity I
• 35,0-39,9	Obesity II
• > 40,0	Obesitiy III

c) Degree of obesity may serve us merely as informative data. Final qualification can be given only after being evaluated the individual load-bearing capacity, as well as over 25,0 BMI according to the determination of body-fat percent." [7]

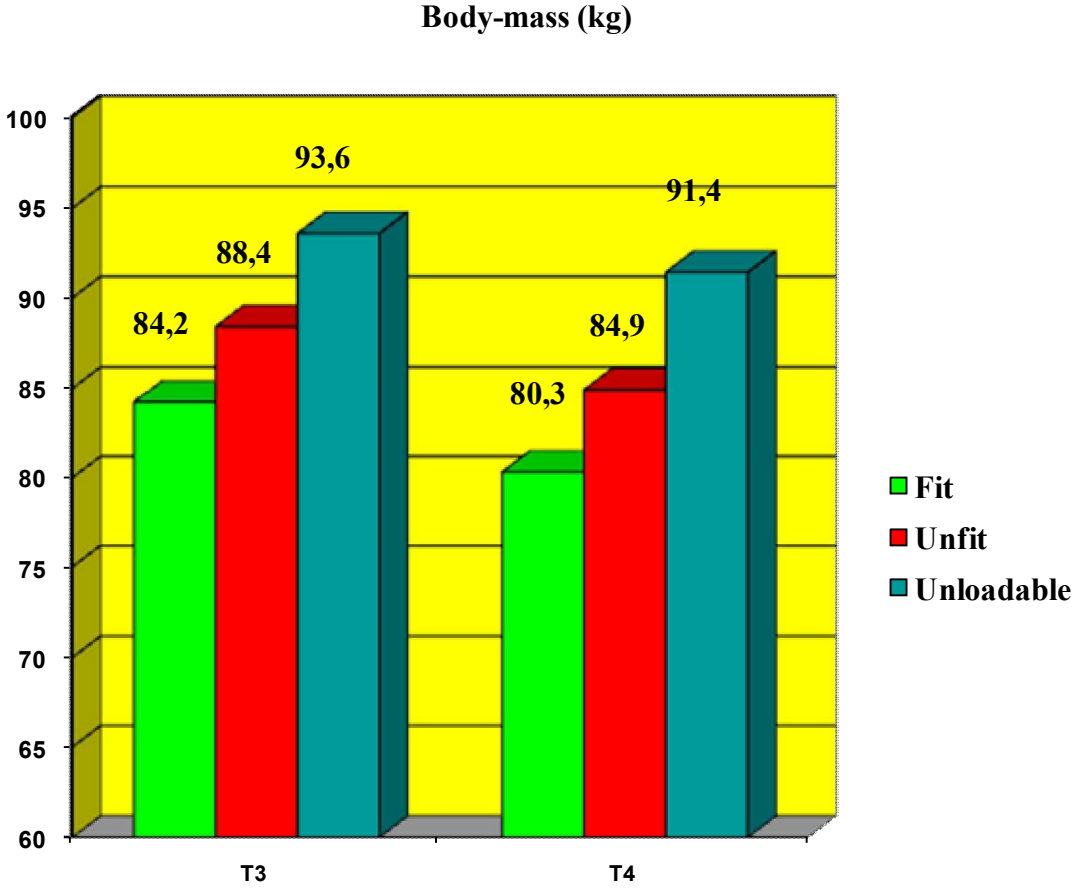


Lean	Normal	Overweight	Obesity I	Obesity II	Obesity III

5. figure. About morphological changes taken as a function of BMI values [8]

Body-mass testing

In the course of body-mass testing we found a clear difference not only between the examination categories (T3-T4) but also inside them there was an expressed difference between the groups *„Fit", „Unfit"* and *„Unloadable".* (Figure 6.) Both in the category of *„T3",* and that of *„T4"* the *„Unfit"* and the *„Unloadable"* had a significantly higher body mass ($p<0,001$) compared to the category *„Fit".* The body-mass of the tested persons *„Unloadable"* was significantly higher ($p=<0,001$) compared to that of the *„Unfit".* At the same time comparing body mass of the same qualified groups to those of *„T3"* and *„T4",* so will the staff *„T3"* possess a significantly higher value ($p=<0,001$).



6. figure. Distribution of the average body-mass of „T3"+ „T4" in terms of the qualifications between 01.01.2007-31.12.2010. (n=12.739 persons, male) [9]

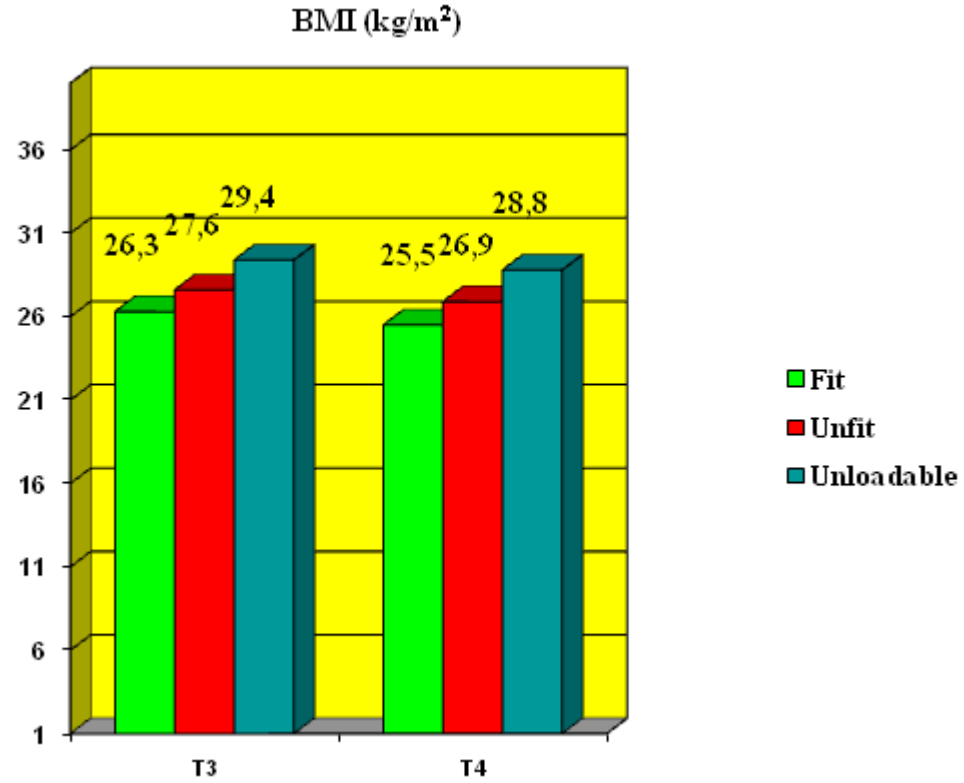
Average body-mass of the staff qualified *„Fit"* belonging to the category *„T3"* was *84,2* +/-12,2kg, that of the *„Unfit"* was *88,4* +/- 12,1 kg, and that of the *„Unloadable"* was *93,6* +/- 15,4 kg. (Figure 6.)

In contrast to that body-mass of the soldiers qualified *„Fit"* belonging to the category *„T4"* was *80,3* +/- 11,3 kg, that of the „Unfit" was 84,9 +/-12,5 kg, and that of the „Unloadable" was *91,4* +/-15,1 kg. Difference of the average body-mass of *„T3-T4"* with the qualification „Fit" was 3,9, that of the *„Unfit"* was *3,5* and that of the *„Unloadable"* was 3,2 kg.(Figure 6.)

BMI (Body-mass Index) test

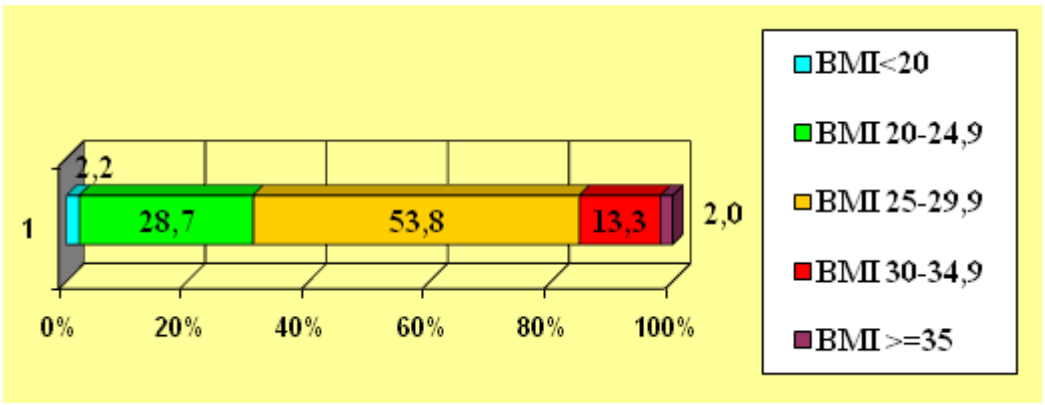
In the course of BMI a gradual rise similar to body masses was to be observed both inside the groups and after being compared the two categories.

Value of the average BMI of the staff qualified *„Fit"* belonging to the category *„T3"* was *26,3* +/- 3,3, that of the *„Unfit"* was *27,6* +/- 3,3 and that of the *„Unloadable"* was *29,4* +/- 4,5. (Figure 7.)



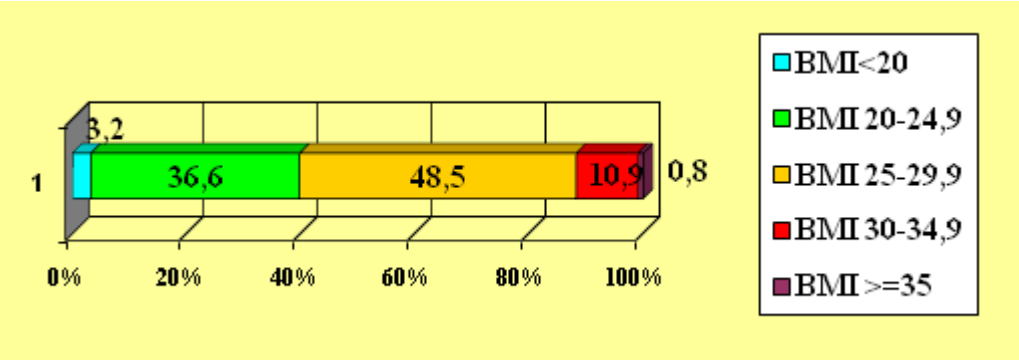
7. figure. Distribution of the average BMI of the „T3+T4" appeared in terms of the qualifications between 01.01.2007–31.12.2010. (n=12.739 persons, male) [10]

Value of the BMI of the staff qualified *„Fit"* belonging to the category *„T4"* was *25,5* +/- 3,1, that of the *„Unfit"* was *27,6* +/-3,5 and that of the *„Unloadable"* was *28,8* +/- 4,3. Both in the category *„T3"* and in the category *„T4"* the *„Unfit"* and the *„Unloadable"* had a significantly higher BMI (p<0,001) compared to that of the *„Fit"*. BMI-value of the *„Unloadable"* was significantly higher (p<0,001) compared to that of the *„Unfit"*. Comparing BMI-values of groups with the same qualification to eachother between the categories „T3" and „T4" there were *significantly higher values (p<0,001) to be found at staff „T3"*.



8. figure. Percent distribution of the BMI-values of the male staff „T3" appeared on the missionary medical test between 01.01.2007–31.12.2010. (n=1.701 persons) [11]

2,2% of the staff *„T3”* had a BMI-value under 20,0*, 28%* of the staff had a value of 20,0-24,9, *53% of it* had a value of 25-29,9, 13,3% had 30,0-34,9, and *2,0%* had a BMI-value over 35. (Figure 8.)



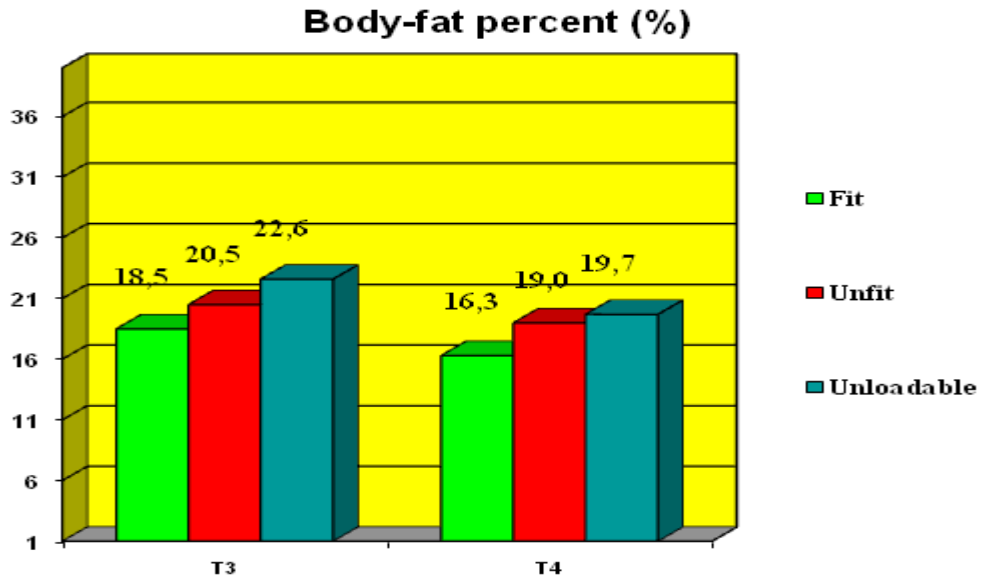
9. figure. Percent distribution of BMI of the male staff „T4” appeared on the missionary medical test between 01.01.2007.-31.12.2010. (n=11.038 persons) [12]

There were more favourable value indexes in the category *„T4”* to be found**.** *3,2%* of the staff „T4” had a BMI-value under 20,0; *36,6%* of it had a value of 20,0-24,9; 48,5% had a value of 25-29,9; *10,9%* had 30,0-34,9, and *0,8%* had a Body Mass Index (BMI-value) over 35. (Figure 9.)

On the basis of the data and figures of the World Health Organisation (WHO) *30,8%* of the staff *„T3”* with the requirement standard „physically fit” was of normal body weight, *53,8%* was overweight, and 15,5% of it was obese. (Figure 8.) Contrary to that *39,8%* of the staff *„T4”* was of normal body weight, *48,5%* was overweight, and *11,7%* was obese. (Figure 9.)

Body-fat percent test

In the course of the body-fat percent test (OMRON BF 306) there was a similar tendency to the body mass and to the BMI to be observed within the groups, as well as after being compared the two categories.



10. figure. Distribution of average body-mass of the staff T3+T4 appeared, in terms of the qulifications (n=12.739 persons, male) [13]

Average body-fat percent of the staff qualified *„Fit"* belonging to the category *„T3"* was *18,5* +/-5,5%, that of the *„Unfit"* was 20,5 +/- 4,9%, that of the *„Unloadable"* was *22,6* +/- 4,1%. (Figure 10.) Body-fat percent of the staff qualified *„Fit"* belonging to the category *„T4"* was *16,3* +/- 5,3%, that of the „Unfit" was *19,0* +/- 5,4%, that of the *„Unloadable"* was *19,7* +/- 4,6%. Average difference of the average body-fat percent of the staff *„T3+T4"* qualified *„Fit"* was *2,2%,* that of the *„Unfit"* was *1,5%,* and that of the *„Unloadable"* was *2,9%.* (Figure 10.)

CONCLUSION AND SUMMARY

On the basis of the measuring results during the 4 years it is altogether to be ascertained that both in the category *„T3",* and in the category *„T4"* the *„Unfit"* and the *„Unloadable"* had a significatly higher body mass, and BMI, as well as body-mass percent compared to those of the *„Fit".* Body mass, BMI-, and body-fat percent values of the *„Unloadable"* were significantly higher in comparison with those of the *„Unfit".* Comparing body mass, BMI-, and body-fat percent values of the same qualified groups between the category *„T3"* and *„T4"* to eachother, *there were significantly higher values at the staff „T3" to be found.*

It is, however, thought-provoking that there was no significant difference between the body mass average values of the staff *„T3"* qualified *„Fit"* and of the staff *„T4"* qualified *„Unfit"* (84,9 +/- 12,5; 84,2 +/- 12,2). At the same time the average age of the group *„Unfit"* of *„T4"* was *4,5 years* significantly ($p<0,001$) lower (29,7 +/-4,5; 34,3 +/- 6,1), *BMI* and the body-fat percent were significantly higher ($p<0,05$).

Over 12% of the staff applying for the mission have a BMI of more than 30. Constitutional data and figures indicate that overweight and theretrough a higher Body-Mass Index were caused unambiguously by a higher body-fat % . Body mass, body-fat per cent, and BMI of the soldiers qualified „unfit" were significantly higher than those of the soldiers qualified *„Fit".* On the basis of the anthropometrical data the *„Unloadable"* soldiers have a considerable overweight and approach the level *„Obesity I"* according to the WHO-classification. In the category *„T4"* setting higher standards the anthropometrical measuring results give us a more favourable picture.

Resources

[1-4] The author's own illustrations

[5] Magyar Közlöny, 31. szám, I. kötet, Budapest, 2006. március 21., 7/2006. (III. 21.) HM rendelet, 2460-2622. o., 2464. o., 11. §, (2) d)

[6] Magyar Közlöny, 31. szám, I. kötet, Budapest, 2006. március 21., 7/2006. (III. 21.) HM rendelet, 2460-2622. o., 2464. o., 11. §, (2) c)

[7] Magyar Közlöny, 31. szám, I. kötet, Budapest, 2006. március 21., 7/2006. (III. 21.) HM rendelet, 2460-2622. o., 1. melléklet a 7/2006. (III. 21.) HM rendelethez, 2490. o.

[8] http://t1.gstatic.com/images?q=tbn:ANd9GcTLD3Nqt1ET-NLhV-k5-

[9-13] The author's own illustrations

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kende György
gyorgy.kende@zmne.hu

Juhász Zsolt
juhaszzsolt@gmail.hu

EXAMINATION OF THE CONNECTIONS BETWEEN MOTION FORMS AND CONSTITUTIONAL FACTORS IN THE CIRCLE OF THE HUNGARIAN ARMY'S STAFF APPLYING FOR FOREIGN SERVICE
(01.01.2007 – 31.12.2010.)

Absztrakt

A fizikai erőnléti állapot következetes és rendszeres vizsgálata a különböző külföldi beosztások eltérő sajátosságai, valamint az emberi szervezetre gyakorolt eltérő jellegű és mértékű negatív hatásai miatt, egyre nagyobb jelentőséggel bír. Jelen munkában mindezek tükrében a külszolgálatokra jelentkező személyi állomány négy év alatti felmérésük során alkalmazott mozgásformák és az alkati tényezők, valamint az életkor és a fizikai teljesítőképességük közötti összefüggéseket kerestük és azok segítségével, a teljesség igénye nélkül igyekeztem egy átfogó képet adni a magyar haderő 2007 és 2010 között megvizsgált külszolgálatra jelentkező állományának fizikai erőnléti állapotáról.

A consistent and regular test of physical condition owing to the different characteristics of diverse foreign military posts, as well as to their negative effects of different kinds and grade taken on human body is being of more and more importance. In this study all these facts will be investigated. It was looked for a connection between the motion forms and constitutional elements used during its survey, as well as for a connection between the age-groups and physical performance of the staff applying for foreign service measured during four years. By dint of all these figures a comprehensive picture of the physical condition of the Hungarian Army's staff applying for foreign service in the period of 2007-2010 was guiven, without aiming at completeness.

***KKulcsszavak**: alkati tényezők, mozgásformák, fizikai teljesítőképesség, külszolgálat ~ constitutional elements, motion forms, physical performance, foreign service*

INTRODUCTION

It is always the character of the motor activities and the complex of the environmental conditions that determine what kind of conditioning faculties can be talked about and whether their developmental stage is sufficient or not. For this reason it is most optimal to carry on the training and drilling under conditions closest to the missionary circumstances in the last phase of the preparations. In this way the staff is able to get adopt to stimulus effects gradually and expediently, under the influence of which their toughness rises onto a higher and higher level both psychologically and physically, and will become firm. Up to the possibilities it is always thecharacter of the missionary activity in question and the local climatic conditions to be taken into consideration, and then taking as its starting point the most suitable methods, exercises and equipments for development of faculties should be chosen.

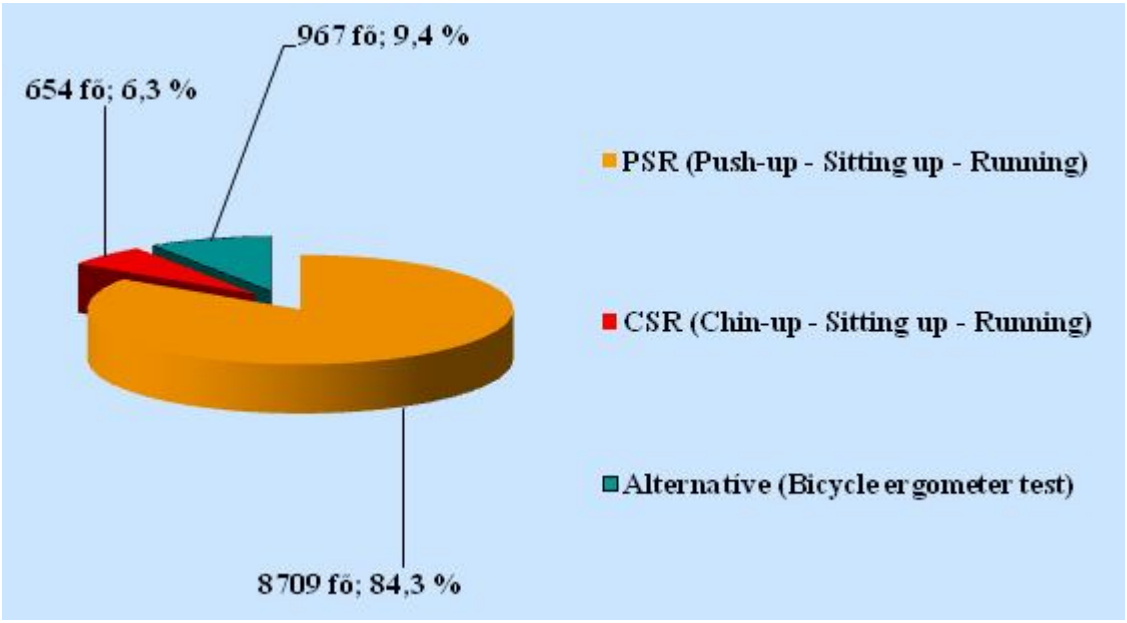
It is striking and is to be explained by existing reduced anthropometrical indexes that a more considerable part of the tests under laboratory conditions falls to soldiers marked *„T3”*, which might be brought into connection with health problems due to obesity.

In the following, results obtained on the physical aptitude test in both categories (T3, T4) were compared to eachother in case of identical motion forms. Results of the groups were compared to each other both under field and laboratory conditions, as well as it was also examined anthropometrical differences between soldiers choosing pulling up and push-up.

EXAMINATION OF THE CONNECTIONS BETWEEN MOTION FORMS AND CONSTITUTIONAL FACTORS

In duties requiring „extended” (T3) physical condition it was 76,6% the ratio of those persons who were tested under field conditions and who chose the motion form group „Pushing up-Sitting up-Running” (hereinafter called PSR) or the motion form group „Pull up Sitting up and Running” (hereinafter called PSR), and *23,4%* of them were able to prove their fitness for service under laboratory circumstances. In case of *„T4”* there were more than *90%* of those who were tested under field conditions, and less than *10%* who underwent the psychical aptitude test under laboratory circumstances. (Figures 1-2.)

1. figure. Distribution of the missionary military male staff „T3” loaded on the basis of motion form groups, between 01.01.2007–31.12.2010. (n=1.593 persons) [1]



2. figure. Distribution of the missionary military male staff „T4" loaded on the basis of motion form groups between 01.01.2007–31.12.2010. (n=10.330 persons) [2]

Compared the staff marked *„T3"* to that marked *„T4"* there were *73,1%* that is *84,3%* of those persons who chose the exercise group *Push-up - Sitting up - Running (PSR)*, that is to say there were *3,5%* that is *6,3%* of them who chose *Chin-up - Sitting up - Running (CSR),* and there were only *23,4%* that is *9,4%* of them who were loaded by bicycle-ergometer tests, which was to be attributed to reasons of health. (Figures 1-2.)

		Chin-up (piece)	**Point**	**Sitting up (piece)**	**Point**	**3200 m running (minute, sec.)**	**Point**	**All scores**
T3 CSR (Fit) n=53	Average	**15**	**86**	**56**	**76**	**941**	**139**	**301**
	Dispersion	6	17	11	14	102	21	37
T4 CSR (Fit) n=596	Average	**16**	**87**	**60**	**77**	**901**	**146**	**310**
	Dispersion	5	15	11	14	88	18	32
t-test		ns.	ns.	p<0,05	ns.	p<0,01	p<0,01	p<0,05

		Push-up (piece)	Point	Sitting up (piece)	Point	3200 m running (minute, sec.)	Point	All scores
T3 PSR (Fit) n=916	Average	**46**	**69**	**51**	**71**	**982**	**134**	**274**
	Dispersion	11	16	10	14	94	18	29
T4 PSR (Fit) n=6275	Average	**52**	**74**	**56**	**74**	**931**	**141**	**290**
	Dispersion	11	15	10	13	81	15	25
t-test		p<0,001	p<0,001	p<0,001	p<0,001	p<0,001	p<0,001	p<0,001

1. table. Distribution of the military male staff T3+T4 fit on the missionary tests CSR (Chin-up Sitting up - Running) and PSR (Pus-up - Sitting up - Running) on the basis of their performance indexes between 01.01.2007–31.01.2010. (n=7.840 persons) [3]

Average performance of the 53 persons marked *„T3"* qualified „physically fit" who had chosen the exercise group *Chin-up-Sitting up-Running (CSR)* was as regards *chin-up 15* ± 6, as regards *sitting up* it was *56* ± 11, recurrent number (piece), and they covered the prescribed course of 3.200 m in 941 ± 102 seconds (sec.). (Table 1.)

Average performance of the 596 persons marked *„T4"* also qualified *„physically fit"* who had chosen the exercise group *Chin-up-Sitting up-Running (CSR)* was as regards *chin-up* already *16* ± 5, regarding *sitting up* it was *60* ± 11, recurrent number (piece), and they covered the prescribed course of 3.200 m in *901* ± 88 seconds (sec.). (Table 1.)

As for the scores, the *average* values of *„T3"* were in *chin-up* was *86* ±17, in *sitting up* it was *76* ± 14, in *running 139* ±21 scores, and *altogether* it was *301* ± 37 scores. (Table 1.) *Average* score-values of *„T4"* were in *chin-up 87*± 15, in *sitting up* were **77** ± 14, and in *running 146* ± 18, *altogether* it was *310* ±32 scores. (Table l.)

Average values of staff of higher number chosen the exercise group *Push-up - Sitting up - Running (PSR)* were, as follows: average performance of 916 persons marked *„T3"* qualified *„Physically fit"*, chosen the exercise group *Push-up - Sitting up - Running (PSR)* was in *push-up 46* ±11, in sitting up it was 51 ± 10, recurrent number (piece), and they ran the prescribed course of 3.200 m in *982* ± 94 seconds (sec). (Table 1.) Average performance of 6274 persons marked *„T4"* qualified also „physically fit" chosen the exercise group *Push-up - Sitting up - Running (PSR)* was considering *push-up 52* ±11, considering *sitting up* it was *56* ±10, recurrent number (piece), and they ran the prescribed course of 3.200 m in *931* ± 81 seconds (sec). (Table 1.)

As for the scores the average values of the staff *„T3"* were in *push-up 69* ±16, in *sitting up* it was *71* ±14, in *running* it was *134* ±18, altogether it was *274* ±29 scores. (Table number 1.) Average score values of *„T4"* were in *push-up 74*± 15, in *sitting up* it was *74* ±13, in *running 141* ±15, and *altogether* it was *290* ±25 scores.(Table 1.)

According to the performance-indexes documented during 4 years for both motion groups of PSR and PSR tied to field conditions it can be seen well that independent of a motion form group, soldiers marked „T4" were able to do a better performance than those marked „T3". (Table 1.) For each motion form group there was a considerable difference between the two „T"-categories shown by the exercise Push-up - Sitting up - Running (PSR). (Table 1.)

		Push-up (piece)	**Point**	**Sitting up (piece)**	**Point**	**Bicycle (watt/kg)**	**Point**	**All scores**
T3 PSC (Fit) n=357	Average	**39**	**64**	**43**	**64**	**3,00**	**144**	**270**
	Dispersion	12	18	13	17	0,35	19	32
T4 PSC (Fit) n=811	Average	**44**	**65**	**49**	**66**	**3,18**	**148**	**279**
	Dispersion	12	16	11	14	0,33	15	25
t-test		p<0,001	ns.	p<0,001	p<0,01	p<0,001	p<0,01	p<0,001

2. table. Distribution of male military staff T3-T4 fit on missionary test in PSC (Pushing up - Sitting up - Cycling) according to the performance-indexes between 01.01.2007–31.12.2010. (n=1.168 persons) [4]

Average performance of the 357 persons marked *„T3"* qualified *„Physically fit"* chosen the exercise group *Push-up - Sitting up - Cycling (PSC)* was as regards push-up *39* ± 12, as regards *sitting up* it was *43* ± 13, recurrent number (piece), and they cycled to be loaded up to *3,00* ± 0,35 watt/kg. (Table 2.)

Average performance of 811 persons marked *„T3"* also qualified *„Physically fit"* chosen the Exercise group *Push-up - Sitting up - Cycling (PSC)* was as regards *push-up* already *44* ± 12, as regards *sitting up* it was *49* ± 11, recurrent number (piece), and they reached a performance of *3,18* ±0,33 watt/kg. (Table 2.)

As for the scores the *average values* of the staff *„T3"* were in *push-up 64* ± 18, in *sitting up* it was *64* ± 17, and in cycling 144 ± 19, and it was altogether 270 ± 32 scores. (Table 2.)

Average score values of *„T4"* were in *push-up 65* ± 16, in *sitting up* it was *66* ± 14, in *cycling* it was *14 6*± 18, altogether: 279 ± 25 scores. (Table 2.)

Average values of the smallest staff chosen the exercise group Chin-up - Sitting up - Cycling (CSC) were the following.

Average performance of the staff marked *„T3"* of 6 persons qualified „physically fit" chosen the exercise group *Chin-up - Sitting up - Cycling (CSC)* was as regards *chin-up 15* ±4, as regards *sitting up* it was *52* ±10, recurrent number (piece), and they reached a performance of *3,42* ± 0,38 watt/kg. (Table 3.)

Average performance of the staff marked *„T4"* of *31* persons also qualified *„Physically fit"* chosen the exercise group *Chin-up - Sitting up - Cycling (CSC)* was, however, considering *chin-up* already *14* ± 3, considering *sitting up* it was *52* ± 16, recurrent number (piece), and they reached a performance of *3,37* ± 0,37 watt/kg. (Table 3.)

As for the scores the *average* values of *„T3"* were in *chin-up 98* ± 4, in *sitting up* it was *78* ±19, in *cycling* it was *156* ± 11, and *altogether* it was 332 ± 33 scores. (Table 3.)

Average score values of *„T4"* were in *chin-up 78* ± 18, in *sitting up* it was *68* ± 20, in *cycling 152* ± 13, altogether it was *298* ± 29 scores. (Table 3.)

		Chin-up (piece)	Point	Sitting up (piece)	Point	Bicycle (watt, kg)	Point	All scores
T3 CSC (Fit) n=6	Average	**15**	**98**	**52**	**78**	**3,42**	**156**	**332**
	Dispersion	4	4	10	19	0,38	11	33
T4 CSC (Fit) n=31	Average	**14**	**78**	**52**	**68**	**3,37**	**152**	**298**
	Dispersion	3	18	16	20	0,37	13	29
t-test		ns.	p<0,01	ns.	ns.	ns.	ns.	p<0,05

3. table. Distribution of male military staff T3-T4 fit on missionary test in CSC (Chin-up - Sitting up - Cycling) on the basis of performance-indexes between 01.01.2007–31.12.2010. (n=37 persons) [5]

There was no difference between the performance-indexes of the motion form groups Chin-up - Sitting up - Cycling (CSC) under laboratory conditions documented for four years, higher scores obtained by „T3" arose from the age of life (age of „T3": 37,6 ±10,3 years; age of „T4": 29,9 ± 5,5 years; p<0,01). (Table 3.)

EXAMINATION OF THE CONNECTION BETWEEN AGES AND PHYSICAL CAPACITIES

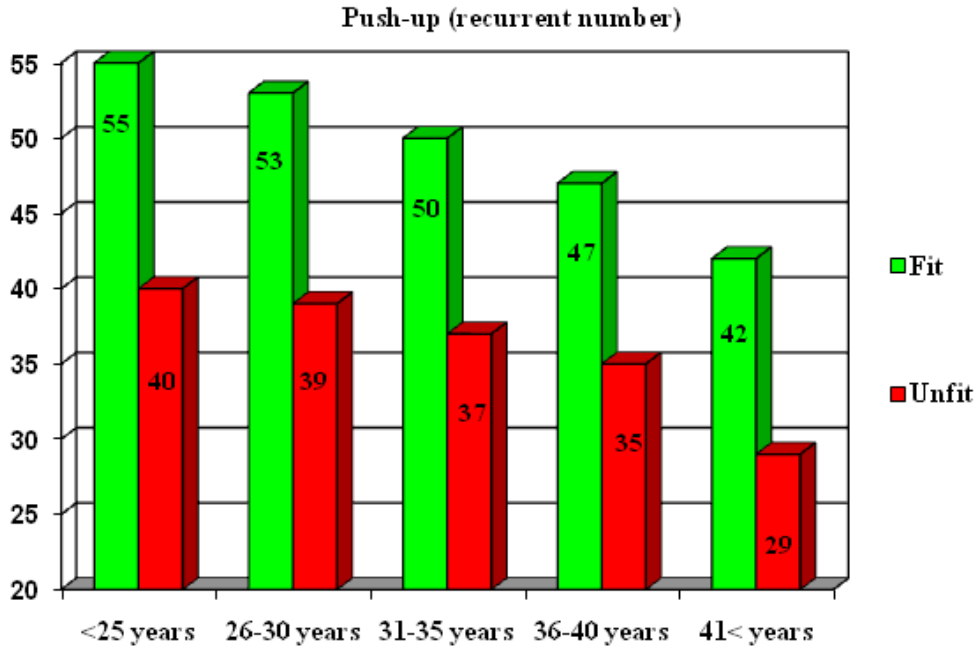
Of the persons applying for different missions during the last 4 years the results of those soldiers were underlined who belong to the category *„T4"* with the requirement to be trained on the highest-level, considering that nearly 85% of the staff (8.709 persons) had chosen the exercise group *Push-up - Sitting up - Running (PSR)*. The almost 9000-strong staff was suitable that the results obtained in this way taken as a function of the age group characteristics could be examined, as well, and so by dint of the representative results for each motion form and age group we could get an objective picture of the Hungarian Missionary Staff's condition of physical preparation.

Average pushing up performance of 6.275 persons marked *„T4"* qualified *„Physically fit"* chosen the exercise group *Push-up - Sitting up - Running (PSR)* broken down by age groups was < under 25 years *55*± 11, 26–30 years it was *53* ±11, 31-35 years it was *50* ± 11, 36-40 years *47* ± 10, and over 41< years it was *42* ± 10 recurrent number (piece). (Figure 3.)

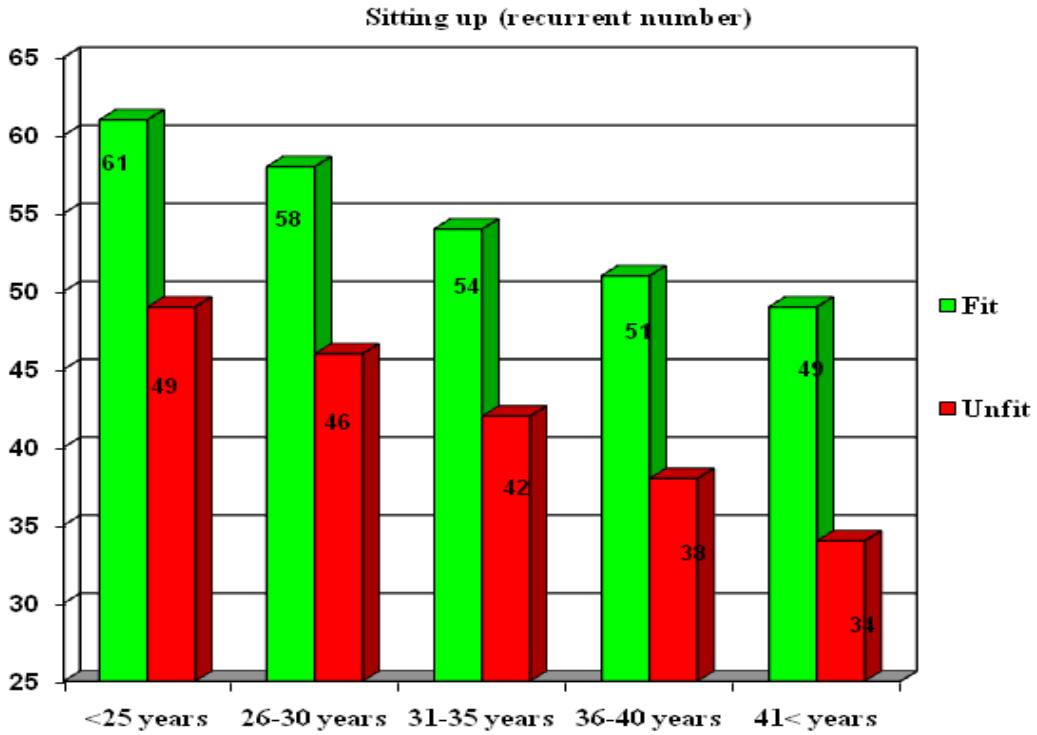
Average pushing up performance of 2.434 persons marked *„T4"* qualified *„Physically unfit"* chosen the exercise group *Push-up - Sitting up - Running (PSR)* broken down by age

groups was <25 years *40* ± 9, 26-30 years it was *39* ± 9, 31–35 years it was *37* ±9, 36-40 years *35* ± 8, and over 41< years it was *29* ± 7 recurrent number (piece). (Figure 3.)

After processing the data of the 4 years and following breaking down by age groups it came into view that the performance-indexes for average push-up show a gradually declining tendency in view of the advanced age. There is a negative connection between the age of life and the push-up performance values. Average performance-indexes for push-up of the *„Unfit"* are significantly lower (p<0,001) compared to those of the *„Fit"*.



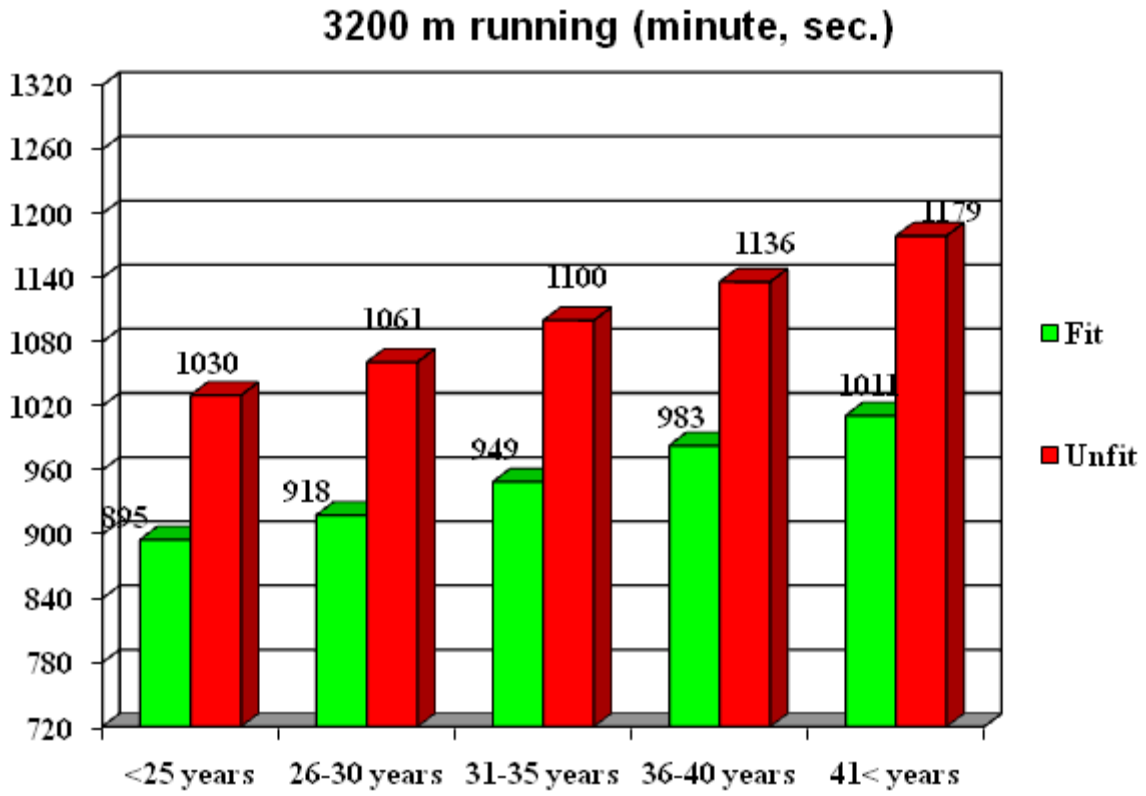
3. figure. Distribution of performance values of the staff „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [6]



4. figure. Distribution of performance values of the staff „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [7]

Average sitting up performance of 6.275 persons marked *„T4"* qualified *„Physically fit"* chosen the exercise group *Push-up - Sitting up - Running (PSR)* broken down by age groups was <25 years *61* ± 10, 26-30 years it was *58*± 9, 31-35 years *54* ± 9, 36-40 years *51*± 10, and over 41< years it was *49* ± 11 recurrent number (piece). (Figure 4.) *Average sitting up performance* of 2.434 persons marked *„T4"* qualified *„Physically unfit"* chosen the exercise group *Push-up - Sitting up - Running (PSR)* broken down by age groups was under <25 years *49* ±10, 26–30 years it was *46* ± 10, 31-35 years *42* ± 10, 36–40 years *38* ± 11, and over 41< years it was *34* ± 9 recurrent number (piece). (Figure 4.)

After processing the data of the 4 years and following breaking down by age groups it came into view that the performance-indexes for average push-up show also a gradually declining tendency in view of an advanced age. There is a negative connection also between the age of life and the performance values of pushing up. Average performance-indexes for push-up of the *„Unfit"* are significantly lower (p<0,001) compared to those of the *„Fit"*.

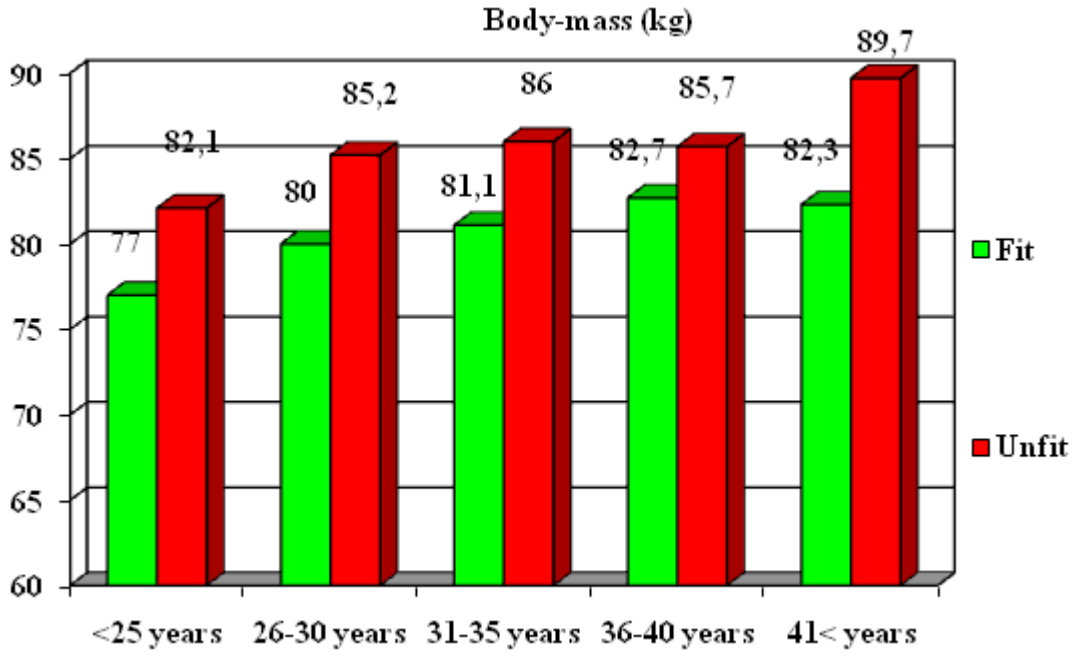


5. figure. Distribution of performance values of the staff „T4" for motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [8]

Average running performance of 6.275 persons marked „T4" qualified „physically fit" chosen the exercise group Push-up - Sitting up - Running (PSR) broken down by age groups running time was under <25 years 895 ± 69 sec., 26-30 years it was 918 ± 72 sec., 31–35 years 949 ± 76 sec., 36–40 years it was 983 ±87 sec., and over 41< years it was 1011±20.

Average running performance of 2.434 persons marked „T4" qualified „Physically unfit" chosen the exercise group Push-up - Sitting up - Running (PSR) broken down by age groups running time was under <25 years 1030± 92 sec., 26–30 years it was 1061 ±97 sec., 31–35 years 1100 ± 97 sec., 36–40 years 1136 ± 96 sec., and over 41< years it was 1179 ± 124 sec. (Figure 5.)

After processing the data of the 4 years and following breaking down by age groups it came into view that the average running time increases. There is a positive connection between the age of life and the running time. Average running time in the group of the „Unfit" is ignorantly higher ($p<0,001$) compared to that of the „Fit".

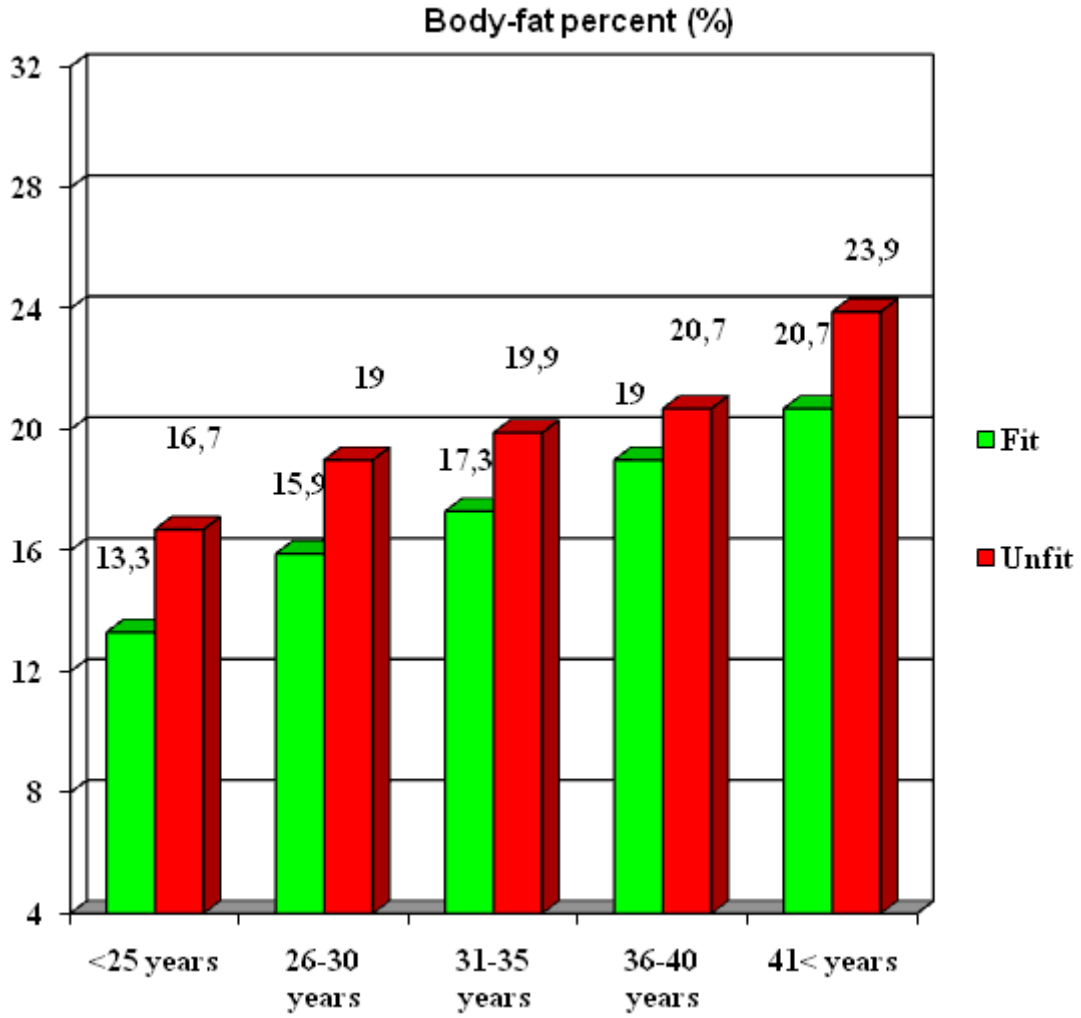


6. figure. Distribution of the average body mass of the „fit" and of the „unfit" of the staff marked „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [9]

In the course of the examinations of anthropometrical indexes then after their processing also it came into view that there is an expressed and quantifiable difference also inside the categories of examination. Independently of the fact whether the population of the *„Fit"* or that of the *„Unfit"* is taken as a starting point it is the *„Unfit"* staff for both „qualifications" that shows a higher body mass values, which is to be brought with a life-style short of motion into connection.*Average body-mass* of the staff qualified *„Fit"* marked *„T4"* belonging to the motion form group PSR (Push-up -Sitting up - Running) broken down by age groups was <25 years *77,0* ±10,2 kg, 26–30 years *80,0* ± 10,8 kg, 31–35 years it was *81,1* ± 11 kg, 36–40 years *82,7* ± 11, and over 41<years it was *82,3* ± 10,3 kg. (Figure 6.)

Average body-mass of the staff qualified *„Unfit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups was under <25 years *82,1*± 11,9 kg, 26–30 it was *85,2*± 12,1 kg, between 31–35 years it was *86,0* ± 12,6 kg, 36–40 years *85,7* ±12,8 kg, and over 41< years it was *89,7* ± 10,5 kg. (Figure 6.)

After processing the data of the 4 years, and following breaking down by age groups it came into view that the average body mass increases gradually in view of an advanced age. There is a positive connection between the age of life and the average body mass values. Average body-mass values of the *„Unfit"* are signicantly higher (p<0,001) compared to those of the *„Fit"*.

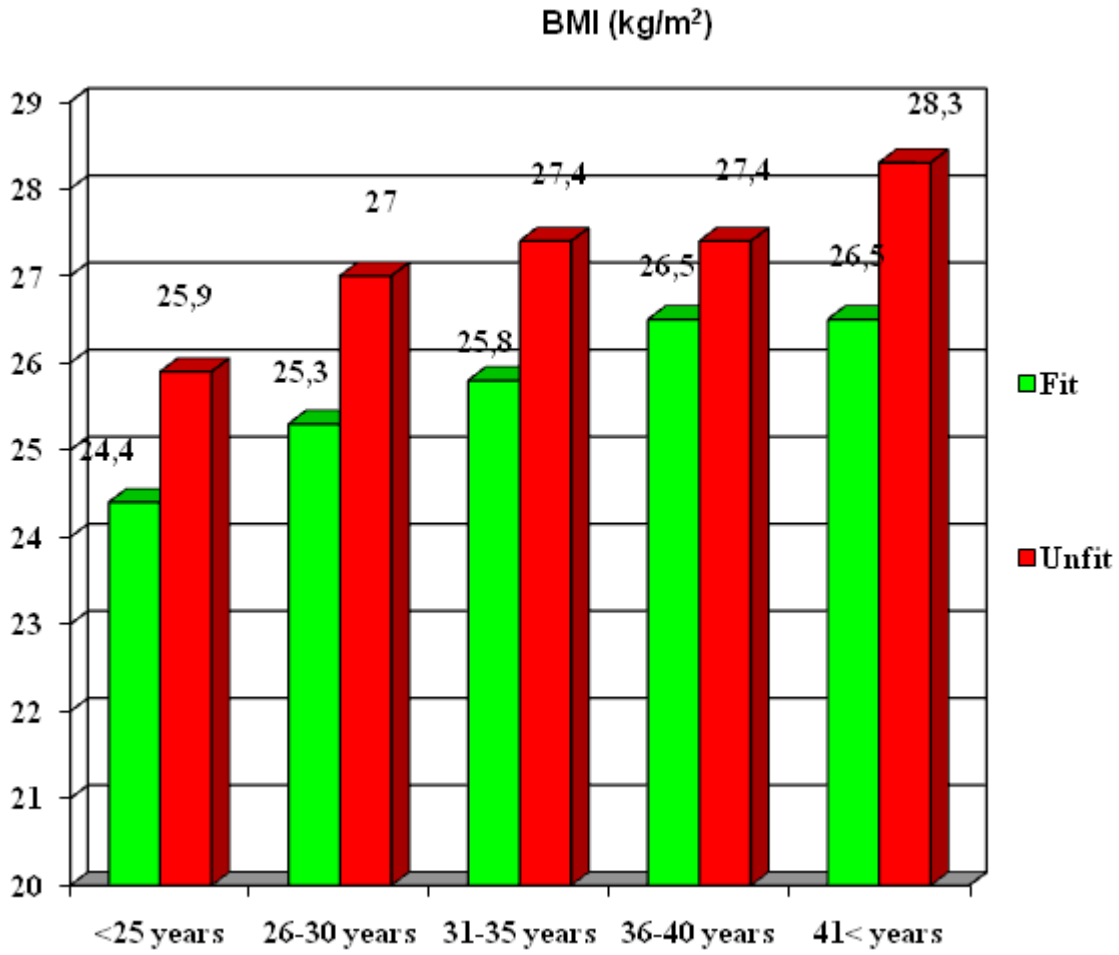


7. figure. Distribution of the average body-fat percent of the „fit" and of the „unfit" of the staff marked „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [10]

Average body-fat percent of the staff qualified *„Fit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups was under <25 years *13,3* ± 4,9%, 26–30 years it was *15,9* ± 4,8%, 31–35 years 17,3 ± 4,9%, 36–40 years *19,0* ± 4,7%, and over 41< years it was *20,7* ± 4,4%. (Figure 7.)

Average body-fat percent of the staff qualified *„Unfit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups was under <25 years *16,7* ± 5,6%, 26-30 years it was *19,0* ± 5,2%, 31 – 35 years *19,9* ± 4,9%, 36–40 years *20,7* ± 4,7%, and over 41< years it was *23,9* ±3,5%. (Figure 7.)

After processing the data of the 4 years and following breaking down by age groups it came into view that the average body-fat percent shows a gradual upward tendency in view of an advanced age. There is a negative connection between the age of life and the average body-fat percent values. Average body-fat % values of the *„Unfit"* are ignorantly higher ($p<0,001$) compared to the *„Fit"*.

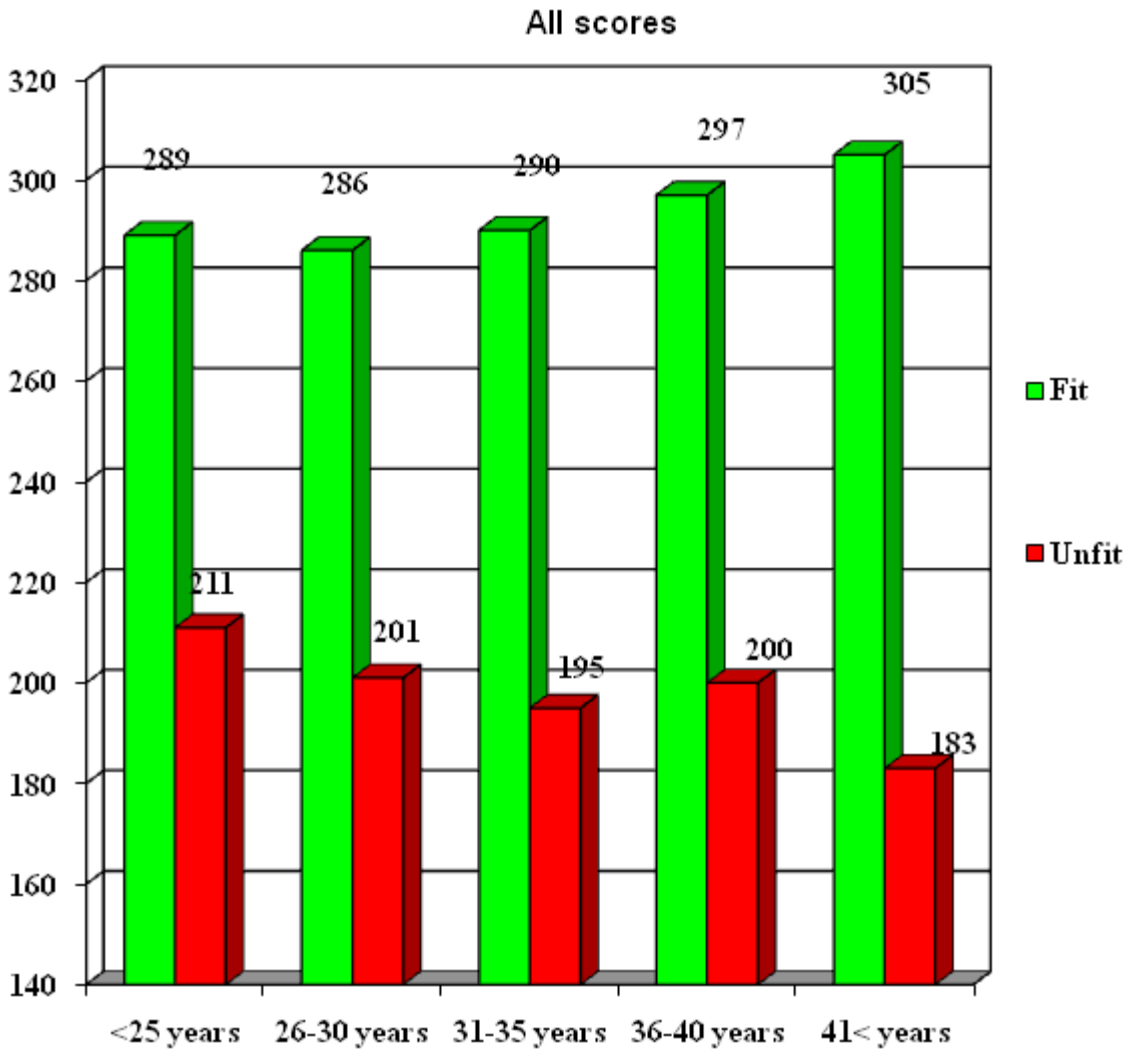


8. figure. Distribution of the average BMI of the „fit" and the „unfit" of the staff marked „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [11]

Average BMI values of the staff qualified *„Fit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups were under <25 years *24,4* ± 2,8%, 26–30 years it was *25,3* ±3,0 , 31–35 years *25,8* ± 2,9, 36–40 years *26,5* ± 2,9, and over 41< years it was *26,5* ± 2,9. (Figure 8.)*Average BMI values (kg/m²)* of the staff qualified *„Unfit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups were under <25 years *25,9* ±3,6, 26-30 years it was *27,0* ±3,4 , 31–35 years *27,4* ± 3,3 , 36–40 years *27,4* ± 3,4 , and over 41< years it was *28,3* ± 2,6. (Figure 8.)

The average BMI values show a gradual upward tendency in view of an advanced age. There is a positive connection between the age of life and the BMI values. Average BMI values of the *„Unfit"* are signicantly higher (p<0,001) compared to those of the *„Fit"*.

Average all scores of the staff qualified *„Fit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups were under <25 years *289* ±24 scores, 26-30 years it was *286* ±22 scores,31–35 years *290* ± 25 scores, 36–40 years *297* ± 28 scores, and over 41< years it was *305* ±31 scores. (Figure 9.)



9. figure. Distribution of performance values of the staff „T4" for the motion form group PSR (Push-up - Sitting up - Running) broken down by age groups between 01.01.2007–31.12.2010. (n=8.709 persons, male) [12]

Average all scores of the staff qualified *„Unfit"* marked *„T4"* belonging to the motion form group PSR broken down by age groups were under <25 years *211* ± 49 scores, 26–30 years it was *201* ± 53 scores, 31–35 years *195* ± 56 scores, 36–40 years *200* ± 53 scores, and over <41 years it was *183* ± 65 scores. (Figure 19.) The average all scores shows a gradual upward tendency in case of the „fit" in view of an advanced age. In case of the „unfit", however, is a declining tendency to be observed.

CONCLUSION AND SUMMARY

In the course of the scientific activities during four years the load-diagnostically measuring tests under field and laboratory conditions were destined for examining the partial local muscular strength endurance of the shoulder girdle and of the trunk, and the long-term stamina.

In general I found that according to the results measured and documented during four years as well as on the basis of my personal experiences the performance indexes of the Hungarian

Army's physical condition show - if not in a spectacular way but – an improving tendency both as for qualitative and as for quantitative values.

On the basis of the data measured during four years it was unambiguously to be proved that in view of an advanced age the constitutional indexes declined significantly and it was also closely related to the decrease of the missionary staff's physical performance.

Almost 88,7% of the in fact loaded staff testified under field conditions to their preparedness. It was 11,3% of them who took part in cycle-loading test as they fought against some health problems (locomotor diseases, cardiovascular problems or metabolic disturbances), which made a continuous check-up at loading necessary.

Performance of the unfit soldiers is identical with that of the fit soldiers over 41 years. It applies to their body mass, too. By advancing in age the anthropometrical indexes and the performance get worse – it is a normal physiological process - , but when these indexes are already in young days bad then it is to be expected even a worse performance at an older age.

Resources

[1-12] The author's own illustrations

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Veres Viktória
info.vveres@gmail.com

ANTI MONEY LAUNDERING AND TERRORIST FINANCING IN PRACTICE WITH THE EYES OF AN ONLINE FINANCIAL BUSINESS

Absztrakt

Ez az írás egy EU tagállam, Ciprus példáján keresztül mutatja be a pénzmosás és a terrorizmus finanszírozása megelőzésére vonatkozó szabályozást. A szerző e szabályozás legfontosabb rendelkezéseit foglalja röviden össze egy gyakorlati példán keresztül: egy online pénzügyi szolgáltatást nyújtó bróker cég szemszögéből. A cikk egy olyan kutatás része, amely a pénzmosást és illegális pénzműveleteket a katasztrófák zavargások és háborúk összefüggésében vizsgálja.

This article examines an EU member state, Cyprus example of the Anti-Money Laundering regulations. The author looks at and summarizes the most important provisions of law from practical considerations, outlines the problems and implementation opportunities related from an online financer service provider (broker) view. This article is bases to a research of money laundering and illegal financial transactions in times of disasters, riots and wars.

Kulcsszavak: *biztonság, pénzmosás elleni szabályozás, pénzmosás elleni küzdelem, internetes broker ~ safety, money laundering legislation, anti-money laundering practice, online broker*

1. INTRODUCTION

„Money laundering is a threat to the good functioning of a financial system; however, it can also be the Achilles heel of criminal activity."[1]

Money Laundering and Terrorist financing is not only a serious threat to economy and business but at large it has a negative impact to society, therefore combating is international responsibility at all level[2].

As the financial system`s complexity has been rapidly growing and changing for example payment methods used more and more frequently for cross border transactions and support customer anonymity and quick movement of money `…a national system must be flexible enough to be able to extend countermeasures to new areas of its own economy`3. These new areas include especially handling the e-society and e-commerce that enables criminals to perform illegal activities in a widely sophisticated way.

Different countries have similar approach towards AML and TF, but the counties of the European Union have taken extra efforts and actions to customize their approach and actions even in their legislation. The AML regulations are very similar in the member states as they are implemented from the same root, the actual money laundering Directive the European Parliament and the Council in the European Union.4 Among other initiatives, the member states require companies registered under their territory to comply with the provisions of the law and report yearly, monthly and on demand to relevant institutions, these institutions share their data if needed. The directive is based among other on the Financial Action Task Force (FATF) recommendations, which working groups are dedicated to work out up-to-date recommendations on Money Laundering and Terrorist Financing related issues from multiple sectors.

The article takes into consideration the Prevention and Suppression of Money Laundering Activities Law N188(I)/22075 in Cyprus and the Directive of Prevention of Money Laundering and Terrorist Financing DI144-2007-086 of the Cyprus Securities and Exchange Commission.7

---

[1] Financial Action Force: Money Laundering FAQ
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[2] Definition of ML and FT: WorldBank Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism Second Edition and Supplement on Special Recommendation IX http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf 2011 2011

[3] Financial Action Force: Money Laundering FAQ
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[4] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

[5] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010
http://www.law.gov.cy/law/mokas/mokas.nsf/All/8019B1816F17B4CCC22577A6002BF960/$file/AML%20consolidated%20law%20188_I__2007,%2058_I__2010_final%2030.7.pdf?OpenElement

[6] Cyprus Securities and Exchange Commission:
Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

7 From here the expressions like Law or Legislation will refer to these 2 implemented in Cyprus based on the 3rd ML Directive of the European Union.

The legislation aims safer financial environment for customers, helps to combat money laundering and terrorist financing, on the other hand companies in the private sector are struggling with the resources to be allocated to these tasks especially in times of financial crises, disasters and political crisis's. Therefore it is essential to make companies interested in AML and TF besides the fact that they are exposed to fines and imprisonment.

This article examines the legislation from operational overview, considers the most relevant provisions of the law and outlines some possible problems and implementation opportunities connected to them from an online broker company and its customers view.

Companies in the brokerage sector or those providing online financial services are more likely involved in the Layering phrase of money laundering than in the Placement or Integration part therefore the assets must be focused on this[8],[9] and also these companies have to cope with the fact that there is no face-to-face interaction with the customers and that most of the transactions are carried out online.

In practice there are 3 key elements on company level to combat money laundering and terrorist financing to avoid the abuse of the company systems for layering ML: risk approach based right procedures and IT solutions to flag suspicious transactions, employee awareness and suspicious client or transaction reporting.

This article will be followed by a research of money laundering and illegal financial transactions in times of disasters, riots, civil wars, etc.

Basic provisions of legislation discussed in this article

The basic provisions of ML and TF of the examined legislation among others are the following for companies[10]:

- Appoint an independent Money Laundering Officer (MLCO)
- Create, maintain and implement an Anti Money Laundering Manual (AML)
- External and internal reporting of suspicious transactions to the relevant authorities
- Report cash transactions to the relevant authorities
- Create, implement, maintain and monitor procedures into the operating systems and control to make sure that the established and implemented procedures prevent the abuse of the Company`s systems for Money Laundering and Terrorist Financing purposes.
- Maintain, monitor and record customer information and transactions in a way that helps to spot suspicious activity
- Evaluate 3rd party dependencies
- Examine new products and markets to combat AML and TF risks arising from the company`s new activities

[8] Money Laundering FAQ 2011
http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html
[9] More on the 3 stages of ML: International Money Laundering Information Bureau
http://www.imlib.org/page5_mlstgs.html
[10] Cyprus Securities and Exchange Commission:
Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

- Improve employee awareness by regular trainings, distribute the AML Manual, make sure employees understand their obligations

ANTI MONEY LAUNDERING AND TERRORIST FINANCING IN PRACTICE

Appointment of Money Laundering and Compliance Officer (MLCO)

Companies under this legislation are obligated to appoint MLCO and ensure that its function is independent. The MLCO is responsible to carry out the provisions of law by actively participating in the company`s policymaking, business development, moreover to create, implement, maintain and monitor procedures of the operating systems and control in order to identify risks arising and take necessary steps.

The employment of an MLCO might cause problems especially for small and medium companies as this profession requires complex legal, economic, business, financial and physiology knowledge and strong personal skills. The MLCO function as full time profession is relatively new therefore there is a shortage at the labor market of well educated and experienced employees. As a result the salary expectation of this profession puts a pressure on small and medium sized, especially new companies. Moreover in order to successfully fulfill its tasks the MLCO is to be trained and needs to train, this is also an addiction to the company costs.

The MLCO shall be involved into the company`s life wherever risks of ML and TF may arise such as when a company develops a new product, introduces a new payment method, or penetrates into a new market. There might be an opposition from the various departments to coordinate with the MLCO on these issues. Understanding the importance of the MLCO involvement of the department managers is essential and must be built and developed from the beginning. Most importantly the successful combat against ML and TF lies in the hands and responsibility of the management in order to assign sufficient resources to these functions.

Anti Money Laundering Manual (AML Manual) and Employee Training

Every company falling under the mentioned legislation must create and update on a regular bases a Manual that describes the company`s AML and TF practices, procedures and measures. This Manual must be distributed, thought and understood by all employees of the company.[11]

AML manuals are usually too long and complex to expect employees to read and take right consequences. Trainings are effective ways to communicate the legislation, AML and TF obligation, needs and procedures. Companies carrying out operations in more branches or countries must find cost effective ways. For example yearly one on-site training, and online training for new employees between on-site training periods. Not only the distribution of the AML manual and training is essential, but the establishment of a dynamic knowledgebase with case studies and examples contribute to the goals. For example knowledgebase and circulars are a good way to update employees dealing with customers from the Middle East on the increasing risks and vulnerabilities following the political crises.

Companies must make sure that their employees understand and follow the AML Manual, but most importantly that they are aware of their obligations such as how not to get part of

---

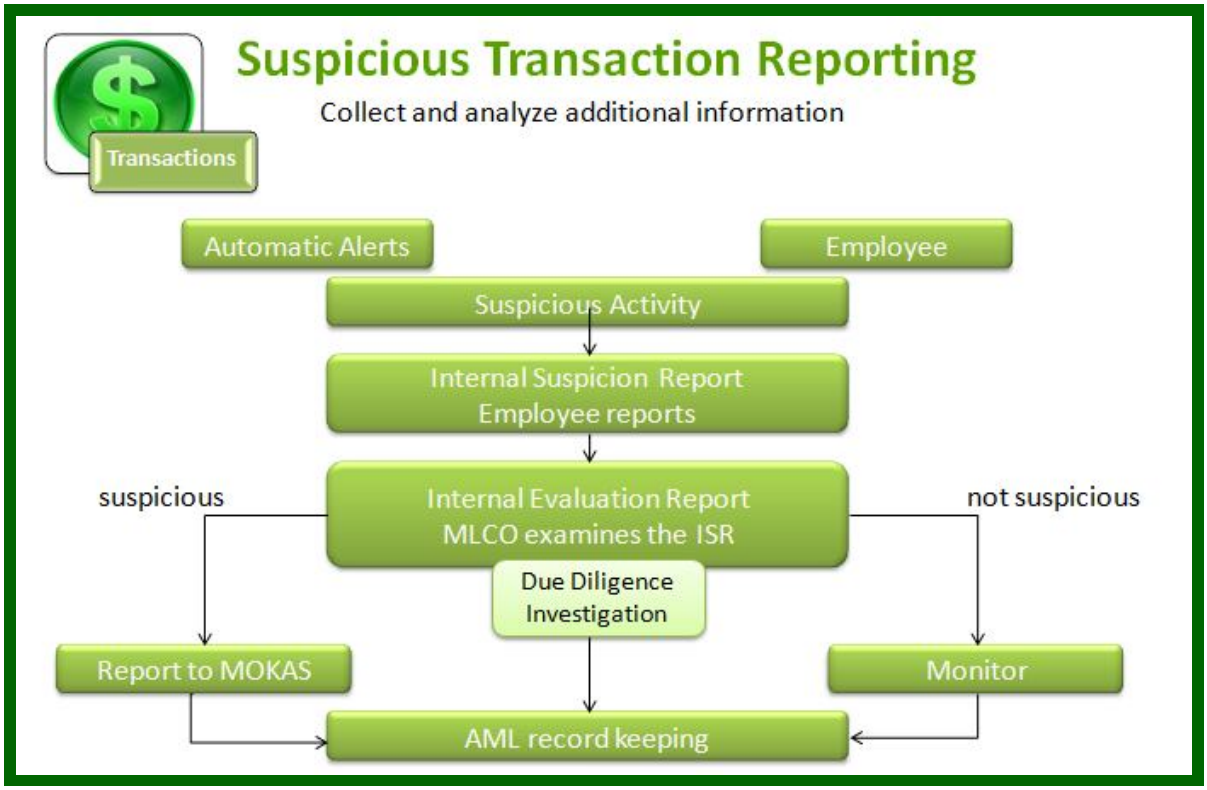
11 Cyprus Securities and Exchange Commission:
Directive Di144-2007-08 & Di144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing
http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf section VIII

ML and TF, how to spot and who to report suspicious customers and transactions. Employees who understand the real meaning of `dirty money` and the flow of the ML activity are more likely to report suspicious activity: at trainings it is important to emphasize something that they are sensitive to, for example that the dirty money can come from child abuse or human trafficking and by not taking steps they indirectly might help these criminals.

Reporting

Companies and employees are obligated for internal and external reporting and cash transaction reporting to an appointed person and relevant authorities.[12]

- Internal Reports: Internal Suspicion Reports are done by employees who suspect that a customer might use the company for ML and TF purposes, the money laundering officer must evaluate these reports, perform due diligence and decide if it is to be reported to the relevant authorities. The main problem with these reporting is that in practice employees with commission based salaries are not interested in reporting suspicious transactions as it can lead to losing customers and commission while the reporting (filling the Internal Suspicion Report forms, participating and providing information for internal evaluation) and follow ups might cause further inconvenience for them. Therefore, the MLCO must find the right procedures and monitoring to enforce the Law. The below slide shows the recommended flow of the suspicious transaction reporting from any employee of the company through the MLCO to the relevant Unit MOKAS in Cyprus.



1. picture. Suspicious Transaction Reporting Flow
Prepared by the author[13]

[12] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010, section 69

- External Reports:
  - Suspicious Transaction reports to relevant authority (based on the evaluated Internal Suspicion Reports)
  - Annual reports to relevant authority[14]
  - In Cyprus, the Relevant Authority (CySec) will not reflect the result of the review of the report to the Company and do not give recommendations to improve specific procedures. Companies can use the services of local External Auditors for this purpose before submitting the report, further costs apply.
  - Cash transaction Reports above a specific amount set in legislation[15]
  - Online companies obligated to issue monthly reports are facing problems with what kind of transaction in considered cash. In practice companies should consider Western Union, MoneyGram, etc transactions as cash, therefore include them into reporting.

Operational solutions for preventing Money Laundering

This part of the article describes the recommended policies and measure taken by online financial companies regarding combating ML and TF including new and existing clients, transactions, new products, new markets, etc.

Operational measures to prevent ML deals with issues related to money laundering and terrorist financing and include the assessments of the current weaknesses. Measures and procedures undertaken by the Company in order to prevent money laundering and terror financing should be based on the relevant legislation of Prevention of Money Laundering and Terrorist Financing. The policies and procedures include steps to be taken by the different operating teams in the Company in order to be able to identify possible Money Laundering and Terrorist Financing activities. However, usually the directives are not tailored for online flow of money. Implementation of such regulation into operational procedures in online financial services might be not cost effective, the risks that companies might take by not complying with the law depends on the company`s illegality tolerance. Using the right assessment tool to understand our compliance risk fitness, the risk based method can help a company to find the right balance to deal with risks arising from non-compliance with the legislation.[16]

---

[13] Slide was prepared by the author for company AML and TF training purposes, picture of the $ sign was taken from http://greenconduct.com/jobs/wp-content/uploads/2011/03/6a00d8341ee15453ef0147e30fc69a970b-800wi.jpg

14 United Kingdom example of how to build an annual report, same can be used in Cyprus or any other EU country: Joint Money Laundering Steering Group MLRO Annual Report http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report

[15] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 sections 60

[16] Open Compliance and Ethics Group (OCEG): Compliance Risk Fitness: Assessing and Treating the Real Risks to Compliance webinar held 2/6/2011 http://www.oceg.org/event/compliance-risk-fitness-assessing-and-treating-real-risks-compliance

Risk based approach

Companies shall implement the risk based approach[17] into their policies and procedures in order to manage risks in an effective and affordable way. The Risk based approach includes the identification, recording and evaluation of combination of triggers and indicators of various Risks which may be related to money laundering and terrorist financing. These can be categorized as the following:

- Risks based on Client`s account type and nature (Corporate accounts, customers from high risk countries)
- Risks based on Client`s behavior (non communicating clients, clients unwillingness to provide identification documents, transactions that are flagged by Automatic system – (as described in point 8 below)
- Risks based on the Client`s initial communication with the Company (clients introduces by third person, branches outside of the Republic, managed accounts)
- Risks based on the Company`s Services and financial instruments (3rd party payments, large and high frequency of transactions)

In order to manage the above mentioned risk categories, the Company should define measures and procedures to be approved by the MLCO and performed by the various teams of the Company. For examples:

- Client Risk Categorization
- Identification Verification
- Due Diligence Procedures
- Transaction monitoring (deposits, withdrawals, money movements)
- Ongoing monitoring of high risk clients, etc

Client categorization

Client categorization is not only provision of law, but also utilized as a tool for the risk management. The division of clients into different risk levels groups enables the risk analyst to cope with high volumes and focus on relevant customers and apply different monitoring and verification procedures for each risk group.

The categorization of the clients and ML prevention processes are based among others, on the type of the client, his geographic location, economic profile, personal information, trading activity, and the funding methods he uses. The risk analysis uses own discretion for categorization. Though regulation gives clear instruction on how to categorize Customers but it cannot be effectively applied at online brokers: all non face-to-face customers should be considered as high risk clients and enchanted due diligence must be performed.[18]

In order to keep the economic sense 4 levels of risk categorization are recommended

- Low risk clients with low-risk results in client identification and due diligence
- Normal risk clients:_for example_clients from EEA countries using EEA registered financial institutions for all kind of money flow

[17] Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing Part IV

[18] Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing Fourth Appendix

- High risk clients with enhanced client identification and due diligence measures: for example countries that have not implemented FAFT recommendations, `Enhanced customer due diligence measures must be taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing.`[19]
- Not acceptable customers, for example customers from groups or countries who are under UN embargo

Client Acceptance Policy

The MLCO is responsible to apply all previsions of the Client Acceptance Policy assisted by other departments and to ensure that the Risk based approach is implemented.

The Client Acceptance Policy is the most cardinal problem of the legislation and practice. There is a conflict of objectives. The legislation requires companies not to establish business relationship with any customers before full Customer Identification Verification (see point 4 below). Also, the General Manager should approve all new Customers before performing any transactions. Customers investing 50-200 USD to try the service will unlikely want to send certified passport and utility bill copies and it is impossible for a General Manager at a company to review and approve personally 100-250 new customers a day. Companies are exposed by losing customers or not complying with the Client Acceptance Policy requirements. Lack of Customer Awareness on regulations will be mentioned later in this article at the difficulties of building an Economic Profile.

Customer Identification Procedure

Companies should apply a Customer Identification Procedure[20] using different Know Your Customer (KYC) protocols for Individual and Corporate accounts. The identification procedure is based on Know Your Customer documents and information recorded and provided by the Client at registration. Verification documents should be accepted only in colored copies.

Clients must provide Identification verification documents as per the following:

- Clear color copy of government issued Passport including written signature (government issued IDs can be accepted as well and in special cases like India, Tax Authority Card provided the photo and signature of the Client is visible)
- Clear copy of recent Utility Bill (any bill that is not older than 3 moths and comes to the trading account holders name and address of residence e.g. water bill, electric, gas, telephone etc…) or Bank Statement
- Clear color copy of both sides of the Credit Cards used to fund the account, if any (the middle 8 digits from the front and the CVV number from the back is to be masked)
- Further supporting documentation may be requested by the risk management team, if required.

[19] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 64 (2)

[20] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 61-62

This can be followed by transaction and trading activity review (if exists): As part of the verification process the Risk Analyst should reviews the Customers Economic Profile including trading activity, relations by computer, payment method and transaction history.

Corporate Client Identification further needs are that all corporate accounts' should undergo a special evaluation by the MLCO before any transactions are carried out.
In order to successfully verify Corporate Clients Company shall carry out a 3 step procedure:

- Identifying the Company, directors, authorized signatories, ownership structure, etc with the following documents:
  - Certificate of shareholders
  - Articles of association
  - Certificate of directors
  - Certificate of incorporation
  - Passport copy of the directors
  - Board resolution
- Identifying the Authorized Person with the same procedure as it was an Individual Client
- Requesting and examining the Power of Attorney given by the directors to an Authorized Person for authorized actions. The Authorized Person can be an employee of the Corporate Client or other such as an Introducing Broker.

World Check as Due Diligence tool[21]

Use of external data base for electronic KYC is recommended. Providers as World Check System[22] can be used in order to identify possible Politically Exposed Persons, perform passport checks, confirm that the customer is not blacklisted or committed crime. Problem with these systems might be that the data provided is not correct (from experience I can tell that for example if an incorrect passport number is uploaded for a person having the same name as a weapon smuggler can be a misleading match that can cause losing customers) so even if a positive match is showing, the case must be reviewed and investigated by the Company to close out incorrect information. In case the positive match is justified the relevant initiations must be informed to help their investigation.

Construction of Client Economic Profile

The construction of the Client Economic Profile should be defined by the MLCO, and carried out by all relevant departments. The data and information collected for this purpose should be stored in the company's systems.

Example of the data that can be collected and evaluated:

- Information required by Client Acceptance Policy
- Client Identification Verification
- Anticipated account turnover
- Purpose of the business relationship with the Company
- Employment history, contacting employer, verifying income
- Family status, number of people living in the same household

[21] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 section 61
[22] World Check http://www.world-check.com/ 2011

- On site visit at the customers residence
- Client transaction history review at Client Identity verification and withdrawal approval

Many customers find the establishing of their Economic Profile as inconvenience, they do not want to provide this kind of information and complain that other companies do not ask for this information. There is a lack of customer education on AML and TF issues and instead of having a greater trust towards companies who comply with regulations they end the business relationship and go to another Company with less `needs`. Experience shows that even if we inform customers that building an economic profile shows that we take regulations seriously. Customers do not consider it as a positive indicator. Especially in the EU there are plenty of official materials on the requirements of regulated financial Companies (example an Appropriateness Test), Customers are simply not aware of it.[23] This resistance and non-cooperation of Customers pushes Companies towards not complying and request less information to keep customers and grow business.

Third Party Payments and double funding

Third Party transactions should not be allowed in the Company's system with the exception of the Clients and the third Party`s written authorization (Power of Attorney) and full Identification Verification. The Company cannot allow deposits from corporate accounts to individual accounts and any private transactions funding corporate account. In such events, the MLCO shall instruct the finance department to refund the money to the same source and will notify the account owner to refrain from such transactions in the future.

Automatic system Alerts:

Money laundering activities can be limited by a set of automatic system alerts and flags of accounts and transactions which are triggered by similar indicators below:

- Apply automatic deposit limitations. In order to release the deposit limits from the account, the MLCO should accept the client.
- Identify and flag Name Conflicts: last and first name of the Credit Card holder are different from the customer name as registered in our system.
- Identify and flag Bin conflicts: client`s country in registration form does not match the Credit Card issuer country.
- Limit the number of allowed eWallet accounts used in the system from the last risk review by maximum 2
- Deposit country Conflict: Client tries to deposit from a country different than the country he has registered from.

The system shall be designed to limit the number of credit cards that are used by the client based on the rules set by the MLCO.

First transaction and deposit manual review

The Company should set monitoring procedures on Customers' deposits. Reviews should apply on all Customers' first deposits. Additional reviews can be carried out in case of alerts

[23]Committee of European Securities Regulators (CESR) A consumer's guide to MiFID Investing in financial products http://www.cesr-eu.org/popup2.php?id=4984

that are generated by the company's proprietary risk system or in case of alerts that are received by the payment service providers. Security reviews are performed by the Risk, Operations and Payment departments. The following deposit characteristics can trigger more detailed investigation:

- Indication for possible fraud by the payment processor (example - decline by the bank due to stolen credit cards)
- Third party payments – the account holder name is different from the owner of the deposited funds.
- Aggressive trading and wrong contact details.
- Multiple accounts connected to the same means of payment.
- Too many transactions, too complex deposit pattern
- Too many declined transactions
- Multiple deposit methods used on the same account
- Sleeping Money – customer deposited but not touching the money
- Too frequent in and outgoing payments
- Change in the deposit behavior - small transactions followed by a not justifiable high deposit

Companies with that integrated multiple regulated e-payment service providers or credit card payment services allow its clients to deposit and withdraw funds from their accounts in real time or almost real time. Regulated e-wallets such as Paypal, MoneyBookers and Neteller are performing identification verification checks to their clients according to European standards, but at the same time allow their clients to shop online securely without disclosing the payment methods that have been used to fund their e-wallet accounts. Most of the Company risk management and verification models relays on verification of ownership of the payment methods but not on verification of the origin of the funds as it would cause not bearable costs for the risk management.

Withdrawal processes

The Company should use identification verification and withdrawal policies in order to protect its Customers and prevent contributing to money laundering activities when sending funds. One of such policies that can be used by the Company in the withdrawal process is as following:

Predefined approval protocol that includes list of authorizations required (MLCO, Trading manager, General Manager) based on amount of money that is requested to be withdrawn. As a rule, withdrawal requests should be processed to the original means of payment that has been used by the Customer to fund his trading account. If the Customer has deposited via credit card or e-Wallet, the payment team must strive to pay the client back to the same cards or e-wallet account. If circumstances prevent the company from transferring the withdrawals to the original means of payment, the owner of the trading account will be requested to provide alternative payment method (by default – wire transfer details).

Withdrawal requests should be manually approved by Risk Department. The following information should be reviewed:

- Withdrawal request amount
- Withdrawal method
- Customer verification
- Copies of all Credit Cards used in our system are provided

- Customer country of origin of the funds and the Client, transaction history

Limited cash withdrawal payments shall be processed and all funds are to be processed via regulated financial entities that are following additional AML protocols. Special attention should be given in cases of large withdrawal requests from high risk countries like Malaysia, Indonesia, Pakistan, Bangladesh, Iran, Iraq, etc. and in cases of large withdrawal requests on accounts with limited trading activity relatively to the amount of funds deposited in the account.

SUMMARY

There are plenty of issues that have not been reflected in this article such as Partner AML and TF risk management, AML program for branches outside of the EEA, customers with specific needs or statuses, etc, but it gives a short overview on the complexity and additional resource needs of implementing AML and TF regulation to Company levels. It is obvious that Companies have difficulties to allocate enough resources and knowledge to create, enforce, maintain and monitor measures to all levels of the company. Countries and Regulatory Bodies should consider the characteristics of online financial service providers when designing the provisions, as to fully comply with the present legislation can lead to an uneconomic operation, loosing market, customers and competitiveness. The key is to ensure that the Company (with the help of the MLCO) establishes, maintains and improves a professional AML policy that is respected and followed by all employees, a policy that prevents money launderers to abuse the Company`s system, also can be supported with resources and do not harm the online based business model.

References:

[1] Financial Action Force: Money Laundering FAQ http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html 2011

[2] WorldBank Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism Second Edition and Supplement on Special Recommendation IX http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf 2011 2011

[3] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:EN:HTML

[4] Law Office of the Republic of Cyprus: The Prevention And Suppression Of Money Laundering And Terrorist Financing Laws Of 2007 and 2010 http://www.law.gov.cy/law/mokas/mokas.nsf/All/8019B1816F17B4CCC22577A6002BF960/$file/AML%20consolidated%20law%20188_I__2007,%2058_I__2010_final%2030.7.pdf?OpenElement

[5] Cyprus Securities and Exchange Commission: Directive Dι144-2007-08 & Dι144-2007-08(A) Of The Cyprus Securities And Exchange Commission For The Prevention Of Money Laundering And Terrorist Financing http://www.cysec.gov.cy/Downloads/Directives/InvestmentFirms/2009/DI144-2007-08.pdf

[6] International Money Laundering Information Bureau
http://www.imlib.org/page5_mlstgs.html

[7] Picture of the $ sign was taken from http://greenconduct.com/jobs/wp-content/uploads/2011/03/6a00d8341ee15453ef0147e30fc69a970b-800wi.jpg

[8] Joint Money Laundering Steering Group MLRO Annual Report
http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report

[9] Open Compliance and Ethics Group (OCEG): Compliance Risk Fitness: Assessing and Treating the Real Risks to Compliance webinar held 2/6/2011
http://www.oceg.org/event/compliance-risk-fitness-assessing-and-treating-real-risks-compliance

[10] World Check http://www.world-check.com/ 2011

[11] Committee of European Securities Regulators (CESR) A consumer's guide to MiFID Investing in financial products http://www.cesr-eu.org/popup2.php?id=4984

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Berki Gábor
berkigabor@t-online.hu

ELEKTRONIKAI HADVISELÉS A YOM KIPPUR HÁBORÚBAN

Absztrakt

A negyedik arab-izraeli háború (közismertebb nevén a Yom Kippur háború) előtt az arab országok jelentős fejlesztéseket hajtottak végre a hadseregekben, a légvédelemben és az elektronikai hadviselés területén is. 1973-ban megpróbálták visszafoglalni az izraeliek által 1967-ben, a hatnapos háborúban megszállt területeket. Új fegyvereikkel és harceljárásaikkal sikerült is meglepni Izraelt.

In the run-up to the Fourth Arab-Israeli War (also known as the Yom Kippur War), Arab countries undertook major reforms to develop their military forces including their air forces and electronic warfare capability. In 1973, Arab forces tried to reoccupy territories held by Israel since the 1967 Six-Day War. New Arab weaponry and battle manoeuvres succeeded in taking Israel by surprise.

Kulcsszavak: *Yom Kippur háború, elektronikai hadviselés, Közel-Kelet, arab-izraeli konfliktus ~ Yom Kippur war, electronic warfare, Middle-East, Arab-Israeli conflict*

ELEKTRONIKAI HADVISELÉSSEL KAPCSOLATOS FEJLESZTÉSEK

A hatnapos háborút követően – mint azt előző cikkemben leírtam – Izrael jelentős területeket elfoglalva megerősödött, míg az arab államok hatalmas katonai veszteségeket könyvelhettek el. Számukra nem csak a pótlás, hanem a minőségi fejlesztés is elsőrendű szempont lett. Ujjá kellett szervezni a fegyveres erőket, korszerűsíteni kellett a kiképzési rendszert, fokozni a harckészültséget és új technikákat kellett rendszerbe állítani. Ebbe beletartozott az elektronikai hadviselési képességek megerősítése is. Az előző háború tanulságait levonva, intenzívvé vált a rádióelektronikai szakcsapatok felállítása, kiképzése, a megfelelő harceljárások kidolgozása. A Szovjetuniótól beszerzett eszközökkel lehetővé vált, hogy az Izraeli haderő híradástechnikai eszközeit, összeköttetését felderítsék és zavarással lefogják, attól függetlenül, hogy milyen hullámtartományban üzemelnek. A légierőt olyan speciális

repülőkötelékekkel erősítették meg, amelyek rádiótechnikai felderítőeszközökkel, rádiólokációs zavaró berendezésekkel és passzív rádiólokációs zavarokat létesítő dipolszóró automatákkal szereltek fel. [1]

Rövid idő alatt pótolták a háborús veszteségeket, 1968-ra az egyiptomi haderő mind mennyiségileg, mind minőségileg meghaladta a háború előtti szintet. Nagy hangsúlyt fektettek a légierő és a légvédelem fejlesztésére. Az egyiptomi légierő mintegy 110 db MiG 21-es és 80 db MíG-19-es vadászt, 120 db MiG-17F/PF és 40 db Szu-7-es vadászbombázót, valamint 40 db IL-28-as és 10 db Tu-16-os bombázót kapott. A légvédelem SA-2 és SA-3 rakétaütegek tucatjait telepítette a Csatorna és Kairó közötti területekre. Szíria szintén komoly fejlesztést kapott a szovjet fegyverekből. [2]

1. kép. SA-3 rakétaüteg [8]

Szintén szovjet segítséggel kialakítottak egy távolfelderítő lokátor hálózatot, amely a kor legfejlettebb, P-12-es radarjaiból állt, és amely az elődjeinél nagyobb hatótávolságú, pontosabb és zavarvédettebb volt. 1969. december 26-án éjjel egy izraeli kommandó Ras Gharib közelében megtámadott egy ilyen lokátor állomást, majd a lokátort szétszedték, helikopterre tették és elvitték. Átvizsgálásából igen sok, hasznos információt szereztek, amelyet később fel is használtak az elektronikai hadviselés során. [3]

Izraeli oldalon is folyt a fejlesztés, a hat napos háború miatt, a nemzetközi tiltakozás okán a franciák nem szállították le a beígért Mirage-5-ös vadászgépeket. A francia embargót kihasználva az Egyesült Államok kezdett fegyvereket szállítani Izraelnek. Kaptak légvédelmi rakétarendszereket és könnyű csatarepülőket. is. A Sinai-félszigeten kiépítették a Bar-Lev-vonalat, amely egy erődrendszer volt és a csatorna partján futott.

Az 1967 és 1973 közötti átmeneti időszak az arab országok részéről egyértelműen a következő háborúra történő felkészülés időszaka volt, azonban ezt koránt sem lehet békésnek nevezni. Szinte folyamatosan zajlottak a csatározások földön, vízen, levegőben. Ezen időszakból meg kell említeni az INS Eilat romboló 1967. október 21-i elsüllyesztését, amelyet az egyiptomi haditengerészet egyik Komar osztályú járőrhajáról, két Styx felszín-felszín rakétával hajtottak végre. [3] A kairói hadtörténeti múzeumban két külön terem is foglalkozik ezzel az akcióval. Természetesen a válaszcsapás sem maradt el, az izraeliek haditengerészeti támaszpontokat és kőolaj finomítót támadtak. Az izraeli légierő újonnan beszerzett F-4 Phantom típusú vadászbombázói 1969. november 4-én kora hajnalban 100 méteres magasságban, hangsebesség feletti tempóban áthúztak Kairó fölött. A hangrobbanás ablakok ezreit törte be. 1970-ben szír pilóták követtek el hasonló csínyt Haifában, amire válaszul

Damaszkuszban is fellendült az üvegesek jövedelme, két F-4-esnek köszönhetően. Közben mindkét oldalon gőzerővel folytak a fejlesztések. Az arab országok a csapatlégvédelmük megerősítésén fáradoztak, ehhez a Szovjetunió szállította a lánctalpas, önjáró vázra szerelt SA-6 csapatlégvédelmi rakétát, amelyből járművenként hármat helyeztek el. Ezek lokátoros irányítással kis és közepes magasságú légi célok leküzdésére szolgáltak.

2. kép. SA-6 csapatlégvédelmi rakéták [9]

A másik rendszer vállról indítható SA-7 rakétákból állt, melyek infravörös önirányításúak és kis magasságú célok ellen alkalmazhatóak. Ezt a két rakétás rendszert egészítették ki a ZSZU-23-as önjáró légvédelmi gépágyúk. Ez a lokátoros tűzvezetésű 23 mm-es, négycsöves fegyver olyannyira jó volt, hogy Izrael a zsákmányolt példányokat hadrendbe is állította.

3. kép. Egy zsákmányolt ZSZU–23–4 az izraeli Yad la-Shiryon múzeumban [10]

Az izraeli fél sem tétlenkedett, az elektronikai hadviselés terén nagy lépést tett, amikor megkapta az Egyesült Államoktól az AN/ALQ-87 és AN/ALQ-101 repülőgépre szerelhető zavarókonténereket. Mindkettőt a General Electric gyártotta, az előbbi egy 1-8 GHz-es frekvenciatartományban működő frekvenciamodulált szélessávú zajzavaró eszköz, utóbbi pedig zajzavaró és válaszzavaró üzemmódban is alkalmazható volt. Ezeket az eszközöket az amerikaiak a vietnami tapasztalatok alapján fejlesztették ki. E két eszközzel sikeresen lehetett blokkolni az ellenséges repülők radarját vagy a földi lokátorokat.

Az az állapot, amely 1970. augusztusáig tartott és a világ War of Attriton-nak, magyarul anyagháborúnak nevezett, a hadipotenciálok fejlesztését, heves harcokat hozott. A következő három év, kicsit nyugalmasabban telt, de ez alatt a hat év alatt az arab országok 189 db harci gépet vesztettek, szemben az izraeliek 46 gépes veszteségével. [4] Ez bizonyos szempontból negatív hatással volt az izraeliekre, túlzottan elbízták magukat, nem is gondolták, hogy veszélyben lennének. Ezért a Yom Kippur háború első felében súlyos árat fizettek.

A HÁBORÚ

Yom Kippur, az engesztelés napja. A zsidók egyik legszentebb ünnepe. Ezen a napon szinte megáll az élet Izraelben. Ezt használták ki az arab országok, amikor meglepetésszerű támadást intéztek mindkét fronton a zsidó állam ellen. 1973. október 6-án délután megkezdődött a negyedik arab-izraeli háború.

A harcok három hétig tartottak, és három szakaszra bonthatjuk őket:

- Október 6-9.: az arab hadseregek jól megtervezett, váratlan előrenyomulása, nagy területen történő időszakos térnyerése.
- Október 10-14.: a mozgósítást követően az izraeli hadseregbe beérkeznek a tartalékosok, elindíthatják az ellentámadásokat, a Golán-fennsíkon sikeresen visszaszorítják a szír csapatokat, a Sínai-félszigeten pedig megállítják az egyiptomi csapatok további előrenyomulását.
- Október 15-25.: a Golán-fennsíkon sikerrel verik vissza a szír támadást, így Izrael újabb egységeket dobhat át az egyiptomi frontra, ahol csapást mérhet az ellenséges csapatokra.

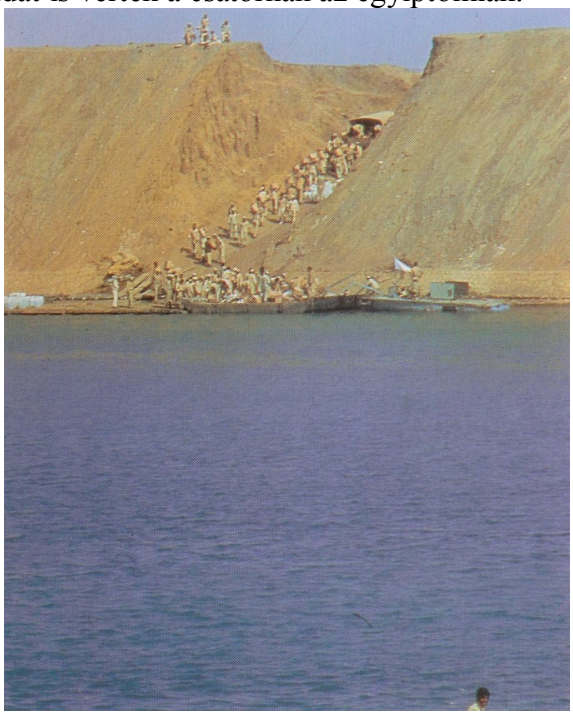
Először bemutatom az egyiptomi front eseményeit, majd a Golán-fennsíkon történteket.

Harcok a Sinai-félszigeten

Az egyiptomi hadsereg éveken keresztül gyakorolta a Nílus-deltában a csatornán való átkelést. Az, hogy ez nem jutott az izraeli hírszerzés fülébe, kisebb fajta csoda számba vehető. Az izraeliek a csatorna partján nem létesítettek összefüggő műszaki zárat, az átkelés elleni védekezésként egy bonyolult csővezetéken keresztül napalmot juttattak volna a csatorna vizére, amit egyszerűen lángba borítottak volna. Egyiptomi búvárok azonban eltömítették ezeket a csővégeket, így ez a fajta védekezés meghiúsult.

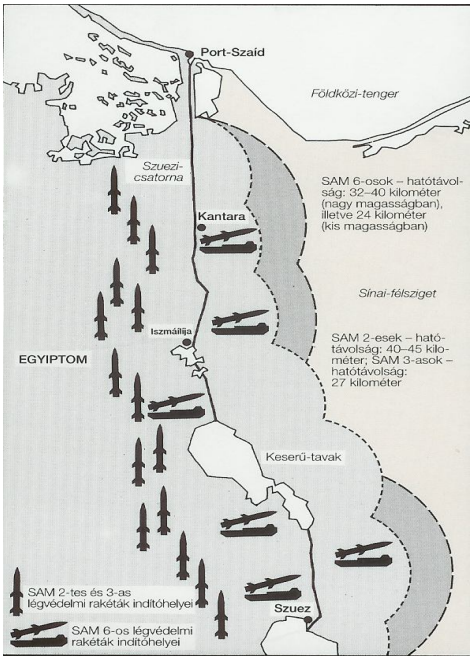
A Szuezi-csatornánál 13.50 perckor 1650 löveg zárótüze által támogatva kezdődött meg a háború. Az egyiptomi csapatok első hulláma több száz rohamcsónakon kelt át a csatornán, elsősorban páncéltörő fegyverekkel felszerelt gyalogságot szállítva, akiknek fő feladata az első vonalban védelembe berendezkedett harckocsik és páncélozott járművek semlegesítése volt, amit sikeresen teljesítettek is. A Bar-Lev-vonal homokfalát 10 helyen vízágyúkkal mosták szét, ami körülbelül egyötödére csökkentette az izraeliek által számolt átjutási időt. A második hullám katonáinak fegyverzetét is még főként páncéltörő eszközök alkották, akiknek

fő feladata már az erődök megszállása és az átkelési pontok biztosítása volt. Az első napon több roham- és pontonhidat is vertek a csatornán az egyiptomiak.



4. kép. Az egyiptomi katonák átkelése a nagynyomású fecskendővel nyitott résen [7]

Október 6-a estére körülbelül 80000 egyiptomi kelt át a csatornán és vetette meg a lábát a túlparton. A nap végére átszállították a légvédelmi rakétákat, így a támadó csapatok rakétafedezet alatt nyomulhattak előre.

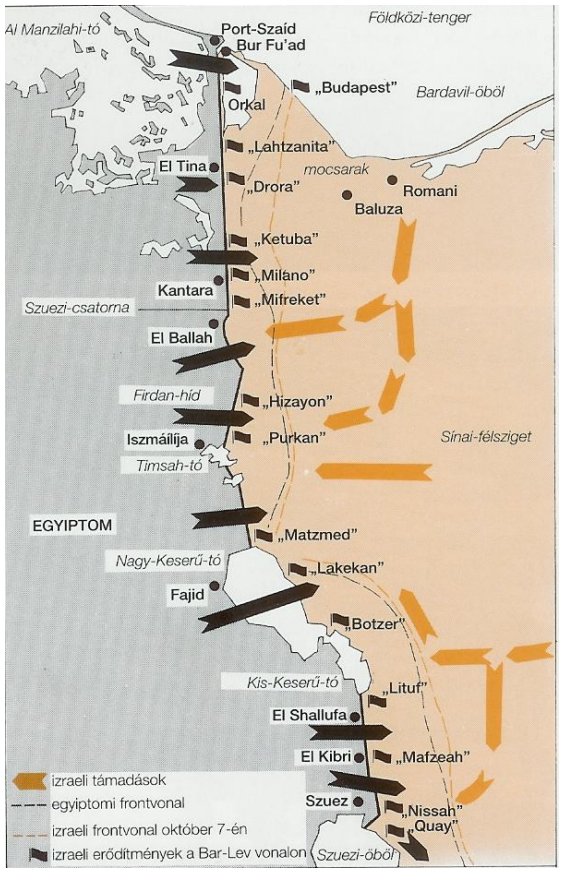


5. kép. Az egyiptomi rakétavédelmi rendszer az átkelés biztosítására [7]

Az izraelieket váratlanul érte a gyors egyiptomi előrenyomulás, és a Bar-Lev-vonal szinte teljes eleste. Az egyiptomi légierő csapásokat mért a félsziget lokátor-, rádió- és zavaróállomásaira, rakétaütegeire valamint három repülőtérre. Az izraeli légierő megpróbálta

akadályozni az átkelést, azonban a hatékonyan kialakított csapatlégvédelem következtében jelentős veszteségeket szenvedtek.

A támadó gyaloghadosztályok átkelésével 5, átlagosan 6-8 km széles és 3-5 km mély hídfő létesült a csatorna keleti partján. Az izraeli kormány elrendelte a teljes mozgósítást és útnak indított két dandárt a csatorna felé.



6. kép. Csapatmozgások a Szuezi-csatorna körzetében [7]

Október 7-én az arcvonal teljes szélességében tovább folytak a harcok, az egyiptomi támadó dandárok tovább nyomultak előre, a hídfőállásokat összefüggővé tették és átlagosan 12 km. mélységűre növelték. Elfoglalták a Bar-Lev-vonal néhány újabb erődjét, a nap végére mindössze a legészakibb, a "Budapest" és a legdélibb, a "Quay" maradt izraeli kézen. A nap folyamán a frontra érkezett két páncélos hadosztály, ezzel a Déli Arcvonalon állomásozó izraeli csapatok létszáma kétszeresére emelkedett (5-ről 11 dandárra). A kiválóan működő egyiptomi légvédelem – köszönhetően az izraeli zavarások kivédésének is – nagyszerű munkát végzett, a második napon 22 izraeli gépet lőttek le. [5]

Izrael légicsapásokat mért egyiptomi repülőterekre, de a légvédelem 17 gépet lőtt le. Itt nagy szerepet kaptak az SA-7 rakéták is. A váratlan, nagyarányú veszteségek arra késztette a légierő vezetését, hogy gyors és hatékony ellenintézkedéseket tegyenek. Az infravörös vezérlésű (önirányítású) rakéták ellen kétféle infracsapdával szerelték fel gépeiket. A MEP típusú 9 vetőcsőből állt. Mindegyik vetőcsőben egy-egy ejtőernyőhöz rögzített, speciális keverékből álló, lőszer formájú hősugárzó volt. A TEP típusú berendezés egy konténer volt, amelyben 5 hősugárzót lehetett elhelyezni. Ezen eszközök hatékonyságát mi sem bizonyítja jobban, mint hogy alkalmazásukat követően jelentősen csökkent az izraeli veszteség. Előfordult, hogy 66 infravörös vezérlésű rakéta indításával egyetlen egy repülőgépet sem sikerült az egyiptomiaknak megsemmisíteniük. [1]

Az izraeli vezetésben kisebb pánikhangulat alakult ki, hiszen senki sem számolt ilyen méretű egyiptomi és szíriai előrenyomulással. A hadsereg vezetői között sem volt egyetértés a teendőket illetően. Voltak olyan vélemények is, miszerint fel kell adni a Bar-Lev-vonal egészét és vissza kell vonulni egészen a Sínai-félsziget hágóiig, majd a helyzet stabilizálódása után lehet egy ellentámadás tervezését megkezdeni. A másik tábor vezetője Saron tábornok volt, aki azonnali ellentámadást sürgetett.

Végül arra a megoldásra jutottak, hogy utánpótlás szempontjából a Golán-fennsík élvez elsőbbséget, mivel ott nincs hely a visszavonulásra, ezért minél gyorsabban meg kell állítani a szír előrenyomulást. Ezért a Bar-Lev-vonalat kiürítik, kisebb ellentámadásokat indítanak, csak annyira közelítik meg a csatornát, hogy az egyiptomi nehéztüzérség közvetlen tüzének még ne legyenek kitéve. Azonban ha a korlátozott ellentámadások során el tudnak jutni a csatorna partjára és ott esetleg el tudnak foglalni egy hidat, akkor átkelhetnek a csatornán és hídfőt alakíthatnak.

Október 8-án az egyiptomi csapatok folytatták erőik átszállítását a csatornán, valamint a hídfőállások megszilárdítását. A terveknek megfelelően az izraeliek megpróbálkoztak egy korlátozott ellencsapással, amely azonban nem vezetett eredményre.

Az elektronikai hadviselés egyik iskolapéldáját hajtotta végre az izraeli haditengerészet október 9-én Baltim térségében az egyiptomiak ellen. A vízfelület közelében Cobra típusú helikopterekkel tengeri célokat imitáltak oly módon, hogy a helikopterek vízközelben a hadihajók sebességével haladtak és rádiókészülékeiket a haditengerészeti rádióforgalmi hálóban üzemeltették. Az egyiptomi hajófedélzeti lokátorok és rádiófelderítők észlelték a jeleket, majd torpedónaszádokról rakétákat indítottak a hadihajóknak vélt célok ellen. Az izraeli helikopterek a rakéták indítását észlelve dipolfelhőt lőttek ki és hirtelen emelkedni kezdtek. Az egyiptomiak elvesztették a célokat, amit úgy értékeltek, hogy megsemmisítették azokat. Eközben a Cobra helikopterek csapást mértek a naszádokra, amelyek közül hármat el is süllyesztettek.[1]

Október 9-13-a között a front vonalában lényeges változás nem történt, a vonalak nagyjából megmerevedtek. Több kisebb támadást mindkét oldalon indítottak, azonban látványos sikereket egyik oldalon sem értek el. Az egyiptomiak újabb erőket szállítottak át a Szuezi-csatornán, amellyel egy október 14-re tervezett támadást készítettek elő, amire a szír vezetés kérte meg őket, mivel ekkorra a Golán-fennsíkon változás állt be a háború menetében. Izraeli oldalon a viszonylagos nyugalmat a veszteségek pótlására és a védelem megerősítésére használták fel.

Az egyiptomi támadás október 14-én 06.00-kor vette kezdetét, hosszabb tüzérségi előkészítést követően. A 2. Hadsereg sávjában a bal szárnyon a 18. gyaloghadosztály 15. páncélos dandárjának Rumána elleni támadása sikerrel indult, azonban ezt a délután folyamán az izraeliek megállították, majd visszaszorították őket kiindulási állásaikba. Középen és a jobb szárnyon is elakadtak a védőkön. A 3. Hadsereg bal szárnyán egy páncélos dandár a Giddi-hágó és a Mitla-hágó elleni támadása során mintegy 10 km-re közelítette meg a hágókat, azonban itt a támadás elakadt. A jobb szárnyon egy páncélos dandár Rász-Szudar ellen indított támadása során körülbelül 20 km-t haladt előre, ekkor azonban az összehangolt páncélos- és légitámadások nyomán összeomlott, majd kiindulási állásaikba vonultak vissza.

Ez alatt a támadás alatt rengeteg páncélost vetettek be, csaknem kétezer harckocsi nézett egymással farkasszemet. [6]

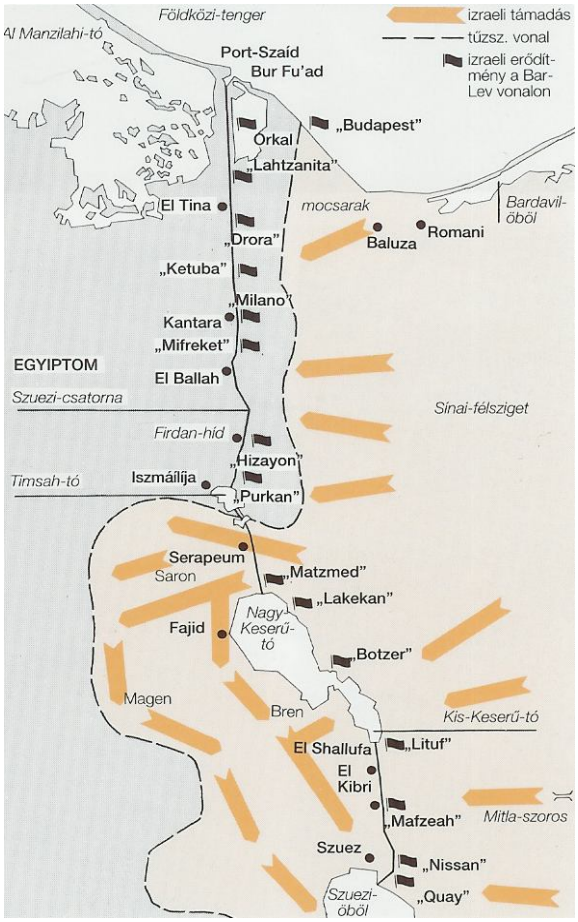
Az egyiptomi támadás azonban eleve kudarcra volt ítélve, mivel a támadásban a csatornán átszállított csapatokhoz képest aránytalanul kevés erőt vetettek be. A 20-22 dandárból mindössze 6-ot. Ennek következtében Izraelnek lehetősége nyílott arra, hogy megkezdje a döntő ellentámadást, amit Saron tábornok már október 7-e óta sürgetett.

A hadművelet a Vízöntő fedőnevet kapta, és lényege az volt, hogy a 2. és a 3. Egyiptomi Hadsereg találkozási pontjánál a Timszah-tó és a Keserű-tavak között, Deversoir közelében 1-2 hadosztállyal átkelnek a Szuezi-csatornán, majd ott hídfőt létesítve eldöntik a háborút. A terv ötletét az adta, hogy a 2. és 3. Hadsereg között egy körülbelül 25 km-es rés mutatkozott a csatorna keleti partján, amelyet az amerikai műholdak és az izraeli légifelderítés mindennap ellenőriztek. [6]

Az hadművelet október 15-én 17.00 órakor vette kezdetét és 16-án 09.00-ra már mintegy 30 harckocsi és 2000 főnyi gyalogság volt a túlparton. Az izraeliek szerencséjére az egyiptomi vezetés nem tett ellenlépéseket az akkor még gyenge hídfővel szemben, valószínűleg nem akarták elhinni a jelentéseket, vagy pedig teljesen meglepődtek ezen a lépésen. [7]

A következő napokban - rendkívül heves harcok közepette - sikerült a hídfőt megerősíteni és kiszélesíteni.

Október 20-ig az izraeli csapatok bekerítettek és felszámoltak jelentős egyiptomi erőket és elérték az el-Sallúfa-Kairo utat és a Szuez-Kairo vasútvonalat.



7. kép. Ellentámadás Szueznél [7]

A két fronton kialakult, - az arab országok szempontjából - egyre kedvezőtlenebb helyzet arra kényszerítette az arabokat, hogy tűzszünet megkötését javasolják, amit az ENSZ és a nagyhatalmak is támogattak. Ennek eredményeként született meg az ún. első tűzszünet, ami október 22-én 18.52 perckor lépett életbe.[6]

Október 22-én az izraeliek növelték a támadások ütemét, tudva, hogy a tűzszünet a nap folyamán életbe lép és jobb pozícióból akartak tárgyalni. A harcok azonban folytatódtak a tűzszünet életbelépése ellenére is, mindegyik fél a másikat vádolta a tűzszünet megsértésével.

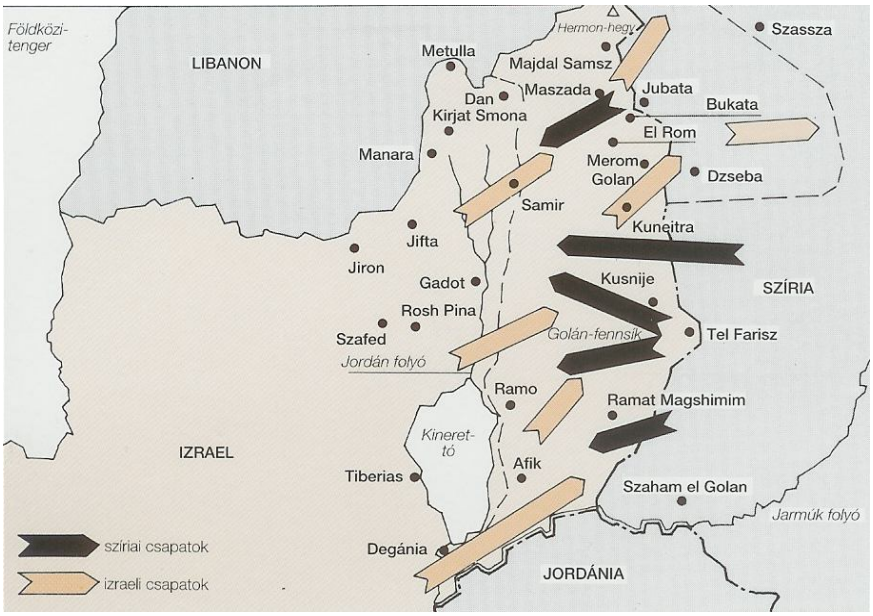
Egy izraeli páncéloshadosztály áttörve az egyiptomi védelmet, elfoglalta Abadiját és kiért a Szuezi-öböl partjára, ezzel bekerítve a 3. Hadsereg erőit.

A tűzszünet életbe lépése után a harcok ellenére a megállapított tűzszüneti vonalak nem változtak. Az izraeli csapatok a 3. Hadsereget végül teljesen bekerítették, habár Szuez városát nem sikerült maradéktalanul elfoglalniuk, ugyanígy a hídfő északi részén lévő Iszmailiját sem sikerült bevenniük. Ennek ellenére az izraeli támadás sikeres volt, hiszen a Szuezi-csatornán túli újabb területszerzéssel, komoly előnyre tettek szert a tűzszüneti tárgyalásokra.

Október 28-a után is folytak még kisebb összecsapások a Sínai-félszigeten, azonban a komolyabb hadműveletek véget értek.

A Golán-fennsík harcai

Az Északi Arcvonalon a szíriai csapatok támadása a Déli Arcvonallal egy időben, 1973. október 6-án tüzérségi és légi előkészítés után 14.20-kor indult.



8. kép. A Golán-fennsík harcai [7]

A szíriai támadást három hadosztály indította. A heves harcokban a sikerült áttörni az izraeli védelmet, a Bíbor vonalat, de nem tudták kibontakoztatni a támadást, mert a védők makacs ellenállásán megtört a lendület. Az Izraeli Légierő is bekapcsolódott a a küzdelembe, de mint ahogy a Déli Arcvonalon, itt is élénk légelhárító tevékenység fogadta őket. Az első délután folyamán 34 gépüket érte rakétatalálat. Mire sikerült kiiktatni a rádiólokátorokat és tűzvezető berendezéseket és visszanyerni a légi fölényt, 80 gépüket vesztették el. [7]

7-én a szíriai ejtőernyőscsapatok elfoglalták a Hermon-hegység csúcsán lévő megfigyelőállást, ahonnan teljesen átláthatták a területet. Az első napon a szíriai támadás délen jól haladt, északon azonban hamar megállították egy gyalogdandár bevetésével.

Október 7-én a szíriaiak minden irányban folytatták a támadást, a főcsapást pedig az arcvonal közepére helyezték át, a Damaszkusz-Illuneitra úttól délre. A nap folyamán folyamatosan érkeztek a frontra mozgósított izraeli csapatok. A délelőtt folyamán az izraeli 7. páncélos dandár kénytelen volt visszavonulni az erőteljes szíriai támadások miatt.

Az arcvonal középső szakaszán a szíriaiak két páncéloshadosztálya megközelítette a Tibériás-tó keleti partját és Kfar-Nafferet, azonban egy izraeli páncélosdandár ellentámadása során estére visszafoglalta a várost. Az arcvonal északi részén az izraeli alakulatok harcolva

vonultak vissza a 7. gyaloghadosztály elől. Az izraeli csapatok az erősítések megérkezése után a Jákob testvérei-híd előtt és a Tibériás-tótól északkeletre megállították az előrenyomuló szír csapatokat.

Október 8-án reggelre az arcvonal középső és déli részén az izraeliek átvették a kezdeményezést, két izraeli hadosztály bekerítéssel fenyegette a szíriai 5. és 1. hadosztályt, melyek ezért 7-8 km-t visszavonultak.Az északi szakaszon azonban nem sikerült megállítani a szíriai erőket, ahol a védekező izraeli erők súlyos vereségeket szenvedtek.

Az összecsapások során az izraeli erők dezinformációs tevékenységének hatékonysága is csökkent. Helyenként ugyan sikerült a szíriai erők megtévesztése, például egy szíriai harckocsi zászlóalj támadási irányát a szíriai csapatvezetés rádióhálójában leadott megtévesztő paranccsal megváltoztatták és a zászlóaljat megsemmisítették, de az előző háborúhoz képest a szírek nagyobb hatékonysággal álltak ellen az elektronikai hadviselés e fajtájának. [1]

Október 9-én reggel a 7. szíriai gyalogoshadosztály továbbfolytatta a támadást, bekerítették és megsemmisítették az izraeli 7. páncélosdandár egyes részeit. Az izraeliek azonban sikeres ellenlökést hajtottak végre a szíriai balszárny ellen és elvágták annak összeköttetéseit, így a szíriai erők kiindulási állásaikhoz vonultak vissza. Tehát így már az északi szakaszon is az izraeliek kezébe került a kezdeményezés.

Október 10-én Irak és Jordánia bejelentette, hogy belép a háborúba és csapatokat vezényel a frontra (Irak két páncéloshadosztály, valamint 100 db repülőgépet, Jordánia pedig egy páncélosdandárt indított el).

Az izraeli hadvezetés eldöntötte, hogy október 11-én döntő ellentámadást indítanak Szíria ellen, a Galán-fennsík északi részéről Damaszkusz irányába. Az izraeli erőket az el-Kuneitra-Damaszkusz irányba csoportosították.

Az ellentámadást négy páncélos ékkel indították, amelyeknek a feladata az volt, hogy átlépve a Bíbor-vonalat áttörjék a szíriai első védővonalat, amely a vonaltól 1-3 km-re húzódott és 5-7 km mély volt, és harckocsi-akadályokkal és aknamezőkkel volt megerősítve.

Az izraeli ellentámadás első napja sikerrel járt, több helyen áttörték a védőövet és 10-15 km-rel visszavetették a szíriai erőket, valamint megközelítették a második védőövet. Ekkor fordult a szír vezetés az egyiptomiakhoz, hogy indítsanak újabb támadást a Sínai-félszigeten az izraeli erők lekötésére.

Eközben a nemzetközi politikában különböző fejleményekre került sor, az Amerikai Egyesült Államok harckészültségbe helyezte erőit, megerősítette a Földközi-tengeren állomásozó 6. flottát, valamint a Szovjetunió is bejelentette, hogy “amennyiben Izrael folytatja bűnös tevékenységét, úgy ezt nem nézheti tétlenül”. A nemzetközi közvélemény is elítélte Izrael újabb területszerzésre irányuló törekvését.

Az izraeli vezetés csapatainak azt a feladatot adta, hogy arcból támadják, illetve délről kerüljék meg a Damaszkusztól 25-30 km-re lévő második védőövet, hogy így Damaszkusz a nagy hatótávolságú tüzérség tüzének hatókörébe kerüljön.

Október 12-én az izraeliek elfoglalták Naszedzset, majd északkeleti irányba, Knaker felé fordult.. Az előrenyomuló hadosztály elérte, hogy előttük páncélos erők bontakozzanak szét ellentámadásra, ezért megálltak, hogy ne sétáljanak bele a csapdába. Bevárták az őket követő páncéldandárt és egy un. tűzzsákot készítettek elő, ahol az ellenséges páncélos erőket csapdába ejthetik és megsemmisíthetik. Mint kiderült ezek a páncélos erők a 3. iraki páncéloshadosztály voltak.

Október 13-án reggel az iraki csapatok megindították a támadásukat, és amikor 2-300 m-re megközelítették a “tűzzsákot” az izraeli csapatok tüzet nyitottak, rövid idő alatt 80 iraki harckocsit kilőttek. Az iraki ellenlökés így meghiúsult, ezután ők is visszavonultak a második

védőövbe, ahová a nap folyamán beérkezett a jordániai páncélos dandár is. Ezen a napon egyébként az izraeli csapatokat feltöltötték és pihentették.

Október 14-én az arcvonal némileg megszilárdult. Október 15-én a szíriai parancsnokság felkészült, hogy a jordániai páncélos dandárral, az idő közben beérkezett szaúd-arábiai páncélos dandárral, a 3. iraki páncéloshadosztállyal és a 9. szíriai gyaloghadosztály egy dandárjával 16-án északi irányban támadást hajtson végre az Izraeli csapatok ellen.

Október 16-án a támadás megindult, ám a 3. iraki páncéloshadosztály állásaiban maradt, ezért az ellentámadás elakadt, így visszatértek kiindulási állásaikba. Délután az irakiak megkésve támadást indítottak, ám rövid idő alatt 60 harckocsit vesztettek és visszavonultak. Az ellencsapás így sikertelen maradt, ezek után két napig csak tüzérségi párbaj folyt és az izraeli légierő szíriai célpontokat bombázott. A zavarótevékenységeknek köszönhetően a szír légvédelem nem volt sikeres a támadókkal szemben.

Október 19-én a szíriai, jordániai és az iraki csapatok több ellenlökést hajtottak végre, sikertelenül. Október 24-én Szíria, Jordánia és Irak is elfogadta az ENSZ 339. sz. határozat tűzszüneti javaslatát, így a harcok az Északi Arcvonalon véget értek. Október 25-én az ENSZ BT-a 340. sz. határozatában a 22-ei tűzszünet harci helyzete alapján határozta meg a tűzszüneti vonalat. [6]

Október 27-én a Déli Arcvonalon is tárgyalni kezdtek az egyiptomi és izraeli erők képviselői a szuez-kairói műút 101-es kilométerkövénél. A megbeszélések november 11-ig tartottak és hat pontban állapodtak meg, amelyek közül az október 22-i helyzet alapján megállapított tűzszüneti vonal váltotta ki a legnagyobb vitát.

November–decemberben Genfben megkezdődtek a békekonferencia előkészületei, melyet követően 1974 január 18-án az izraeli és az egyiptomi vezérkari főnök aláírta a Déli Arcvonalra vonatkozó csapatszétválasztási megállapodást. Ennek lényege a következő volt: Izrael visszavonja csapatait a Szuezi-csatorna nyugati partjáról, a keleti parton levő erői pedig 20-30 km-es sávban csökkentett erővel helyezkednek el; ugyanígy tesznek az egyiptomiak is 8-12 km mélységben a csatorna nyugati partján, majd megnyitja a Szuezi-csatornát, és a Vörös-tenger bejáratát. A két fél között 6-8 km széles "ütközőövezetet" létesítenek, amelyet az ENSZ csapatok felügyelnek.

Az Északi Arcvonalon a kisebb összecsapások 1974 áprilisáig is eltartottak. Májusban a csapatszétválasztási tárgyalásokon némi előrelépés történt, így május 30-án a két fél elfogadta a megállapodást, amit május 31-én alá is írtak.

Ennek lényege a következő volt: Izrael visszavonja csapatait Szassza város körzetéből, kiürít kb. 770 km2 elfoglalt területet; Izrael Kuneitra városból csapatait 300 m-re nyugatra vonja vissza; 500 m-től 4 km-ig terjedő ütközőövezetet hoznak létre az ENSZ erők ellenőrzése mellett, a csapatszétválasztást azonnal megkezdik, a hadifoglyokat kicserélik.

ÖSSZEGZÉS

A negyedik arab-izraeli háború előtt az arab erők komoly fejlesztéseket hajtottak végre haderejükben, beleértve az elektronikai hadviselési képességeiket is. Olyan speciális szakcsapatokat hoztak létre, amelyek hatékony felderítést és zavarást tudtak kifejteni, ugyanakkor ellenállóak voltak az izraeli zavarásoknak is. A csapatlégvédelem fejlesztése óriási méreteket öltött. Izrael kissé elbízta magát, ezért nem fordított kellő figyelmet az arab készülődésekre. Ez odáig vezetett, hogy a háború első szakaszának végére az atomfegyver bevetését is fontolóra vette az izraeli vezetés. Szerencsére azonban a helyzet megváltozása miatt erre nem került sor. A háború után Izraelben is megerősítették az elektronikai hadviselési kutatásokat, fejlesztéseket. Nagymértékben automatizálták a zavarberendezéseket, a korszerűsítették a frekvenciaugratásos rádióállomásaikat.

Ebben a háborúban is egymásnak feszült, ha áttételesen is a két nagyhatalom. A vietnami konfliktust követően, itt is amerikai és szovjet fegyverek álltak egymással szemben. Az alkalmazásukkal kapcsolatos tanulságokat mindkét nagyhatalom felhasználta a további fejlesztésekhez. Megerősödött az a nézet, miszerint az elektronikai hadviselést elsőrendű feladatnak kell tekinteni. A világ majd húsz évvel később, az első Öböl-háborúban tapasztalhatta, hogy ezt komolyan is vették.

Felhasznált irodalom

[1] Bokor Imre - Papp Iván - Várhegyi István: Elektronikus Hadviselés Bp., Műszaki könyvkiadó, 1992. . ISBN: 963 10 9415 4

[2] Gál József: A közel-keleti légi háborúk története Top Gun 1997/9 20-21.oldal ISSN 0866-3165

[3] Mario de Arcangelis: Electronic warfare Blanford Press Ltd. 1985. ISBN 0 7137 1501 4

[4] Gál József: A közel-keleti légi háborúk története Top Gun 199710 22.oldal ISSN 0866-3165

[5] Gál József: A közel-keleti légi háborúk története Top Gun 1998/1 20.oldal ISSN 0866-3165

[6] Réti Ervin: Háború és béke a Közel-keleten. Bp., Zrínyi, 1975. ISBN: 9633260124

[7] Ian V. Hogg: Az izraeli hadigépezet Quatro Puglising Limited, 1983 ISBN: 9638380934

[8] http://forums.bistudio.com/showthread.php?t=37177&page=4

[9] http://en.wikipedia.org/wiki/File:SA-6_Gainful_SAM.JPEG

[10] http://hu.wikipedia.org/wiki/ZSZU-23-4

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

Munk Sándor
munk.sandor@zmne.hu

AZ ADATBÁZIS-BIZTONSÁG SZABÁLYOZÁSÁNAK ALAPJAI A MAGYAR KÖZTÁRSASÁGBAN

Absztrakt

A publikáció az adatbázis biztonság szabályozásával foglalkozik. Ennek érdekében a szerzők megvizsgálják az adatbázis-biztonságot érintő informatikai biztonsággal kapcsolatos szabályozó dokumentumok típusait, bemutatják az adatbázis-biztonság és az informatikai biztonság szabályozási rendszerének jelenlegi szereplőit; végül feltárják a magyar adatbázis biztonsági szabályozó rendszer lehetséges felépítésének lehetőségeit.

The publication studies the regulation of database security. The authors examine the different types of regulatory documents related to information security and database security, describe the different actors of the hungarian information security regulation and finally outline the possible design of the hungarian database security regulation.

***Kulcsszavak**: adatbázis-biztonság, informatikai biztonság, adatbázis-biztonság szabályozása, közigazgatás ~ database security, information security, database security regulation, government*

BEVEZETÉS

Az informatikai biztonság az informatikai rendszer olyan állapota, amelyben az informatikai rendszerben kezelt adatok, valamint a rendszer elemei a fenyegetések ellen a megkívánt mértékben védettek. Az adatbázis-biztonság az informatikai biztonság részterülete, az adatbázis-kezelő rendszerek és az adatbázisokban tárolt adatok olyan állapota, amelyben ezek a fenyegetések ellen a megkívánt mértékben védettek.

A publikációban az adatbázis-biztonság állami szabályozásának kereteit és lehetőségeit vizsgáljuk a magyar viszonyok között. Az informatikai biztonság állami szabályozása a közigazgatás szereplőire és a kritikus infrastruktúrákra vonatkozóan lehet kényszerítő eszköz, ugyanakkor a magán szféra szereplői (saját döntés alapján) felhasználhatják szervezetük informatikai biztonságának biztosítására.

Konkrétan adatbázis-biztonságra vonatkozó szabályozó nem létezik, ezért egy tágabb terület, az informatikai rendszerek biztonságára kiterjedő állami szabályozást tanulmányozzuk és feltárjuk ezek adatbázis-biztonságot érintő vonatkozásait. Mivel a magyar törvényeknek és rendeleteknek összhangban kell állniuk a velük kapcsolatos Európa Uniós szabályozásokkal, a publikációban kizárólag a magyar szabályozókat vizsgáljuk.

Jelen publikáció alapvető célja, hogy megvizsgálja a közigazgatás informatikai rendszerein belül az adatbázis-biztonság szabályozásának lehetőségeit, kereteit. Ennek érdekében a publikáció:

- elemzi adatbázis-biztonságot érintő informatikai biztonsággal kapcsolatos szabályozó dokumentumok típusait, rendeltetését, tartalmát, célközönségét;
- rendszerezi az adatbázis-biztonság és az informatikai biztonság szabályozási rendszerének jelenlegi szereplőit;
- feltárja a magyar adatbázis biztonsági szabályozó rendszer lehetséges felépítését.

ADATBÁZIS ÚTMUTATÓK HELYE AZ INFORMATIKAI BIZTONSÁG DOKUMENTUMAINAK KÖRÉBEN

A következőkben megvizsgáljuk az informatikai biztonságot és a kritikus infrastruktúrákat érintő magyar jogszabályokat és a közigazgatásra vonatkozó ajánlásokat, majd kiemeljük ezek adatbázis-biztonságot érintő aspektusait.

Jogszabályok

Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény [1] határozza meg a központi elektronikus szolgáltató rendszer útján nyújtott elektronikus közszolgáltatások alapelveit, szabályait, használatának feltételeit. A törvény az elektronikus közszolgáltatások biztonságáról általános alapelveket fogalmaz meg, leírja például, hogy az elektronikus közszolgáltatás nyújtónak biztosítania kell az alkalmazott informatikai és kommunikációs rendszerek műszaki megfelelőségét és biztonságos működésének feltételeit. A törvényben felhatalmazást kap a Kormány arra, hogy rendeletben állapítsa meg a központi rendszer működtetésével, valamint szolgáltatásainak igénybevételével összefüggő részletes informatikai-biztonsági, adatbiztonsági követelményeket. Ennek kapcsán jött létre a 223/2009. (X. 14.) Kormányrendelet.

A 2009. évi LX. törvény felhatalmazása alapján létrejött *223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatás biztonságáról* [2] a közszolgáltatást végző informatikai rendszerek személyi, szervezeti és műszaki követelményeit tartalmazza - a következőkben szintén ismertetett - KIB 25. és 28. ajánlásokkal összhangban. A kötelező

erővel bíró rendelet hatálya az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, és igénybe vevőire terjed ki és kimondottan informatikai biztonsági szempontokat tárgyal.

A rendeletben találunk az adatbázis rendszer – mint az informatikai rendszer részrendszere - biztonságát érintő követelményeket, előírásokat is. A kormányrendelet adatbázis-biztonságot is érintő főbb előírásai a következők:

- Az elektronikus közszolgáltatásoknak a rendszerben tárolt adatokra nézve meg kell valósítaniuk a bizalmasság, sértetlenség, rendelkezésre állás és kockázatarányos védelem elveit.
- Az elektronikus közigazgatási rendszerek biztonsági felügyeletét a közigazgatási informatikáért felelős miniszter látja el, aki a feladat ellátására az irányítása alá tartozó informatikai biztonsági felügyelőt jelöli ki.
- A magyar kritikus információs infrastruktúra védelméért a Nemzeti Hálózatbiztonsági Központ a felelős. Az elektronikus közszolgáltatás alapját képező Központi rendszer a kritikus infrastruktúra része, védelmét a kritikus infrastruktúrára vonatkozó, nemzetközileg kialakult biztonsági követelményeknek megfelelően kell kialakítani.
- Az elektronikus közszolgáltatást működtető szervezetnek információbiztonsági irányítási rendszert kell létrehozniuk. Ezen belül meg kell valósítani a minőségbiztosítást és szabályzati rendszert kell létrehozni. A rendelet a KIB 25. és 28. ajánlásokkal összhangban lévő dokumentáltsági követelményeket fogalmaz meg. A rendelet kimondja a következőket:

  „a tárolt és kezelt adatok biztonsága érdekében szolgáltatásműködési szabályzatot kell készíteni, meg kell határozni a rendszer működéséért felelős, az adatgazda, az adatkezelő, illetőleg az adatfeldolgozó, az üzemeltető és az igénybe vevők jogait és kötelezettségeit, valamint az adatkezelés, adattovábbítás és adatszolgáltatás eljárásrendjét”

  „az informatikai rendszerben forgalmazott adatok illetéktelen személy által történő megismerhetőségének megakadályozását elektronikus úton kell biztosítani az adatok keletkezési helyétől azok végső tárolási helyéig bezárólag, beleértve az adatok nyilvános hálózaton történő forgalmazását is”
- A kritikus rendszereket naplózni, menteni és archiválni kell.
- Adattovábbítás során kriptográfiai megoldásokat kell használni az adatok titkosítására.
- A hozzáférés-védelmet mind logikai, mind fizikai szinten gondosan meg kell tervezni és valósítani.
- Az üzemeltetés biztonságai elveinek kialakítása során a legjobb gyakorlatokra kell alapozni.
- Az elektronikus közszolgáltatásokat biztonsági auditnak kell alávetni az erre felhatalmazott szervezet által.
- Az elektronikus közszolgáltatás egyes elemeit biztonsági osztályokba kell sorolni, meg kell határozni az egyes biztonsági osztályokhoz tartozó védelmi szinteket és biztonsági követelményeket. A szolgáltatást nyújtó szervezetnek a biztonsági osztályba sorolást és a meghatározott védelmi szinteket az informatikai biztonsági tervében meg kell jelenítenie.

Informatikai rendszerekben tárolt és kezelt adatokra vonatkozóan számos, különböző vonatkozásokkal bíró törvény és kormányrendelet foglalkozik. Említést érdemelnek a

személyes adatok védelmével, a közérdekű adatok nyilvánosságával, illetve a minősített adatok kezelésével foglalkozó jogszabályok [3], [4], [5], [6]. Ezek az adatbázis-biztonság témáját csak nagyon távolról érintik, részletesebb vizsgálat a publikáció kereteibe nem fér bele.

Mivel a közigazgatás informatikai rendszerei a kritikus információs infrastruktúra részét alkotják, a kritikus infrastruktúra hazai szabályozását is vizsgálnunk kell. A magyar kormány a Kritikus Infrastruktúra Védelem Európai Programja hatására kiadta a *2080/2008 (VI. 30.) Korm. Határozatot a Kritikus Infrastruktúra Védelem Nemzeti Programjáról* [7], mely mellékletként a hazai Zöld könyvet is tartalmazza. A határozat általánosságokban tárgyalja a kritikus infrastruktúra fogalmait, a különböző ágazati hatáskörbe tartozó kritikus infrastruktúra védelmi tevékenységek feladatait és kereteit. A határozat a kritikus infrastruktúrákat 10 ágazatba és azon belüli alágazatokba sorolja, az ágazatokhoz kormányzati szerepkörrel bíró felelősöket rendel. A közigazgatási szolgáltatások alágazat a Jogrend – Kormányzat ágazat részeként szerepel a dokumentumban. Az informatikai biztonság témáját a határozat csak nagyon felületesen érinti.

Ajánlások

A következőkben a kormányzati informatikai rendszerek biztonságos működését elősegítő, de jogi értelemben nem kötelező erejű ajánlásokkal foglalkozunk. A Közigazgatási Informatikai Bizottság (a továbbiakban: KIB) az elektronikus közszolgáltatások biztonságos működésének elősegítése céljából adta ki 2008-ban a 25. számú és 2009-ben a 28. számú ajánlásait [8], [9]. A kötelező erejű 223/2009. (X. 14.) Korm. rendelet az ajánlásokkal összhangban született meg. A *KIB 25. számú ajánlása* a Magyar Informatikai Biztonsági Ajánlások (MIBA) címet viseli. Ez tulajdonképpen egy ajánlássorozat, amelynek fő célja, hogy nemzetközi szabványokhoz és ajánlásokhoz igazodva biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A MIBA három fő részből áll:

A *Magyar Informatikai Biztonsági Keretrendszer (MIBIK)* [10] szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól. A MIBIK az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR) [11], amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK) [12], amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV) [13], amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A *Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)* [14] technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre. A MIBÉTS az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokon, illetve a nemzetközi legjobb gyakorlatokon és nemzeti sémákon alapul. Keretet biztosít arra, hogy az informatikai termékek és rendszerek tekintetében a biztonsági funkciók teljessége és hatásossága értékelésre kerüljön. Értékelési módszertana alkalmas az operációs rendszerek, hardverek (pl. hálózati eszközök, tűzfalak, behatolás észlelők, intelligens kártyák), szoftveralkalmazások (pl. különböző programnyelveken megírt kritikus

alkalmazások) speciális biztonsági szempontjainak értékelésére. Ezzel a MIBÉTS a megbízható harmadik felek által végzett biztonsági ellenőrzés és audit egységes szempontrendszerét alkotja meg.

Az *Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)* [15] olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel. Az IBIX elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben. Javasolt az anyag azon szervezetek számára, ahol a szervezet méreténél fogva nem áll rendelkezésre külön emberi és egyéb erőforrás az informatikai rendszerek biztonságának kialakítására és üzemeltetésére, hanem ezt „házon belül" kell megoldani.

A *KIB 28. számú ajánlása* [9] egy Követelménytár, amely az elektronikus közigazgatás fejlesztéséhez és üzemeltetéséhez szükséges szabványokat, követelményeket, előírásokat és információs anyagokat tartalmazza, az ajánlás webes felületen megjelenő segédeszköznek is tekinthető. Az *IT biztonsági követelmények*, és a *Termékek, szolgáltatások értékelésének, auditjának előkészítése* a 25. számú ajánlásra épülve, azt kiegészítő vagy végrehajtását támogató előírásokat, mintákat és követelményeket tartalmaz, illetve az *Egyéb követelmények, ajánlások* számos biztonsági szabványt, módszertant mutat be.

Az IT biztonsági követelmények részei:

- Biztonsági tervezési útmutató;
- IT biztonsági követelményrendszer - biztonsági szintek követelményei;
- IT biztonsági Követelményrendszer érvényesítésének módja;
- IT Biztonsági Politika követelményei;
- IT biztonsági stratégia követelményei;
- IT Biztonsági szabályzatok követelményei;
- IT biztonsági szintek és biztonsági kategorizálási minta;
- Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere;
- Szabályzatmenedzsment rendszer követelményei;
- Útmutató az IT biztonsági szintek meghatározásához.

Termékek, szolgáltatások értékelésének, auditjának előkészítése rész tartalma:

- IT biztonsági értékelő labor koncepció;
- Létező tanúsítások megfeleltetése - Technikai leírás;
- Összetett termékekre vonatkozó értékelési módszertan;
- Rendszerekre vonatkozó értékelési módszertan;
- Termékekre vonatkozó értékelési módszertan;
- Útmutató akkreditorok számára;
- Útmutató rendszer-értékelők számára;
- Útmutató rendszer-integrátorok számára;
- Útmutató tanúsítók számára.

Dokumentumok értékelése, összegzése

Az informatikai biztonsággal kapcsolatos jogszabályokból és ajánlásokból az adatbázis-biztonság szabályozására nézve a következő pontokat tartom fontosnak kiemelni.

- Jelen pillanatban kimondottan adatbázis-biztonság szabályozásával jogszabályok és ajánlások nem foglalkoznak. Az elektronikus közszolgáltatás biztonságát szabályozó 223/2009. számú kormányrendeletnek vannak adatbázis-biztonságot érintő előírásai, a rendelet egy esetleges adatbázis-biztonság szabályozás számára a kereteket adja meg. A jövőben megszülethet a szükséglet arra –például a kritikus infrastruktúrák védelmének szabályozása kapcsán-, hogy jogszabályi vagy ajánlási szinten is megjelenjen az adatbázis-biztonság szabályozása.

- Az adatbázis-biztonság szabályozásának szervezeti szintjén a rendszabályoknak illeszkedniük kell a szervezet informatikai biztonsági szabályzatainak, dokumentumainak rendszerébe. A közigazgatási informatikai rendszerek szervezeti szintű biztonsági szabályozásának elemeit a 223/2009. számú kormányrendelet is tartalmazza, a KIB 25. számú ajánlás IBIR kötete pedig részletesen meghatározza a következők alapján:

  - *Informatikai Biztonsági Politika (IBP):* „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során.”

  - *Informatikai Stratégia:* „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú).”

  - *Informatikai Biztonsági Szabályzat (IBSZ):* „Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat, megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információ-feldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológia független tudjon maradni.” Az Informatikai Biztonsági Szabályzat nagyobb szervezeteknél kétszintű legyen. A szervezeti szintű IBSZ tartalmazza az általánosan és mindenre érvényes részletesebb szabályokat, míg a rendszer-specifikus szabályokat a rendszerszintű IBSZ tartalmazza.

  - *Informatikai Felhasználói Szabályzat (IFSZ):* „A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket.”

  - *Eljárásrend gyűjtemény:* „Az eljárásrend gyűjteménybe tartozó végrehajtási. utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszer függetlenül megkövetel.”

Az adatbázis-biztonsági rendszabályok a fenti szabályozási dokumentumok közül az Eljárásrend gyűjtemények körébe beilleszthetők. Bizonyos esetekben – például kritikus adatbázisokat üzemeltető szervezetek esetén – az Informatikai Biztonsági Szabályzatban is szükséges lehet egy részt az adatbázis rendszerek biztonsági szabályozására fordítani. Önmagában azonban egy jó eljárásrend kiadása még kevés, használatát elő kell írni. Szintén elő kell írni, hogy a külső és belső informatikai biztonsági auditok során az alkalmazását vizsgálni kell.

- A jogszabályokban és a szervezeti szintű szabályzatokban megtalálható, az adatbázis rendszerek biztonságos üzemeltetésével kapcsolatos előírásoknak (például mentés, naplózás, audit) összhangban kell lenniük az adatbázis-biztonsági rendszabályokban meghatározott előírásokkal.
- Az adatbázis-biztonsági rendszabályok követelményeinek függniük kell a tárolt adatok, illetve az adatbáziskezelő-rendszer biztonsági kategóriájától. Tehát az adatbázis-biztonság szabályozásának megvalósításánál az informatikai rendszerek és a feldolgozott információk biztonsági szintjeinek osztályozását figyelembe kell venni.

A KIB 25. és 28. számú ajánlása szerint (legalább) három szinten kell az informatikai rendszerek védelmét megvalósítani: (1) kiemelt szint, mely a minősített adatokat feldolgozó rendszereket jelenti, (2) fokozott szint, mely a belső használatú, bizalmas információkat kezelő rendszerekre vonatkozik, valamint (3) az alap szint, mely a széles körben, interneten keresztüli hozzáférést biztosító rendszerek védelmi szintje. A KIB 28. számú ajánlásban megtalálható IT biztonsági szintek megállapításának módja a következő három lépésből áll össze:

1. lépés: A tárolt adatok biztonsági kategóriájának megállapítása

A három biztonsági célra (bizalmasság, sértetlenség, rendelkezésre állás) külön-külön meg kell állapítani a biztonsági szintet, melynek lehetséges értékei: nem értelmezhető, alacsony, fokozott, kiemelt. (A nem értelmezhető szint csak a bizalmasság biztonsági célra vonatkozhat.)

2. lépés: Az informatikai rendszer biztonsági kategorizálása a biztonsági célok alapján

Az informatikai rendszert kell besorolni a bizalmasság, sértetlenség és rendelkezésre állás biztonsági célok alapján biztonsági osztályok (alacsony, fokozott, kiemelt) egyikébe. Az informatikai rendszerek biztonsági kategorizálásakor meg kell vizsgálni a rendszerben tárolt, feldolgozott, továbbított minden információ típus biztonsági kategorizálását, és ezen információk alapján kell megállapítani a rendszerhez rendelt biztonsági kategóriát. A három biztonsági célra (bizalmasság, sértetlenség, rendelkezésre állás) vonatkozóan külön-külön meg kell határozni a rendszerszintű biztonsági kategóriát, az egyes információ típusokra kapott legmagasabb értékek megállapításával.

3. lépés: Az informatikai rendszer biztonsági kategorizálása

A teljes informatikai rendszerre kell megállapítani egy biztonsági kategóriát. Az alacsony biztonsági kategóriájú rendszerben mindhárom biztonsági cél szerinti biztonsági kategória alacsony szintű. A fokozott biztonsági kategóriájú rendszerben legalább az egyik biztonsági cél fokozott szintű, és nincs fokozottnál erősebb szintű biztonsági cél. Végül a kiemelt biztonsági kategóriájú rendszerben legalább az egyik biztonsági cél szerinti biztonsági kategória kiemelt szintű.

A 223/2009. (X. 14.) Kormányrendelet is kimondja, hogy az adatokat érzékenységük és kritikusságuk szempontjából osztályozni kell. Az alkalmazásokat és az infrastruktúra elemeit a kezelt adatok biztonsági osztályával összhangban kell besorolni biztonsági osztályokba. A fejlesztők és üzemeltetők a biztonsági besorolásnak megfelelő adminisztratív és technikai védelmet kell, hogy kialakítsanak. A rendelet által előírt osztályozás nem teljesen egyezik a

KIB ajánlásokban található osztályozási rendszerrel, három helyett öt kategória használatát írja elő, melyek a következők:

(1) Különlegesen védendő (minősített) adatok, amelyekhez a belső és külső hozzáférés csak erősen korlátozva, szigorúan ellenőrizve és dokumentálva engedélyezhető,

(2) Érzékeny adatok, amelyekhez a belső és külső hozzáférést korlátozni, a hozzáférést naplózni kell,

(3) Belső adatok, amelyekhez a külső hozzáférés nem lehetséges, belső hozzáférés korlátozása nem kritikus,

(4) Nyilvános, közhiteles adatok, ahol a rendelkezésre állás és a megváltoztathatatlanság biztosítása kritikus,

(5) Általános kezelésű adatok.

ADATBÁZIS BIZTONSÁGI ÉS AZ INFORMATIKAI BIZTONSÁG SZABÁLYOZÁSI RENDSZERÉNEK SZEREPLŐI

Mint azt korábban már bemutattuk, az adatbázis biztonság önmagában általában nem képezi szabályozás tárgyát, vagy az informatikai biztonság, illetve a kritikus információs infrastruktúrák védelmének részeként jelennek meg adatbázis biztonsági szabályozási elemek, vagy ezen szabályozások előírásai érvényesítendőek, adaptálhatóak az adatbázis biztonság területére. Ennek megfelelően a következőkben az informatikai biztonság és a kritikus információs infrastruktúra védelem szabályozási rendszerének felépítését vizsgáljuk meg, bemutatva annak szereplőit, feladat- és hatásköreit (feltárva az esetleges adatbázis biztonsági sajátosságokat). A szabályozási rendszer két nagy szférára (szintre) osztható, amelyből az első a kormányzati szintű szabályozás, a második az intézményi szintű szabályozás. Ez utóbbit részben – meghatározott körben – a kormányzati szabályozás írhatja elő, más része az intézmények (szervezetek) saját döntésének függvénye.

A kormányzati szintű szabályozási rendszer szereplői

Az informatikai szakterületi feladatok a Magyar Köztársaságban kormányzati szinten két nagy területre oszthatóak:

- - a közigazgatási informatika fejlesztése: a közigazgatás működésének javítása, az e-közigazgatás fejlesztése (cél: az állampolgárok minél magasabb szintű kiszolgálása);
- - az informatikai szolgáltatások körének, elérhetőségének bővítése: az informatika társadalmi, gazdasági, kulturális, oktatási, stb. célú alkalmazásának támogatása (cél: az információs társadalom kialakulásának elősegítése).

A kormányzati szintű szabályozási rendszer szereplői két nagy csoportba sorolhatóak. Az elsőbe a jogszabályok[1] előkészítésében érintett szereplők, a másodikba az ajánlások kidolgozásában részt vállaló szereplők sorolhatóak. A kormányzati szabályozási rendszer szereplői más szempontból csoportosíthatóak az állami vezetőkre (miniszterek, államtitkárok, helyettes államtitkárok), az irányításuk alatt álló minisztériumi (pld. főosztály-) vezetőkre és más szerepkörökre, illetve különböző kormányzati irányítás alatt álló, vagy kormányzati megbízás alapján feladatot ellátó bizottságokra, szervezetekre és hatóságokra.

A jogszabályok előkészítése a szakmailag illetékes miniszter feladata. A miniszterek feladat- és hatáskörét legmagasabb szinten a miniszterek feladat- és hatáskörét szabályozó kormányrendelet [16], valamint az egyes törvények képezik. Az állami vezetők feladat- és hatásköre az informatikai biztonságot átfogó módon nem tartalmazza. 2010 óta az e-

[1] Törvény, kormányrendelet, miniszterelnöki rendelet, miniszteri rendelet és más rendeletek.

közigazgatásért a *közigazgatási és igazságügyi miniszter*, a postaügyért, az audiovizuális politikáért, az informatikáért, a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért és az elektronikus hírközlésért pedig a *nemzeti fejlesztési miniszter* felelős. [16, 2. és 84. §] A nemzeti fejlesztési miniszter feladatai között – a közigazgatási intézményekre és az állami, vagy részben állami tulajdonban lévő társaságokra vonatkozóan – szerepel az informatikai biztonsági előírások megfelelőségének, betartásának ellenőrzése, valamint az informatikai biztonságért felelős vezetőkkel kapcsolatos jogok.

Az informatikai és ezen belül az adatbázis-biztonsági kérdésekhez szorosan kapcsolódó, a személyes adatok, illetve a minősített adatok védelmének szabályozási feladatai a *közigazgatási és igazságügyi miniszter* feladat- és hatáskörébe tartoznak.

A kritikus információs infrastruktúrákhoz kapcsolódó feladatok önállóan szintén nem jelennek meg, a kormányrendeletben egyedül a *belügyminiszter* kritikus infrastruktúra védelmi kormányzati koordinációs feladata, valamint a katasztrófák elleni védekezéssel kapcsolatos feladatkörében az infrastruktúra kritikus elemeivel kapcsolatos jogszabály-előkészítési és rendeletalkotási joga szerepel.

A miniszterek feladat- és hatáskörének megvalósítási rendjét, ezen belül a további állami vezetők (államtitkárok, helyettes államtitkárok) feladat- és hatáskörét, valamint az alapvető minisztériumi szervezeti egységek (főosztályok) feladatait az egyes minisztériumok Szervezeti és Működési Szabályzatai rögzítik. Eszerint az informatikához kapcsolódó miniszteri feladatkörök megvalósítása a Közigazgatási és Igazságügyi Minisztériumban a közigazgatási államtitkár irányítása alatt az *e-közigazgatásért felelős helyettes államtitkár*, a Nemzeti Fejlesztési Minisztériumban az *infokommunikációért felelős államtitkár* és irányításával a *kormányzati informatikáért*, illetve a *hírközlésért és audiovizuális médiáért felelős helyettes államtitkárok* feladata. [17, 61. §; 18, 21. §] Az államtitkári feladatok között informatikai biztonsághoz kapcsolódóak nem találhatóak.

A *Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala* a közigazgatási és igazságügyi miniszter – illetve egyes tevékenységek tekintetében a belügyminiszter, illetve a nemzeti fejlesztési miniszter – irányítása alatt álló központi hivatal, amelynek alaprendeltetése országos alapnyilvántartások vezetése, a közigazgatás korszerűsítésében való részvétel, ügyfélbarát közigazgatási eljárások kidolgozása, valamint az elektronikus közszolgáltatások továbbfejlesztése. Feladatai között szerepel a közreműködés a közigazgatási informatikai biztonsági politika kialakításában. [19, 6.2.a.14]

Az elektronikus közszolgáltatások biztonságáról szóló kormányrendeletben meghatározásra kerül a közigazgatási informatikáért felelős miniszter irányítása alatt működő *informatikai biztonsági felügyelő*, amelynek feladata az elektronikus közszolgáltatást nyújtó rendszerek eljárási és biztonsági követelményeknek való megfelelőségének felügyelete, ellenőrzése. [20, 5-6. §] Az informatikai biztonsági felügyelő feladatkörében azonban szabályozási feladatok nem szerepelnek.

Ugyanezen kormányrendeletben jelenik meg a közigazgatási informatikáért felelős miniszter felügyelete és az informatikai biztonsági felügyelő ellenőrzése alatt álló *nemzeti hálózatbiztonsági központ*, amelynek alaprendeltetése – a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikáció biztonsága, a vírus- és más támadások káros hatásainak korlátozása érdekében – a központi rendszer szolgáltatásait az Interneten keresztül érő támadások elleni védelem. Nevesített feladatai közé tartozik az informatikai és a hálózatbiztonságra, valamint a kritikus információs infrastruktúrák védelmére vonatkozó stratégiák és szabályozások előkészítésében történő részvétel.

A Nemzeti Hálózatbiztonsági Központot a kormány és más szervezetek által 2009-ben alapított *Puskás Tivadar Közalapítvány* működteti, az Országos Informatikai és Hírközlési

Főügyelet ügyeleti rendszerével párhuzamosan. Az elektronikus közigazgatás kialakítása és fejlesztése érdekében a központ feladatai közé tartozik a részvétel a közigazgatási informatikai biztonsági politika, az ellenőrzési rendszer és a megvalósításához szükséges alapfeltételek, valamint szabályozás kidolgozásában. [21, 16. o.]

A *Nemzeti Biztonsági Felügyelet* a közigazgatási és igazságügyi miniszter irányítása alatt álló, a Közigazgatási és Igazságügyi Minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező szervezet, amelynek rendeltetése a minősített adatok védelmének hatósági felügyelete, kezelésük hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása. A felügyelet konkrét szabályozási feladatokkal nem rendelkezik.

A *Közigazgatási Informatikai Bizottság* a kormány által 2007-ben létrehozott kormánybizottság [22], amelynek rendeltetése a szolgáltató állam kiépítésének meggyorsítása, az állampolgárbarát, gazdálkodóbarát közigazgatás megvalósítása, az informatika eredményeinek a közigazgatás egészében való terjesztése. A bizottság feladatkörébe tartozik többek között a közigazgatási informatikához kapcsolódó informatikai műszaki, biztonsági előírásokra vonatkozó szabályozások kezdeményezése, ajánlások elfogadása. [22, 5.c] A Közigazgatási Informatikai Bizottság és jogelődjei eddig hat informatikai biztonsági témájú ajánlást (ajánláscsomagot) fogadtak el.[2]

A *Kormányzati Koordinációs Bizottság* a kormány által a katasztrófavédelmi törvény felhatalmazása alapján 1999-ben létrehozott bizottság, amelynek rendeltetése a katasztrófák következményeinek felszámolására való felkészülés, a megelőzés és a végrehajtás feladatainak tárcák közötti koordinációja. A bizottságot 2010-től a belügyminiszter vezeti, tevékenységét a belügyminisztérium és az Országos Katasztrófavédelmi Főigazgatóság támogatja.

A kormány 2008-ban a KKB javaslatára fogadta el Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló Zöld Könyvet [23] és elrendelte a hazai infrastruktúra létfontosságú elemeinek védelméről szóló szabályozási koncepció összeállítását. 2010 őszére volt tervezve egy kritikus infrastruktúra védelmi törvény elfogadása, erre azonban nem került sor.

A bemutatott – esetenként potenciális – szereplők, illetve feladat- és hatáskörük alapján ***összegzésképpen*** a következők fogalmazhatóak meg. Az informatikai biztonság átfogó szabályozása nem szerepel a magyar kormányzati szabályozásban, helyette más – szűkebb – megközelítésű biztonsági szakterületek, mindenekelőtt a személyes adatok védelmének, a minősített adatok védelmének, illetve az elektronikus közszolgáltatások biztonságának szabályozásaival találkozhatunk. Ezek törvények és kormányrendelet formájában kerültek kiadásra. A kör a jövőben várhatóan bővülni fog a kritikus információs infrastruktúrák védelméhez kapcsolódó szabályozásokkal. A szabályozásokhoz kapcsolódóan az alapvető szerepet a jogszabályt előkészítő, feladat- és hatáskör szerint illetékes állami vezetők és minisztériumok játsszák.

Az eltérő megközelítésű, de az informatikai biztonsági kérdések esetében egymáshoz szorosan kapcsolódó szabályozások még ugyanazon minisztérium esetében sem állnak egymással teljes összhangban. Számos példa mutatható eltérő fogalmakra, kifejezésekre, értelmezésekre, eltérő elvekre és megoldásokra. Az aktuális jogszabályok fogalomrendszere nem egyezik meg a nemzetközi szabványok és bevált gyakorlatok alapján kidolgozott Magyar Informatikai Biztonsági Ajánlásokkal sem. Mindez a különböző jogszabályok hatálya alá tartozó tevékenységek – pld. minősített és személyes adatokat is kezelő közigazgatási

[2] ITB 8. (Inf. bizt. módszertan), ITB 12. (Inf. rsz. biztonsági követelményei), ITB 16. (Common Criteria), KIB 25. (Magyar Inf. Bizt. Ajánlások), KIB 26. (elektronikus azonosítás), KIB 28. (E-közigazgatási keretrendszer Követelménytár).

informatikai rendszerek – esetében megnehezíti az informatikai biztonság irányítását és megvalósítását.

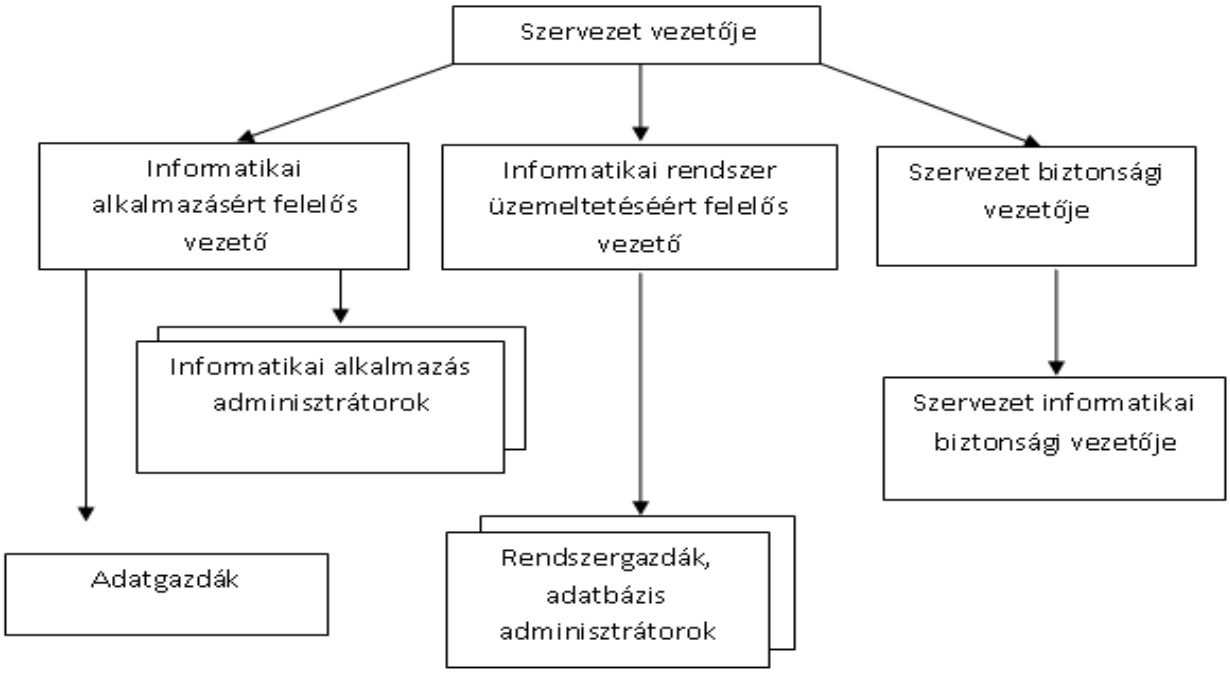
Az informatikai biztonság kormányzati szabályozása, valamint bármely szervezet informatikai biztonsági tevékenysége során felhasználható ajánlások kidolgozásának alapvető szereplője a Közigazgatási Informatikai Bizottság, amely összetétele alapján hosszú távon is megfelelő eszköze a széles körben hasznosítható dokumentumok megvitatásának és elfogadásának, ezzel a korszerű nemzetközi megoldások honosításának. Az ajánlások kidolgozásában – amire kormányzati, vagy szakmai kezdeményezésre, kormányzati fejlesztési tervek, programok, illetve megbízási szerződések keretében kerülhet sor – különböző állami, piaci és civil szervezetek vehetnek részt.

Az informatikai biztonságnak az átfogó nemzeti biztonságon belül, a közigazgatási informatikában és az információs társadalom építésében előre láthatóan egyre növekvő jelentősége miatt, az eredményes és hatékony, egymással harmonizáló megoldások érdekében megítélésünk szerint szükség lenne az informatikai biztonsággal kapcsolatos különböző szabályozások összehangolására, egy ezzel kapcsolatos koordinációs feladatkör megfogalmazására és ennek – a jelenlegi helyzetben – a közigazgatási és igazságügyi miniszterhez rendelésére. Mindezt a jelenlegi szabályozási területek, hatóságok és háttérintézmények önállóságának megtartásával célszerű megvalósítani.

Az intézményi szintű szabályozási rendszer szereplői

A 223/2009. (X. 14.) Kormányrendeletben is követelményként jelenik meg, hogy a szervezeten belül a biztonsági feladatok ellátására és ellenőrzésére azonosítható szerepköröknek kell rendelkezésre állniuk. Az adatbázis-biztonság szabályozása kapcsán megjelenő feladatokat társítani kell az informatikai biztonság szervezeti struktúrájában megjelenő különböző szerepkörökhöz. A következőkben ezek áttekintését végezzük el.

Az informatikai rendszer biztonságával kapcsolatos szerepköröket és ezek egy lehetséges kapcsolatrendszerét a következő ábra szemlélteti (a nyilak a közvetlen alá-fölé rendeltségi viszonyt jelzik).



1.ábra. Szervezeti szerepkörök az informatikai biztonság területén

Szervezet vezetője

Felelősségi körébe tartozik az elektronikus információvédelem gyakorlati megvalósítása, az elektronikus információvédelemre vonatkozó jogszabályok és előírások betartása, betartatása. Feladatkörébe tartozik a szervezet informatikai biztonságának személyi, szervezeti és pénzügyi feltételeinek megteremtése, a biztonsággal kapcsolatos felelősségi körök szabályozása, az informatikai biztonsági politika és stratégia kidolgoztatása, illetve megvalósítása. Rendszeresen kell ellenőriznie a bevezetett intézkedések betartását, hatékonyságát és gazdaságosságát [24].

Biztonsági Vezető

A szervezeten belül a biztonság komplex kezeléséért felelős. Gondoskodik az informatikai biztonságra vonatkozó jogszabályok, illetve az informatikai biztonságpolitika, az informatikai stratégia és az Informatikai Biztonsági Szabályzat végrehajtásáról, e körben szabályozási koncepciókat, szabályzat tervezeteket készít, a szakterületek megkeresésére vagy saját hatáskörben szakmai állásfoglalást ad ki.

Az informatikai biztonság szempontjából véleményezi a szervezet szabályzatait és szerződéseit. Irányítja és ellenőrzi az Informatikai Biztonsági Vezető munkáját [12].

Informatikai Biztonsági Vezető (Informatikai Biztonsági Felelős)

Felelős a szervezet informatikai rendszerével kapcsolatos biztonsági feladatok kezeléséért. A szervezet által üzemeltetetett, illetve annak adatait feldolgozó informatikai rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtése és fenntartása, ennek tervezése, szervezése, irányítása, koordinálása és ellenőrzése. Nagyobb szervezeteknél munkáját a vezetése alatt álló Informatikai Biztonsági Munkatársak segíthetik.

Jogosult az ellenőrzési tevékenysége során, a szervezet tulajdonában vagy használatában lévő dokumentumba, adatbázisba, számítógépes adathordozó tartalmába való betekintésre, az informatikai és távközlési eszközök vizsgálatára. Az informatikai biztonsági vezető szerepköre összeférhetetlen az informatikai rendszerért felelős vezető funkciójával, sőt annak alárendeltségében, tőle függő viszonyban sem lehetnek [12].

Feladatai közé többek között az alábbiak tartoznak:

- Felméri és elemzi az informatikai biztonsággal összefüggő veszélyforrásokat, meghatározza a kockázatkezelés módszerét.
- Kidolgozza az informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat, utasításokat, terveket és irányelveket.
- Részt vesz:
  - a rendkívüli események kezelésére szolgáló tervek elkészítésében, azok naprakészen tartásában;
  - a fizikai biztonsági feltételek kialakításában, követelményeinek meghatározásában;
  - az informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában;

- Szakmai szempontból közvetlenül irányítja a szervezet informatikai biztonsági tevékenységét.
- Ellenőrzi az informatikai biztonsági előírások végrehajtását.

Az informatikai alkalmazásért felelős vezető

Felelős az általa felügyelt informatikai rendszer egészének alkalmazásáért, bevezetésének és használatának megszervezéséért, illetve továbbfejlesztéséért és a kapcsolódó eljárási rend kialakításáért. Felelős továbbá a szervezet Informatikai Biztonsági Szabályzatának saját szervezeti egységét érintő részének elkészítésért és az abban foglaltak betartásáért.

Adatgazda

Felelős a számára meghatározott adatok meglétéért (beszerzéséért és előállításáért), hitelességéért és azok időben történő biztosításáért. Az adatgazda viseli a jogi és pénzügyi felelősséget az adatokért, ő tekinthető az adatok jogi értelemben vett tulajdonosának. Feladata a rendszerben tárolt adatok, információk osztályozása és védelme, a hozzáférés engedélyezése, tiltása. A hozzáférés engedélyezési jogkörét a kinevezett jogosultságigény engedélyezőkön keresztül gyakorolja.

Az adatgazda a nyilvántartó rendszerek esetében nem informatikus, hanem egy felhasználó, aki általában a leginkább érintett funkcionális terület vezetője (számlavezetés, könyvelés, stb.). Az informatikai kiszolgáló alkalmazásoknak (pl. Windows domain rendszer, Active Directory, adatátviteli hálózat vezérlő alkalmazás, naplógyűjtő és elemző alkalmazás stb.) adatgazdája informatikus [25].

Informatikai rendszer üzemeltetéséért felelős vezető

Felelős a szervezet informatikai rendszereinek rendeltetésszerű, előírt követelményeknek megfelelő működéséért. Felelős továbbá a szervezet Informatikai Biztonsági Szabályzatának saját szervezeti egységét érintő részének elkészítésért és az abban foglaltak betartásáért.

Általános rendszergazda, adatbázis adminisztrátor

A rendszergazda feladata az informatikai rendszer folyamatos üzemeltetése, beleértve az incidensek elhárítását, az adat- és rendszermentések szabályok szerinti elkészítését és tárolását, szükség esetén az adat visszaállítás végrehajtását, a karbantartási tevékenységek végrehajtását, a változások élesítését az üzemi környezetben; az üzemeltetői hozzáférési jogok beállítását az informatikai rendszereken a biztonsági felelős utasításainak betartásával.

Az adatbázis adminisztrátor feladata az adatbázis-kezelő rendszer által biztosított menedzsment feladatok kezelése, a rendszer folyamatos üzemeltetése a szabályzatokban szereplő feladatok elvégzésével.

A szervezeten belül el kell határolni az informatikai rendszert kezelő, fejlesztő, üzemeltető szerepeket a felhasználói funkcióktól. Az intézmény informatikai szervezeti egysége vezetőjének, a nagyobb és fontos alkalmazási területek vezetőivel egyeztetve a fontos alkalmazásokhoz rendszergazdákat kell kijelölniük, pontosan meghatározva feladataikat és felelősségüket. El kell különíteni a fejlesztői környezetet az alkalmazói környezettől, külön kell szabályozni a fejlesztői, működtetői és adminisztrációs hozzáférési jogköröket.

Az előbbiekben áttekintett szerepkörök közül az adatbázis-biztonságot szabályozó dokumentumokban szerepet kapnak a következők: az Informatikai Biztonsági Vezető, a

beosztásában lévő Informatikai Biztonsági Munkatársak, az Adatgazda, az általános rendszergazda és az adatbázis adminisztrátor.

A MAGYAR ADATBÁZIS BIZTONSÁGI SZABÁLYOZÓ RENDSZER FEJLESZTÉSÉNEK IRÁNYAI

A következőkben az adatbázis-biztonság szabályozó rendszerének fejlesztési lehetőségeit tekintjük át a magyar közigazgatáson belül. Abból indulunk ki, hogy egyrészt a hazai informatikai biztonság szabályozásában már sok fontos lépés történt, ezt a cikk első felében már felvázoltuk Másrészt a jelenleginél szigorúbb és részletesebb hazai központi szabályozás szükséges az informatika egyes részterületeinek védelme tekintetében, különös tekintettel a működés kritikus területeken. A magyar szabályozásban e tekintetben jelenleg egy hiányzó láncszemet érzékelünk. Célunk a nemzetközi szabványokhoz és a hazai jogszabályokhoz illeszkedő adatbázis-biztonság megteremtéséhez és fenntartásához szükséges lépések megfogalmazása.

További elemzésre és megfontolásra érdemes javaslat a jelenlegi Nemzeti Hálózatbiztonsági Központ bázisán, vagy azt magában foglaló megoldással egy Nemzeti Informatikai Biztonsági Központ kialakítása, amelynek feladatköre a hálózatbiztonság mellett kibővülne a közigazgatási informatikai rendszerek és a kritikus információs infrastruktúrák teljes körű informatikai védelmének koordinációs és egyes konkrét feladataival. A központ közigazgatási és igazságügyi, illetve nemzeti fejlesztési miniszterek irányítása alatt állhatna, egyben – ágazati résztvevőként – együttműködne a kritikus infrastruktúra védelem feladatait megvalósító, várhatóan a katasztrófavédelmi szervezetrendszer részét képező szervezettel.

Az adatbázis-biztonság szabályozását megítélésünk szerint az informatikai biztonság szabályozó rendszerének integráns részeként, a jelenleginél mélyebb tartalommal és az előzőekben bemutatott önálló dokumentumokkal szükséges megvalósítani, az átfogó informatikai biztonságért felelős miniszter feladat- és hatáskörében. Mindezt a Közigazgatási Informatikai Bizottság által elfogadott adatbázis-biztonsági ajánlások támogatnák, az adatbázis-biztonság felügyeletével és megvalósításával kapcsolatos konkrét feladatok pedig célszerűen a Nemzeti Informatikai Biztonsági Központ feladatkörébe tartoznának.

Javaslatunk szerint az adatbázis-biztonsági szabályozásnak egy többszintű rendszert kellene alkotnia. A szabályozás egyik részét képezné a szervezet és tevékenység független általános adatbázis-biztonsági útmutató, mely rendszabályok rendezett listája lenne és egy kormányzati központi szerv adná ki. Az általános adatbázis-biztonsági útmutató keretszabályozást jelentene, az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági követelményeket szervezet, tevékenység és termék független módon tartalmazná. A dokumentum mintaként szolgálna a szervezetek számára a saját adatbázis-biztonsági útmutató elkészítéséhez, mely már szervezet és tevékenység specifikusan tartalmazná a követelményeket, előírásokat. A dokumentumban lehetne egy termékfüggő adatbázis ellenőrzési lista elkészítését az adatbázis üzemeltetők feladatául kijelölni.

Az útmutató önmagában nem egy kötelező erejű jogszabály lenne, helyét magyar viszonylatban a KIB ajánlások között tudnánk elképzelni. Használatát viszont meghatározott szervezetek számára egy kormányrendelet elrendelhetné.

A szabályozás másik része szervezet specifikus dokumentumokból állna. A szabályozás hatálya alá eső szervezetnek ki kellene dolgoznia a saját általános adatbázis biztonsági útmutatóját az előző pontban leírt útmutató adaptációjával. Ebben az adatbázis rendszerre vonatkozó követelményeket saját szervezetére vonatkoztatva kellene megfogalmazni. Továbbá a szervezetnek az általános biztonsági követelményeket át kellene fogalmaznia

konkrét biztonsági elemek, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes, ez lenne a szervezet adatbázis-biztonsági ellenőrző listája. Ebből a két dokumentumból épülne fel a szervezet adatbázis biztonsági szabályzata.

A szervezet általános adatbázis biztonsági útmutatóját a szervezeti szintű informatikai biztonság szabályozás részének a következő dokumentumok közé lehetne beilleszteni:

- Nagyobb szervezetek esetén a rendszerszintű Informatikai Biztonsági Szabályzatok közé
- Egyszintű Informatikai Biztonsági Szabályzat esetén annak egy fejezetének
- Eljárásrendek közé

A magyar közigazgatásban jelenleg nincs és valószínűen még sokáig nem is lesz egy olyan központi szerv, mely fel tudná vállalni azt a feladatot, hogy a jelentősebb adatbázis-kezelő rendszerek esetében adatbázis-biztonsági ellenőrző listákat állít fel és tart karban. A rendszer specifikus adatbázis-biztonsági ellenőrző listákat a szervezet készíti el a saját környezetére vonatkoztatva, a szervezet biztonsági dokumentumainak rendszerében az Eljárásrendek kategóriájába sorolható be.

Ha az általános adatbázis-biztonsági útmutató bizonyos szervezetek számára kötelező erővel bíró szabályozás részeként jelenne meg, akkor szükség lenne egy központi szervezetre – például az előzőekben javasolt Nemzeti Informatikai Biztonsági Központra -, melynek feladatába tartozna az alatta álló szerveken a felügyelet gyakorlása. A központi szerv feladat lenne annak ellenőrzése, hogy a kritikus adatbázisokat üzemeltető szervek létrehoztak-e szervezeti szintű általános adatbázis-biztonsági útmutatót és ellenőrzési listát, illetve elvégzik-e ennek alapján a biztonsági vizsgálatot. Elő kellene írni központilag, hogy milyen gyakran kell a szervezetben a biztonsági szabályozás alapján az ellenőrzést lefolytatni, annak eredményét dokumentálni kell és külső audit során az adatbázis-biztonsági szabályzat meglétét és az annak való megfelelés dokumentumát be kell mutatni. A központi szerv javaslatokat, segítséget nyújthat abban, hogy a termékfüggő adatbázis ellenőrző listákat milyen forrásokra támaszkodva tudják az üzemeltető szervezetek elkészíteni.

Felhasznált irodalom

[1] 2009. évi LX. törvény az elektronikus közszolgáltatásról

[2] 223/2009. (X. 14.) Kormányrendelet az elektronikus közszolgáltatás biztonságáról

[3] A1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

[4] 2009. évi CLV. törvény a minősített adat védelméről

[5] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

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

[7] 2080/2008 (VI. 30.) Korm. Határozatot a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[8] A KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA) http://www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf

[9] e-Közigazgatási Keretrendszer Kialakítása projekt (2008): A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár, IT biztonsági műszaki követelmények

[10] Muha Lajos: Magyar Informatikai Biztonsági Keretrendszer (MIBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[11] Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

[12] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányítási Követelmények (IBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[13] Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Budapest: Miniszterelnöki Hivatal, 2008.

[14] Balázs István, Szabó István: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS), Budapest: Miniszterelnöki Hivatal, 2008.

[15] Krasznay Csaba, Muha Lajos, Rigó Ernő, Szigeti Szabolcs: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX), Budapest: Miniszterelnöki Hivatal, 2008.

[16] 212/2010. (VII. 1.) Korm. rendelet az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről.

[17] 17/2010 (VIII. 31.) KIM utasítás a Közigazgatási és Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról.

[18] 9/2011. (II. 15.) NFM utasítás a Nemzeti Fejlesztési Minisztérium Szervezeti és Működési Szabályzatáról.

[19] 42/2011 (IV. 20.) KIM utasítás a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala Szervezeti és Működési Szabályzatáról.

[20] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról.

[21] A Puskás Tivadar Közalapítvány Szervezeti és Működési Szabályzata (módosításokkal egységes szerkezetben). – Puskás Tivadar Közalapítvány Kuratóriuma, 2009.11.27.

[22] 1026/2007. (IV. 11.) Korm. határozat a közigazgatási informatikai feladatok kormányzati koordinációjáról.

[23] 2080/2008 (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[24] Póserné Oláh Valéria A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei, Hadmérnök II. Évfolyam 4. szám, 2007.

[25] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Inkovics Ferenc
ferenc.inkovics@gmail.com

THE SYSTEMS OF INFORMATION AND COMMUNICATION TECHNOLOGY APPLYED BY THE GOVERNMENT

Absztrakt

Magyarország a többi EU-s tagállammal együtt próbál megfelelni korunk új követelményeinek. Ennek a tevékenységnek vannak már most pozitív eredményei, de még sok kihívás áll előttünk. E kihívásokkal az állampolgároknak és a kormánynak együtt kell szembe nézniük.

Hungary, together with the other EU members is trying to meet the new requirements of our age. This activity has already positive results, but we have a great number of challenges in front of us. The citizens and the government together have to face these challenges.

Kulcsszavak: *kormány, infokommunikáció, elektronikus szolgáltatások ~ government, information and communication technology, e-services*

INTRODUCTION

During the past decades but mostly in the past few years Information and Communication Technologies (ICT) have undergone an explosion-like development, moreover day by day we can meet continuously novelties. This is no wonder, as we are in the age of Information Society. The result of this is also that the formerly mysterious 'e-' prefix appears more and more often in our everyday life and it has become an everyday occurrence during the past years. Probably e-mail (electronic mail) is one of the most common expressions with this prefix 'e-', but there are some more activities that we can perform electronically e.g. e-administration, e-work, e-signature etc..

Practically ICT means[1] are almost present on all spheres of activities in our life. Today, many of us cannot imagine such a scope of activity that could not partly or wholly be performed on or by internet e.g. a driver does not look it up on a paper map where he has to go for picking up his boss but he starts a search on an internet-based map or he may use his PNA (Personal Navigation Assistant); or rather in private life the number of families is constantly increasing, where video telephone contacts are used for e.g. keeping contact with their grandparents instead of giving them a ring. The number of digital illiterates is constantly decreasing. Elementary and high school students come into daily contact with ICT means. One can also say that they come into contact with digital literacy already in the school.

According to the Hungarian Central Statistical Office (HCSO) [1] the number of internet subscribers is constantly increasing and their majority prefers broadband internet access. According to the data of the HCSO there are nearly 3.5 million internet subscriptions in Hungary, but this does not mean that 3.5 million inhabitants have internet access. However, this figure is misleading, because there are people who have land-line and mobile internet access, as well. But this is true vice versa, because in most cases where a family has one internet access it is used by each member of the family.

This article will mention some examples how the government may use the development of ICT means. Directives and regulations were created by the government in order to ensure the smooth transition to e-government.

E-PUBLIC ADMINISTRATION

Parallel to the social and technical changes of the past decades the public sphere is also changing and developing. It is fact that the public sphere is somewhat lagging behind, but the direction is correct. Nowadays the expressions like central and local e-governments, e-administration and e-Hungary are already accepted in everyday life. With the appearance of electronic services the functioning and operation of the public sphere may become quicker, more cost-intensive and more rational. In the interest of all these the EU and the European states including Hungary have prepared and are preparing e-governmental strategies. Even political decision makers recognize that these strategies promote the reassessment the connections between states and citizens. The electronic services will become more effective and quicker than traditional services if strategies and their execution will not be extended only to utilize and improve technical achievements, but together with those we simplify and ameliorate the methods and processes, as well. The government can naturally also function without the introduction of new technical achievements, but in order to keep up pace /step/

[1] ICT means consists of all technical means used to handle information and aid communication, including computer and network hardware, communication middle-ware as well as necessary software.

with citizens and other countries, the system of e-government and electronic public administration must be elaborated. The aim of electronic public administration is that apart from the traditional channels or later instead of them electronic channels should be applied between the two parties of public administration and that should be maintained in a wide circle. The 2 parties of the administration are: on one side providers of administration services as central and local governments and their institutions and on the other side the beneficiaries of administration services as citizens, enterprises, other organizations and institutions. Applying e-governmental channels administration can be achieved through an advanced client-oriented service package.

This means that in the course of e-administration the following aspects should be realized:

1. publication of information on the WEB or on the internet
2. information of the citizens should be effective
3. interactive services and e-administration should be applied everywhere

A quick and inexpensive stream of information characteristic for an information society has to be achieved within the government, as well. The aim is that the information should be available in the proper form, with the required contents, as necessary. This refers to the obtainment, achievement, storing, handling, organizing, searching of data and introducing them in a modified form, as well. All these are important as these activities significantly influence the competitiveness and the whole economic life.

In Hungary, in the past century already the idea has emerged to start the joining of information societies. Formerly, taking a decision was hindered by lack of information. Nowadays, practically all information can be made available within seconds. Now we have to face the problem of deciding which information out of the available information stream is exactly needed. The solution of this problem is: the installation and operation of such information systems that are able to properly handle the available information stream and are able to support decision making and can supply decision makers with necessary information within a reasonable time limit, as well.

As we proceed on the road of development, our fellow citizens are expecting an early, exact, more and more accurate and detailed information. This means that the sharing of the constantly increasing number of information must be ensured. Computers are a great help in this sharing e.g. there is a given customer service that is supposed to meet the different requirements of customers. At present a significant number of customers are able not only to find the required answers by searching the internet but they also require a similar information service. In case the quality of electronic information and service is acceptable, then the traditional overburdening of the customer service and even its maintenance cost also may be reduced.

We should not think that the e-government consists only of the application and operation of the newest means of ICT. It is necessary to check, by all means, even in case of e-governmental and electronic public administration solutions whether the application and wide use of new Information and Communication Technologies promote the following [2]:

1. political participation
2. equal, free and unhindered access to information
3. transparent and clear governmental activities
4. the more open and clear relation between state and citizens
5. etc.

The examination of these is the most important question of e-governmental strategies.

When joining the European Union the e-governmental strategy of Hungary was based on the eEurope2005 e-governmental program. It was our task – among others – to create a possibility of securing electronic access to the twenty basic services required by the EU. Nowadays the

citizens and the enterprises already draw a benefit from electronic public administration services. A successful example is that the 'Ügyfélkapu' (the official Hungarian portal for electronic public administration services) has more than 800 thousands users and services of more than 30 governmental institutions can be reached electronically through this system [3]. Some examples of the offered services are [4]:

1. eBev services (electronic tax declaration)
2. administration regarding different certificates (birth, marriage etc.)
3. administration regarding sole trader's license
4. administration regarding automobile registration
5. administration regarding home address card
6. administration regarding international driver's license
7. Office of Government Issued Documents on internet
8. etc.

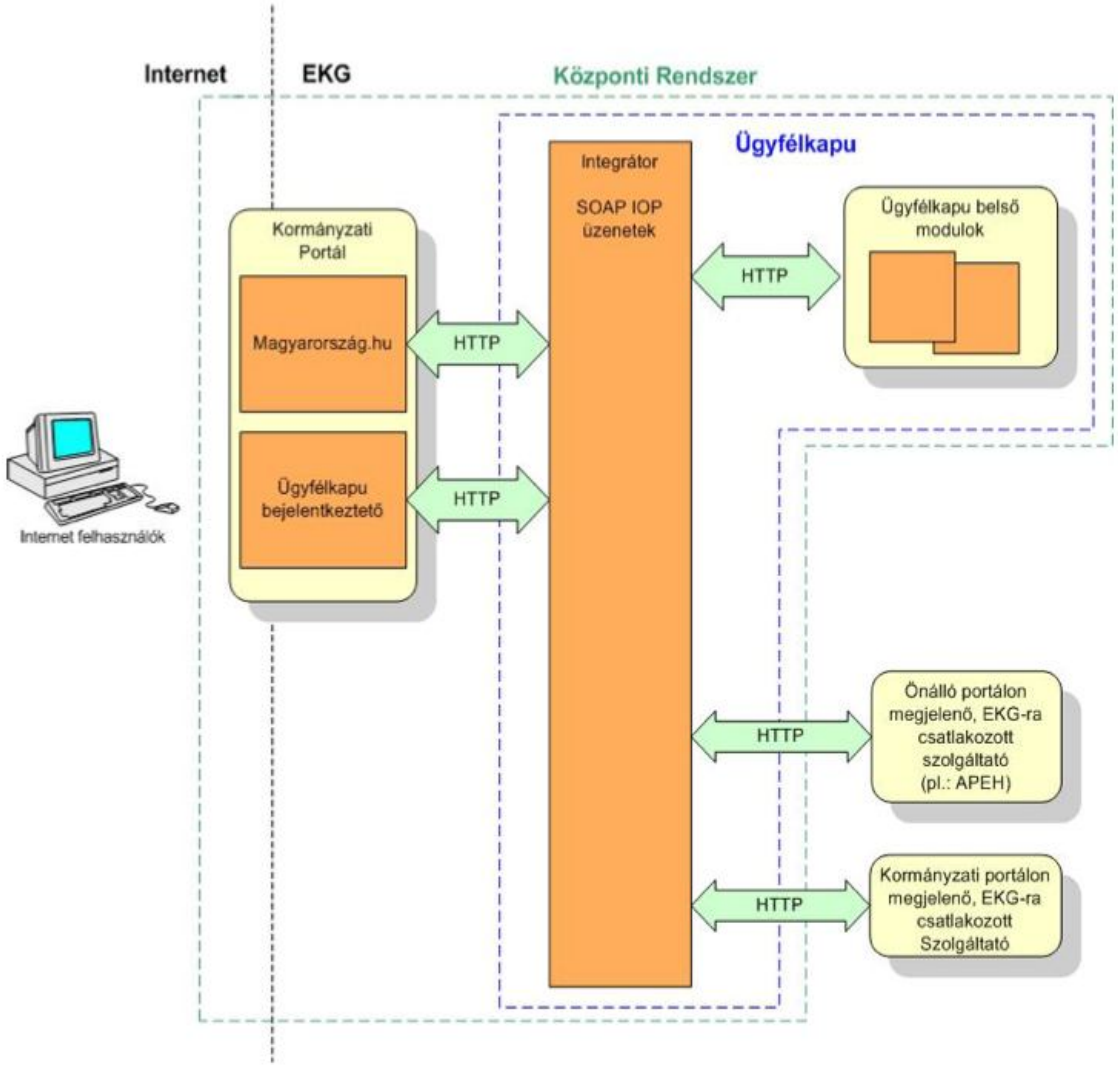


Figure 1.
Technical description of connection to 'Ügyfélkapu' portal [5]

Former e-governmental targets as improvement of governmental services, more effective and cost saving operation of the state, and the increase of the democratic participation of citizens even today form an organic part of e-governmental targets. Aims of the e-government are being realized in the form of e-services. From these services both, the administration and the

citizens, the enterprises also enjoy different advantages. The actual advantages of the electronic public administration are:

1. less human resources are needed and the administration is more effective
2. performance is more favorable, deadlines are shorter (the citizens' requirements can be completed in a shorter time, thus the government official can sooner perform his task)
3. less time is needed for filling-in and managing the different forms
4. administration gets simpler, certain processes can be automized and consequently expenses can be reduced
5. e-democracy will be realized: through the different portals citizens will get to know the activities and work of central and local governments and other organizations

Concerning the above, an actual example is the establishment of e-administration in case of the Courts of Registration [6]. In July 2008 the electronic services of the Courts of Registration were introduced, thus registration process of the different enterprises is performed completely electronically. Today anybody can register a company within one hour supposing that the registration is carried out via the application of a sample contract. For a quick registration we have to choose a legal adviser who disposes of an electronic signature. This is important because an e-signature is an indispensable prerequisite of the e-registration of the Court of Registration. This method is advantageous for both, the citizens and the Court, as well. For the Court it is not necessary any more to spend such a long time with the registration, as the information system will do that for them, thus, they can spend more time on legal controlling activities.

In case of electronic services it is important that proper trust should be formed. This also refers to security and authenticity. This authenticity is by all means supported by the fact that according to chapter VII of Act CXXX (year 2010) 'Magyar Közlöny' (Official Journal of Hungary)) has to be published as an electronic document on the governmental portal. This electronic publication must be accepted as authenticated document.

It is a requirement of electronic services that these should be simple, respectively simpler than the former traditional services. Otherwise a great part of their initiatives will be lost. Electronic services may also be quite new, formerly non-existent services. An interesting example is one of the innovations of the state-owned MÁV (Hungarian State Railways Company): the eMIG [7] – by this service the actual movement and status of trains can be followed. Apart from the data figuring on the map information is available on each train: departure and destination; probable delay and early arrival; and station data.

It is necessary to talk about regulations, too. Obligatory and generally applied regulations can be found everywhere. The electronic public administration is no exception either. As we live in a constitutional state, law-enforcement organizations and officers are responsible for law and order. The public transportation system is regulated the KRESZ (Hungarian Code of highway) at the same time for smooth operation and in order to avoid peremptory decisions the proper legal background must be created in e-administration, as well.

According to the above it may be stated: a well-functioning e-government must have a stable basis of 4 pillars. These pillars are [8] :

1. regulations and processes: no territory can be found where regulations are not needed, no processes are elaborated and the e-government is no exception either
2. human abilities and culture: it is necessary to form the digital literacy of the citizens and enterprise employees
3. ICT infrastructure: increase of the number of internet accesses and improvement of their quality is imperative
4. organization: precondition of an Information Society is the proper organizational structure corresponding to the challenges of an Information Society. The organizations, their tasks, their legal sphere of activity and responsibility, furthermore their hierarchy of their organizations has also to be clarified.

STATUTES, STRATEGIES AND RECOMMENDATIONS OF E-GOVERNMENT

For the application of ICT systems in public administration there are two types of regulations in Hungary: general IT regulations and special ones [10]. Statutes not specifically applied in electronic public administration are called general statutes (e.g. act on electronic signature). While those specifically applied in the electronic public administration are the special statutes. Some important statutes concerning electronic public administration in Hungary are:

1. Act XXXV of 2001 on Electronic Signatures
2. Act CXL of 2004 on the General Rules of Administrative Proceedings and Services (Chapter X.)
3. Act LX of 2009 on Electronic Public Services
4. Act CLVII of 2010 on Enhancing the Protection of Public Registries Belonging to Public Digital Assets
5. 222/2009 Decree of the Government on the Operation of Electronic Public Services
6. 223/2009 Decree of the Government on the Security of Electronic Public Services
7. 224/2009 Decree of the Government on the Identification of Clients of the Central Electronic Public Services and on the Identification Services
8. 225/2009 Decree of the Government on the Electronic Public Services and the Utilization of the Electronic Public Services
9. Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (i.e. 'the Data Protection Law')
10. Act IV of 1978 on the Criminal Code

Hungary started the establishment of its electronic public administration system on the basis of electronic strategy defined by the government in the past years. The results of this are the above mentioned statutes. Although, as compared to the situation of 10 years ago, a great number of statutes were brought concerning the electronic public administration, however these are not yet complete. There is still much to be done for a real electronic public administration, and statutes are only a part of the tasks to be done. This was recognized by the present government and therefore the digital renewal action program was created, hoping that the realization of this plan will speed up the evasion from the economic crisis and to pave - among others – the road of the future of electronic administration for the coming years [11]. According to the planners of this action program, in a short time significant improvement can be achieved in quality of life by securing access to the up-to-date ICT infrastructure furthermore on-line contents and services. The short-time expectation can be accepted, but unfortunately the number of digital illiterates is rather large. Digital illiterates can only enjoy a small part of these advantages. Fortunately, the aims include the plan of transforming the majority of the population into digitally literate persons and regular internet users.

The center of the action plan is the citizens, the enterprises, the public administration and development of ICT infrastructure. All of these are indicated in 83 proposed measures, and in contradiction to former IT strategies this action program covers not only specific territories but also a complex unit with actions and proposed measures connected to each sector. However, in order to achieve success the importance of ICT should be introduced with identical importance in each sector's action plan and concept.

As we are an EU member state we have to act in accordance with the endeavors of the European Union. One of these is that by the end of 2013 broadband internet should be accessible everywhere. Because the digital illiterates probably won't take advantage of the ICT technologies available, they are not going to subscribe for a broadband internet access for home use, because they will not be able to utilize it. They will probably ask somebody else to do certain things for them. It is therefore advantageous that the teaching of ICT is planned to be carried out not only in schools but for adults, too. Summarizing: we can state that such an

action program was needed by the whole country. Although this action program contains ideas that have already been reconsidered by the government itself (e.g. who will be responsible for managing data elaboration tasks of the national data property), however, it is hoped that the government will continue to act in the same spirit, will succeed in observing the deadlines, and further sector's action plans and proposed measures will also be outlined.
Following the statutes and the action program we have to mention the recommendations, as well. The Information Technology recommendations, as it is indicated, were not prepared as obligatory instructions. These are not summaries of special regulations but represent only short requirements and summaries of alternatives elaborated by experts of great experience in this field and to be understood by everybody.
Some recommendations concerning public administration of the former Public Administration Committee for Information Technology (in Hungarian: KIB – Közigazgatási Informatikai Bizottság) are:

1. KIB's Recommendation No 19 on internet activities of central governmental organizations (in Hungarian: KIB 19. ajánlása: A központi államigazgatás szervezeteinek internet-tevékenységére, valamint az általuk működtetett honlapok tartalmi és formai követelményeire 3.0)
2. KIB's Recommendation No 21 on technical specification of 'Ügyfélkapu' portal and Official portal (in Hungarian: KIB 21. ajánlása: Az ügyfélkapu és hivatali kapu kapcsolódás műszaki specifikációja)
3. KIB's Recommendation No 22/1 on IT strategy of governmental institutions (in Hungarian: KIB 22/1. ajánlása: Kormányzati Intézmények Informatikai Stratégiájának készítése).
4. KIB's Recommendation No 22/2 on E-governmental strategies for local governments and smaller communities (in Hungarian: KIB 22/2. ajánlása: E-önkormányzati stratégiakészítési ajánlás kistérségek és önkormányzatok számára
5. KIB's Recommendation No 25 on MIBIK, MIBÉTS, IBIX (in Hungarian: KIB 25. ajánlás: MIBIK, MIBÉTS, IBIX)
6. KIB's Recommendation No 26 on Hungarian requirements for different electronic hardware (in Hungarian: KIB 26. ajánlás: A Magyarországon elektronikus azonosításra, hitelesítésre, aláírásra és elektronikus azonosítók hordozására alkalmas eszközök követelményei /HUNeID/ 1.0 verzió)
7. KIB's Recommendation No 27 on Directives for electronic application of forms of public administration (in Hungarian: KIB 27. ajánlás: Útmutató a közigazgatási eljárások során használt nyomtatványok elektronizálásához 1.0 verzió)
8. KIB's Recommendation No 28 on Collection of requirements in public administration system (in Hungarian: KIB 28. ajánlás: Az e-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár)
9. KIB's Recommendation No 29 on Cost-profit analyses of electronic public administration (in Hungarian: KIB 29. ajánlás: Az elektronikus közigazgatási projektek költség-haszon elemzéséről) for details see Bibliography annex, details according to ...page...

As ICT means and systems are developing, more and more experience will be gained in connection with their planning, installing and operating, thus new recommendations or the updating/revision of the older ones will be necessary. After months and years the revision is required because when taking the recommendations into consideration it happens or it may happen that experiences may be gained that have to be included into the revised recommendations. Furthermore problems may occur that should be or have to be eliminated, therefore revision can also help in avoiding future problems and troubles. It has already happened that certain elements of the recommendations have been included in statutes.

The EU has also been interested in economic, social and environmental protection renewal, it is no wonder because development is in everybody's interest. For this purpose the EU has elaborated several action programs and carried out these more or less successfully.
Some programs, action programs, action plans and strategies of the European Union in connection with the formation and development of Information Society) are:

1. IDA (electronic Interchange of Data between Administrations) program
2. e-Europe 2002 Action Plan
3. PROMISE program (Multi-annual Community program to stimulate the establishment of the Information Society in Europe)
4. e-Europe 2005 Action plan
5. MODINIS program (this program provided financial support for the implementation of the e-Europe 2005 Action plan)
6. i2010 European Union policy framework – a European Information Society for growth and employment
7. Europe 2020 Strategy– the European Union growth strategy for the coming decades (Digital Agenda for Europe is one of the seven flagship initiatives of the Europe 2020 Strategy)

SUMMARY

Because of the introduction of ICT means it can already be seen that the speed of administrative work is becoming quicker and quicker. E.g. a tax declaration can be presented to NAV (in Hungarian: Nemzeti Adó és Vámhivatal, this is the National Tax and Customs Administration of Hungary – formerly APEH, in Hungarian: Adó és Pénzügyi Ellenőrzési Hivatal, i.e the Hungarian Tax and Financial Control Administration) within a minute by applying the filling-in program of NAV. This program is able to communicate directly with the 'Ügyfélkapu' portal (official governmental portal for electronic public administration). The confirmation of dispatch will be received immediately from NAV. In such cases we must remember our fellow citizens, who are presenting their tax declaration in the very last minute and have therefore to queue up for hours at the Post Office for mailing their declaration in time. However, it's very probable that they will not change this procedure in case of electronic dispatch either, but it must not be forgotten that too many late mailers may overload the system and they will miss the deadline if they postpone their obligations to the last minutes.
Another example is that the activities of the Office of Government Issued Documents have also been speeded up. Urgent passport applications may take only 3 hours [12].
It is expected that the number of different cards (ID card, Driving license card, TAJ card - Hungarian health insurance card) issued by the government will be reduced already by the end of this year). It is planned that a unified national card system will substitute the former ID card, Driver's license card, Health Insurance card etc. in the future. Actually, with the exception of the passport nearly all (5-6 pieces) documents issued by the authorities will be included in this newly planned document. In consequence of this the administration of office work will become simpler and citizens will have to carry fewer documents with them and last but not least the costs of the government can be decreased.
Considering the above, we have big steps in front of us. Not only the government but we, the citizens, have to take these big steps in order to enable our nation to keep up pace with the requirements of the 21st century and to create a better world for us. It is important that we should want and be ready to accept new developments. Let us be open and not be afraid of learning. We have reached a point where intelligent buildings (houses, offices, institutions,

etc.), public utilities, schools and transportation will assist our everyday life. It is important that all these should not be auto telic but should assist our lives.

REFERENCES

[1] Internet előfizetések http://portal.ksh.hu/pls/portal/ksh_web.portalsearch.search?lang=HU&filter_nyelv=--&filter_csoport=--&filter_csoport_ev=--&szo1=2010%20internet&filter_nyelv=HU&filter_csoport=-2&filter_csoport=-1&filter_csoport=1&filter_csoport=2&filter_csoport=0# (downloaded: 2011.05.01)

[2] Információs társadalom – Informált Polgár, 2. Szám, 2004. március http://www.ekozigazgatas.helyinfo.hu/domain63/files/modules/module15/37269C2CC088FA2E.pdf (downloaded: 2011.05.26)

[3] Múlt és jövő – Eredmények és lehetőségek az infokommunikációs és az e-közigazgatás területén http://www.e-magyarorszag.hu/2009_prezentaciok/emagyar2009_Baja_Ferenc.ppt (downloaded: 2011.05.23)

[4] Belépés után elérhető szolgáltatások https://ugyfelkapu.magyarorszag.hu/ (downloaded: 2011.05.23)

[5] A KIB 21. sz. ajánlása: Az ügyfélkapu és hivatali kapu kapcsolódás műszaki specifikációja (2.0) http://www.ekk.gov.hu/hu/kib/kib_21_v2.0.pdf (downloaded: 2010.05.29)

[6] A magyar internet portálok összehasonlítása http://www.sg.hu/cikkek/61549/az_e_ugyintezes_atalakitotta_a_birosagok_feladatait (downloaded: 2011.05.28)

[7] Halad a korral a MÁV cikk, Gödöllői Szolgálat, XX. Évfolyam 8. Szám, 2.oldalán, 2011 március 9. http://www.szolgalat.com/gszolga110309.pdf (downloaded: 2011.05.28)

[8] E-közigazgatás http://www.ekozigazgatas.helyinfo.hu/gss/alpha?do=63&pg=675&m1192_doc=2014&m-1_curr=1&m1188_act=5&st=1695 (downloaded: 2011.05.01)

[9] A magyar internet portálok összehasonlítása http://www.freeweb.hu/komocsip/portals.html (downloaded: 2011.05.28)

[10] E-közigazgatási informatikai rendszerek jogi szabályozása. http://www.kovacsvg.hu/C_E-kozigazgatasiRendszerekSzabalyozasa.html (downloaded: 2011.05.29)

[11] Digitális megújulás Cselekvési Terv. http://www.kormany.hu/download/7/e2/10000/Digitalis_Megujulas_Cselekvesi_Terv.pdf (downloaded: 2011.05.27)

[12] Digitális cselekedeteink http://www.itbusiness.hu/hetilap/cimlapon/Digitalis_cselekedeteink.html (downloaded: 2010.05.29)

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Harmati István
harmati@iit.bme.hu

Kisfaludi Péter
kisfaludi.peter@gmail.com

MILITARY STRATEGY PLANNING FOR AUTONOMOUS GROUND VEHICLES

Absztrakt

Több ágenst tartalmazó katonai robotrendszer koordinációs problémája játékelméleti keretek között hatékonyan vizsgálható. A koordinációs probléma megoldásához a mesterséges intelligencia módszerek eszköztára, így például a megerősítéses tanulás is alkalmazható. A cikkben bemutatásra kerül egy olyan, megerősítéses tanuláson alapuló stratégiatervezési módszer, amely képes több ágenst tartalmazó ember nélküli földi járművek esetén az ágensek számára optimális stratégiát kialakítani.

The coordination problem within a multiagent robot system can be efficiently examined in a game-theoretic framework. The solution for the coordination problem can be found using artificial intelligence methods, for example with reinforcement learning. In this article, a reinforcement learning based method is described, which is capable of finding an optimal strategy for a group of Unmanned Ground Vehicle (UGV).

Kulcsszavak: *megerősítéses tanulás, gépi tanulás, multiágens stratégiatervezés, multiágens robotrendszer ~ reinforcement learning, machine learning, multiagent strategy planning, multiagent robot system*

INTRODUCTION

Military strategy planning plays important role in battles since ancient ages. The scientific research of this discipline arrived in a new era since computers and autonomous military vehicles (robots) had appeared on the battle field. It is especially true if one considers that strategies can be simulated and analyzed by computing science. Artificial Intelligence (AI) and game theoretic methods in computer games has also impact on the state-of-the-art military strategies. Military strategies consider and coordinate such tactical operation as for example task assignment, pursuit-evasion games, formation control. Successful mission requires cooperation between agents (UGVs) to reach global (shared) goal. At the same time individual agents (or a group of agents) should execute different, coordinated actions in order to achieve the global and shared goal for the team. Since optimal maneuver planning is too complicated, it is a reasonable approach to decompose the mission planning into different levels. On higher level, the strategy defines a global goal to every team member or groups of team members. It also means that individual military goal is defined for each team mate (or group of team mates) by the strategic level. UGVs should solve their task individually on tactical level. This often includes path planning and collision avoidance algorithms [1]. Based on the planned paths, low level control method should provide control signal to the UGVs via actuator. For example, if UGVs are represented by tanks, low level control signals are the velocities of the wheels on the right hand side and the left hand side. The advantage of splitting up the problem is that the group level computations can be done in a parallel manner, and the complexity of these several computations is less than the complexity of solving the coordination problem for the whole team.

There are several potential methods which attempts to reach optimal strategies to the troops [2]. Since the problem is very complicated, they are mostly based on heuristics, soft computing methods [3], [4] e.g. fuzzy systems, neural network, swarm intelligence, reinforcement learning) or hard computing methods which provide at least sub-optimal solutions (e.g. game theory [5], [2], [6]).

In this paper, we propose reinforcement learning method for high level military strategy planning. Unfortunately, classical reinforcement learning techniques [7], [8] do not provide straightforward solution for team games and thus for military operation planning. On the other hand, these techniques are performing well in their domain (for example in single agent frameworks), that is why one can hope that an extension of these techniques to team games will solve the coordination problem emerging in military operations planning with still a good performance. In the reinforcement learning methods, we apply WoLF principle [7]. This is a solution for efficient reinforcement learning in a multiagent framework, and this method is able to find a locally optimal solution in the multiagent domain, and it is also proven that by applying the principle to reinforcement learning methods these methods become convergent, which is an important issue during military operations planning. In this paper, we propose a possible extension of the single agent framework to a multiagent domain and match it to military operations planning. As a result, military operation planning using hierarchical reinforcement learning is introduced.

Another problem emerging in the domain of team games is that the state space and the action space can easily grow to an intractable level, and therefore some simplifications should be applied to them to make the learning algorithms tractable (this means that without the simplifications, the algorithms can still find a solution in the original space but the computation time will become intractable). One way of simplification is to discretize the state and the action space. Discretization reduces the size of the space to a manageable size, but at the cost of losing information, because after discretization, two previously distinct states or actions can become indistinguishable. Another way of reducing the size of the state and action

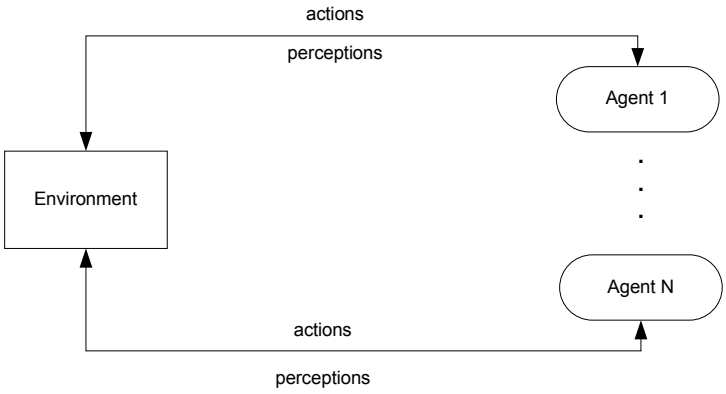
space is to create a simpler model of the environment (for example, by omitting existent but unimportant features of the environment), thus reducing the complexity (and size) of the state and action space.

The methods for strategy planning for military operations are analyzed in a simplified demonstration domain. In this domain, two teams of tanks fight against each other. The tanks are able to move on the map and they can shoot at each other. On the demonstration domain, the map is divided to cells and these cells make up a standard grid. The allowed movement of the tanks is reduced to the four main directions in this grid. The demonstration game simulates the battle in discrete timesteps, the units can move from a cell to an adjacent cell in a timestep or they can shoot. The team that succeeds in destroying all the units in the enemy's team is declared the winner. The multiagent coordination methods are tested and evaluated in this simplified demonstration domain.

The paper is organized as follows. In Section 2, we summarize the theoretical background of multiagent systems, the main results of reinforcement learning methods. Section 3 is devoted to framework used in our investigation and to a specific solution based on reinforcement learning approach is established. Section 4 demonstrates the proposed method via an illustrative example. Finally, we draw the conclusions in Section 5.

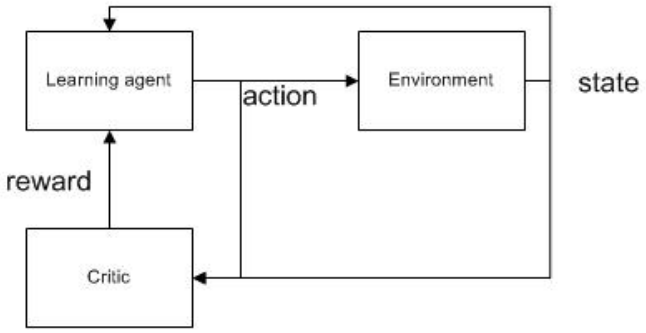
THEORETICAL BACKGROUND

In the field of artificial intelligence and machine learning, agents play a central role. Agent is an entity which can have perceptions from its environment and can change the state of its environment by means of its actuators [3]. The agent generally consists of three main parts: perception, reasoning and actuator, where the reasoning part is responsible for deciding which action the agent should execute based on the actual and previous perceptions. The schematic of an agent is seen on Figure 1. In our description, UGVs can be considered as agents. In multiagent environment one should coordinate their action for successful mission (winning the battle).



1. figure. Multiagent concept

In this paper, we develop a cooperative multiagent control on the base of reinforcement learning. Reinforcement learning is a machine learning technique capable of learning an optimal strategy based on reward signals (see Figure 2). A strategy in this context means a probabilistic distribution over the agent's available actions in a given state. A reinforcement learning problem can be described with the agent's state space and action space. Generally, the actions available to the agent can be different for different states, but usually it is assumed that the available actions are the same for all states. The reward is a signal that is distinct from the state of the environment and the agent is capable of treating the reward signal and the state of the environment distinctly.



2. figure. Reinforcement learning

Thus the learning agent has two inputs: one input is the state of the environment, the other is the actual value of the reward signal. A reward is optionally provided to the agent after executing an action; it is possible that the agent does not receive a feedback (reward) about its executed action. The goal of the learning agent is to maximize the value of the reward signal on the long run. As there are no correct state-action pairs provided to the agent (unlike in supervised learning), the agent can only learn by executing actions in the available states and observing the reward for each state action pair. This also means that the agent should somehow explore its environment, because only after suitably exploring the environment can the agent be sure to have found a strategy which maximizes the long term reward.

Several techniques exists which ensures suitable exploration of the state space, one of them (which is used in the proposed solution) is called the ε-greedy exploration. The ε-greedy exploration makes the agent execute a random action with low probability that is independent of the current strategy. This way no action will be excluded in any state from execution, and the agent has the chance to explore the whole state space.

MILITARY STRATEGY WITH REINFORCEMENT LEARNING

The proposed solution for military operations uses an extension of a single agent reinforcement learning algorithm suitable for stochastic games. The chosen reinforcement learning technique is the GraWoLF technique, it is extended to the domain of team games by using the aggregated agent concept, and the complexity of the solution is reduced by defining a hierarchy between the agents.

Let us start the discussion with some definition. The domain of team games is a subset of stochastic games (stochastic games are multiagent, multistate games [9]). In team games, the agents are partitioned into an arbitrary number of teams and every team has its own reward scheme and goal. The goal and reward are common amongst the agents of the same team, meaning that during learning using a reinforcement learning technique only a single reward signal is provided to the whole team, which all agents can perceive. The agents in the same team are allowed to execute different actions and communication between them is also allowed. Communication makes coordination (executing such individual actions that result in better expected reward than executing actions without coordination) between team members possible. The reward signal is dependant on the performance of the team as a whole.

Military operations belong to the domain of team games, because in a military operation, there are usually more units controlled by the same team trying to achieve a common goal, and the adversary team (or teams) is trying to prevent the team from doing so.

Formally, a team game can be described as a tuple (N, S, $A_{1...N}$, T, $R_{1...N}$), where

- N is the number of teams
- S is the set of states in the game
- A_i is the set of actions available for team i
- T is the transition function
- $T : S \times A_1 \times A_2 \times \ldots \times A_N \times S \rightarrow [0,1]$
- $T(s, a_1, a_2, \ldots a_N, s') = P(s_{t+1} = s' | s_t = s, a_{1_t} = a_1, a_{2_t} = a_2, \ldots a_{N_t} = a_N)$
  $\forall s \in S, \forall a_i \in A_i \quad \sum_{s' \in S} T(s, a_1, a_2, \ldots a_N, s') = 1$
- Ri is the reward function for team i
  $R_i : S \times A_1 \times A_2 \times \ldots \times A_N \rightarrow \Re$

The policy of the agent determines with what probability the agent chooses a particular action from its available action set in a given state. Formally, a policy is a mapping from state and action pairs to a probability. The policy returns the probability of taking a particular action at a given state.

Formally, the policy is denoted by π:
$\pi : S \times A \rightarrow [0,1]$
$\forall s \in S \quad \sum_{a \in A} \pi(s,a) = 1$, where
S is the set of states
A is the set of actions

When one develops a military strategy, then appropriate policies should be found that lead the team to a winning state.

Reinforcement learning in stochastic games: GraWoLF

Reinforcement learning techniques exist that are capable of finding a strategy for a single agent even in the domain of stochastic games. In the domain of team games however, the strategy should handle multiple agents (the team controlled by the strategy), and instead of returning a single action it should return a list of actions where every action in the list corresponds to one agent in the team.

One reinforcement learning technique that is suitable for stochastic games is the GraWoLF (Gradient based Win or Learn Fast) technique [7]. The algorithm is summarized as follows:

1. Let $\alpha \in [0,1], \beta \in [0,1], \delta^l > \delta^w \in [0,1]$ be learning rates
Initialize $\lambda, \gamma, \Delta t, \varepsilon$
Initialize $w \leftarrow \overline{0}, \theta \leftarrow \overline{0}, \overline{\theta} \leftarrow \overline{0}, e \leftarrow \overline{0}$

2. Repeat

(a)
Select action a from state s according to policy π with suitable exploration using ε.

(b)
Observe reward r and next state s'

$$Q_w(s,a) = w^T \phi_{sa}$$
$$Q_w(s',a') = w^T \phi_{s'a'}$$
$$\delta = \begin{cases} \delta_w \text{ if } \sum_a \pi_\phi(s,a) Q_w(s,a) > \sum_a \pi_{\bar{\phi}}(s,a) Q_w(s,a) \\ \delta_l \text{ otherwise} \end{cases}$$

$$e \leftarrow \lambda \gamma^{\Delta t} e + \phi_{sa}$$
$$w \leftarrow w + e\alpha(r + \gamma^{\Delta t} Q_w(s',a') - Q_w(s,a))$$
$$\theta \leftarrow \theta + \gamma^{\Delta t} \delta \sum_a \pi_\phi(s,a) Q_w(s,a)$$

(c)
Update average parameter vector $\bar{\theta} \leftarrow \beta\theta + (1-\beta)\bar{\theta}$

(d)
If s' is the initial state or trial is over then $t \leftarrow t_0, e \leftarrow \bar{0}, s \leftarrow s_0$

In this pseudo code, α is the learning rate for the approximation of the Q-values. The weighting parameter for the maintenance of the average parameter vector is denoted by β. The two other learning rates, δ^l and δ^w means the step size during gradient ascent when the agent is losing or winning, respectively. Parameter λ is influencing the speed of Q-values estimation, γ is the discount parameter for the reward formulation, Δt is the length of one timestep. Parameter ε is the probability of choosing a random action instead of executing an action according to the policy (this is the exploration parameter used in ε-greedy exploration).

Parameter w is used to approximate the Q-values corresponding to states and actions, this is the weighting vector for the approximation function, f_w. The actual parameter vector is denoted as θ, the average parameter vector with $\bar{\theta}$. The e vector is called the eligibility trace, basically it describes the contribution of the state and action pair to the actual error in the estimation of the Q-values.

In step (a), the agent chooses an action according to the actual policy, but with a small probability (ε) it chooses a random action from its action list. In step (b), the agent observes the new state of the environment (s') after executing the chosen action and it optionally receives a reward signal. After that, the approximations for the Q-values are updated (this means updating the weighting vector w and the eligibility vector e). The new parameter vector is calculated using the new approximation of the Q-values and the learning parameter is based on whether the agent is winning or losing. In step (c), the average parameter vector is calculated using β as the learning parameter and using the previous value of the actual and the average parameter vector. In step (d), the agent checks whether it is in its starting state or the time limit for the learning trial is reached, when the trial is restarted and the state of the environment is reset to the initial state and the eligibility vector is nullified.

This technique is scalable and it is able to find a locally optimal strategy for a single agent acting in a stochastic game domain. It requires a Boolean vector describing the state of the game (this vector is called the feature vector) as an input and provides a parameter vector as a result of learning. The action of an agent can be calculated by using the parameter vector and the feature vector. The strategy using the parameter vector calculated with GraWoLF is

locally optimal with regards to the reward function. A strategy (π) in this context means a mapping from state and action pairs to a number between 0 and 1, which is the probability of the agent choosing the given action in a particular state. Formally, $\pi : S \times A \rightarrow [0,1]$ and as the strategy defines a probabilistic distribution over the state-space:

$\forall s \in S \quad \sum_{a \in A} \pi(s,a) = 1$ where S is the set of states and A is the set of actions.

GraWoLF is a gradient ascent technique, meaning that in every learning step it modifies the parameter vector in the direction of the positive gradient of the expected reward function (note that the goal of the agent is to maximize the expected value of the reward, thus it modifies the parameter in the direction of the positive gradient). The step size for the gradient ascent technique is chosen according to the Win or Learn Fast principle. Win or Learn Fast means that the step size is relatively small if the agent is "winning" and the step size is relatively large if the agent is "losing".

Winning and losing are determined by comparing the performance to a so called average performance (it is impossible though to determine exactly if the agent is winning or losing).

Extending GraWoLF to the domain of team games

Handling multiple agents

GraWoLF in its original form is capable of finding a strategy for a single agent, but in team games, an action list for the team is required, where the actions in the list correspond to individual agents in the team.

Handling of multiple agents can be done by using the so called "aggregated agent" concept. The aggregated agent concept is a technique that can be used for an arbitrary number of agents. It defines an aggregated agent, whose state space is the joint state space of the state spaces of the individual agents and the action space of the aggregated agent is the joint action space of the action spaces of the individual agents. Every state and action in the state and action space of the aggregated agent has a unique identifier assigned, therefore the aggregated agent can be treated as a single agent, because it is in one state at a time and executes one action at a time (although the state denotes a list of states and the action denotes a list of actions).

The problem with the aggregated agent concept is that the state and the action space increases exponentially with additional agents, therefore in order to keep the solution tractable, the number of agents in the aggregated agent must be kept small.

Example of an aggregated agent: Two agents with two actions

Assume that there are two agents in the environment; both agents can execute an action from an action list which length is 2. The two agents belong to the same team. The action list for all agents is {a1, a2}.

If S1 denotes the state of agent 1 and S2 denotes the state of agent 2, the state of the game is described by the joint state space of the agents, S1xS2.

The action list for agent 1 is denoted by A1, the action list for agent 2 is denoted by A2 (note that A1=A2={a1, a2}). The action space available for the team, which consists of these two agents, is A1xA2 according to the aggregated agent concept. The resulting action list available for the team as follows {a1xa1, a1xa2, a2xa1, a2xa2}.

Reducing complexity

By using the aggregated agent concept, the size of the state and the action space can easily grow to an intractable size. A hierarchy between the agents is defined in order to reduce the size of the state and the action space. The agents of the same team are partitioned into subgroups, and the subgroups make up the whole team.

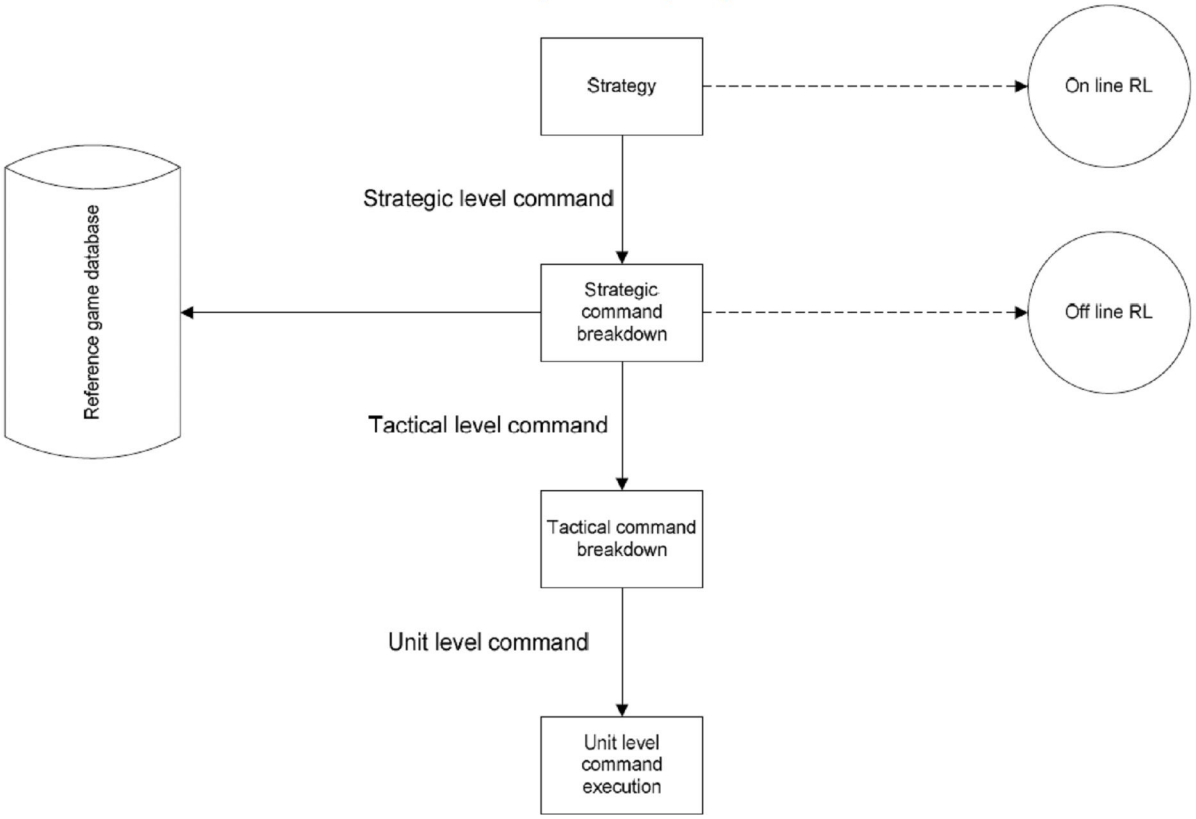
Defining a hierarchy between the agents efficiently reduces the complexity of the aggregated agent at every level, because generally there are less groups than units, and from the point of view of the team, only the actions for the groups has to be calculated.

Only the agents in the same group are allowed to communicate, this restriction in the communication channels means that the strategy will tend to be sub optimal, but this is a trade off between optimality and complexity. Every level in the hierarchy is connected only with at most two other levels, it is the responsibility of every level to transform the action received from a higher level to an action acceptable to a lower level (this process is called action breakdown).

CONCRETE SOLUTION

Hierarchy

In this particular solution, the hierarchy defined within the team has three levels: team (strategic level), group (tactical level) and unit level. Basically, the strategic action calculated at team level is broken down to a list of tactical level actions applicable to groups in the team, and group level actions are broken down into a list of unit level actions. This way a strategic action can be broken down to a list of unit level actions, where the commands can be directly executed by the units. The levels of the strategy and the process of converting a strategic action to a list of unit actions are shown on figure 3.



3. figure. Levels of the strategy [10]

The hierarchy is built up using spatial information between the units. The groups are created from units that are near each other. The number of groups and the number of agents in a group could change dynamically as the agents change their location, but in this particular solution the number of agents in a group and the number of groups was fixed, only the actual groups were created dynamically. The partitioning of the team members into groups is done according to the following algorithm [10]:

```
initialize DistLim, GrNumLim
groups ← ∅
foreach units in team
   group ← ∅
if allocated(unit)
   continue
endif
group ← group ∪ unit
neighbors ← team / unit
repeat
   nearest ← getNearestNeighbor (unit)
   if allocated(nearest)
      continue
   endif
   if distance (nearest) > DistLim
      continue
   endif
   group ← group ∪ nearest
   set Allocated (nearest)
   if size (group) > GrNumLim
      break
   endif
end repeat
```

- DistLim: the maximum distance between the units in a group
- GrNumLim: the maximum number of units in a group.
- Allocated: If the unit is already assigned to a group
- The "group", "groups" and "neighbors" are mathematical sets; the union operation means adding a new item (unit) to the set, the subtract operation means removing an item (unit) from the set. After running this algorithm, all units are partitioned into groups (the variable "groups" will contain the final partitioning), and the distance between the units in a group is less than DistLim, and the number of units is less than GrNumLim.

The strategic actions defined in the demonstration game are the Encircle, Retreat, Advance and Destroy commands; these are the actions available to the team agent at the highest level.

The meaning of these commands:

- Encircle: The chosen groups that are executing the encircle command are trying to encircle the chosen groups of the enemy, meaning that the goal of the action is to block the movement opportunities of the opponent groups in as many directions as possible
- Retreat: The group executing the retreat command tries to increase the distance between itself and all enemy groups.
- Advance: The goal of the advancing group is to decrease the distance between itself and all enemy groups.
- Destroy: The group that executes the destroy command tries to kill as many opponent units from the chosen opponent group as possible.

At tactical and unit level, the Left, Right, Forward, Shoot commands are available.
The meaning of these commands:

- Left: The unit/group turns left.
- Right: The unit/group turns right.
- Forward: The unit/group moves forward.
- Shoot: The unit/group shoots.

Learning at the levels of the hierarchy

Reinforcement learning is used at two parts of the algorithm: at calculating the strategic action for the team, and at strategic command breakdown.

The strategic action calculation part uses GraWoLF in its original form, because the team is treated as a single agent which can execute one action at a time. The action set available to the team is the set of strategic actions (Encircle, Advance, Retreat, and Shoot); the state of the game is represented as the joint state of the teams. This part of learning runs on line, and it is the responsibility of the lower hierarchy levels to convert the chosen strategic action to a list of unit level actions.

The strategic command breakdown module is responsible for creating a list of actions applicable to groups from a strategic action. As the number of groups in a team is usually greater than one, the original form of GraWoLF cannot be used; rather the extension of GraWoLF using the aggregated agent is used.

For every strategic action, at least one reference game is stored in a reference game database. In this database, every entry contains a game state and the locally optimal parameter vector to be used in that particular game state. The optimal parameter vectors are calculated during an off line reinforcement learning session. During this off line learning, the aggregated agent concept is used by the learning agent.

The action set available to the learning agent is generated according to the aggregated agent concept, which means that the actions are lists of actions in their inner representation, where each list item correspond to a group in the team. These action lists are assigned a unique identifier and the learning agent chooses from the set of these identifiers, meaning that from the point of view of the learning agent, the problem is single agent reinforcement learning in a stochastic game domain, where a locally optimal policy can be calculated using GraWoLF. But upon execution of the actions, the chosen action is split (this can be done because the action in reality is an action list), and the resulting group actions are executed by the groups in the team.

Tactical command breakdown is the process of converting a group level action to a list of unit level actions. This process is implemented in a predefined way, meaning that the rules for the breakdown are not updated during the game and no learning is done at this level of the hierarchy. As the action set available to a group is identical to the action set available to a unit, the breakdown is implemented in a simple way: first, the orientation of the agents in the same group is made equal to each other, and then all units in the group execute the action sent to the group.

SIMULATION RESULT

A simulation environment was developed in Matlab to enable development and evaluation of military strategies. The simulator module is the work of Lajos Szarka and Peter Kisfaludi. The simulator is capable of simulating a military operation on an arbitrarily sized two-dimensional map with an arbitrary number of units partitioned into two teams. The module simulates the battle in discrete timesteps. The map on which the battle takes place is also discretized, thus the location of every unit is also discrete (at every timestep, a unit resides on a discrete location called a tile). The orientation of the units is also discretized: it can be any of 0, 90, 180 or 270 degrees.

Environment

The environment of the concrete game where the experiments are carried out is a two dimensional, discretized map in which multiple units reside. The map is represented by a weighted graph, where the nodes of the graph correspond to locations on the map, while the edges of the graph represent paths between two locations.

In the current implementation, the map is a standard grid, where the length of the path between any two adjacent nodes is equal to 100. The edges of the graph are weighted, the weight of an edge corresponds to the length of the path between the two locations the edge connects.

The state of the environment is made available to the learning agents in discrete timestep, and the state update also happens in such fashion.

Objects on the map

Objects on the map can be moving objects or static objects. The static objects are not controlled by any of the teams; the moving objects (the units) are assigned to one of the teams in the game. Every object on the map occupies exactly one node on the map at a time.

The possible objects on the map are the following:

- control point: the control point is a special location on the map which can be owned by any of the teams participating in the battle, or it can be neutral, which means that none of the teams has possession over the control point.
- obstacle: obstacles are locations on the map to where tanks cannot move (and control points also cannot be located there), although path can lead to nodes which contain an obstacle.
- unit: units are moving objects on the map, they are controlled by one of the teams and they are described in detail at Section 4.3.

Units

The moving units on the map are tanks, which can move on the edges of the graph and can execute actions in their environment. The units can be individually controlled by a team. There are two teams present in this environment which battle against each other. All the units are identical regarding their properties, they can be described by the same parameters. These parameters are the position, orientation, healthpoint. The meaning of these parameters is

- position: the location of the tank identified by the node on the graph. A unit can occupy exactly one node at a time, and at most one unit can reside on a node (this restriction also applies to units in the same team).
- orientation: the angle of the tank, which determines the angle of shooting and on which edge the unit can move forward. The orientation of the tank considering that the map is a standard grid can be 0, 90, 180 or 270 degrees.
- health point: the health point of the unit is the number of shots the unit can take without being destructed. If the health point of a unit is above zero, the unit can execute actions and can move on the map. If the health point of a unit reaches zero, it means that the unit is destructed and it cannot execute actions and cannot move. It is also removed from the node it resided in, and another unit can occupy that node.

The available actions for the individual agents are the Left, Right, Forward, Shoot and NoOperation (NOP). The meaning of these actions is:

- Left: the orientation of the unit changes by +90 degrees
- Right: the orientation of the unit changes by -90 degrees
- Forward: the unit tries to move to the adjacent node in the direction of its orientation. If the adjacent node is an obstacle or there is no adjacent node (because the unit is located at the perimeter of the graph) the unit remains on the same node it tried to move away from.
- Shoot: the unit shoots. The angle of the shoot is not deterministic, every tank has a spread of shoot and the actual angle of shoot is the orientation of the tank modified by a random positive or negative angle between 0 and the half of the maximum angle of shoot. The range of shoot is unlimited, and in case of the shoot hits another unit, the health point of the unit that was hit is decreased by one. Friendly fire is available, i.e. tanks from the same team can also shoot each other. Units cannot shoot through obstacles and control points. The path of the bullet that is fired is calculated using the actual angle of the shoot. Every discrete location (node) on the map this path intersects is tested for hit, by always checking the nearest unchecked tile starting from the firing unit. If the path intersects a node that is not empty, the object located on the node is considered hit and the bullet stops. If the object is a tank, the tank that is hit loses a healthpoint, while in case of obstacle and control points nothing happens. The process of determining which object is shot is shown in the following pseudocode:

```
angle ← calculate shoot angle (orientation, spread)
path ← calculate path (angle, position)
nodes ← get intersecting nodes (path)
while there is unchecked node in nodes
  node ← get nearest node (nodes, position)
  if isChecked (node)
    continue
  endif
  setChecked (node)
  obj ← getObject (node)
  if obj ∈ {empty, obstacle, controlPoint}
    break
  endif
  if obj is tank
    decrease HP (tank)
    break
  endif
end while
```

- NOP: the unit does nothing (does not shoot and stays where it was).

Teams

Two teams are present in the concrete game, each team controls four units. The starting position of the units is predefined; they are located at opposite sides of the map. The teams control their units by means of strategic level actions. The available list of strategic level actions is: Encircle, Retreat, Advance and Destroy. The strategic level actions are sent to the whole team, and are further broken down to group level actions. The meaning of these strategic level actions is as follows:

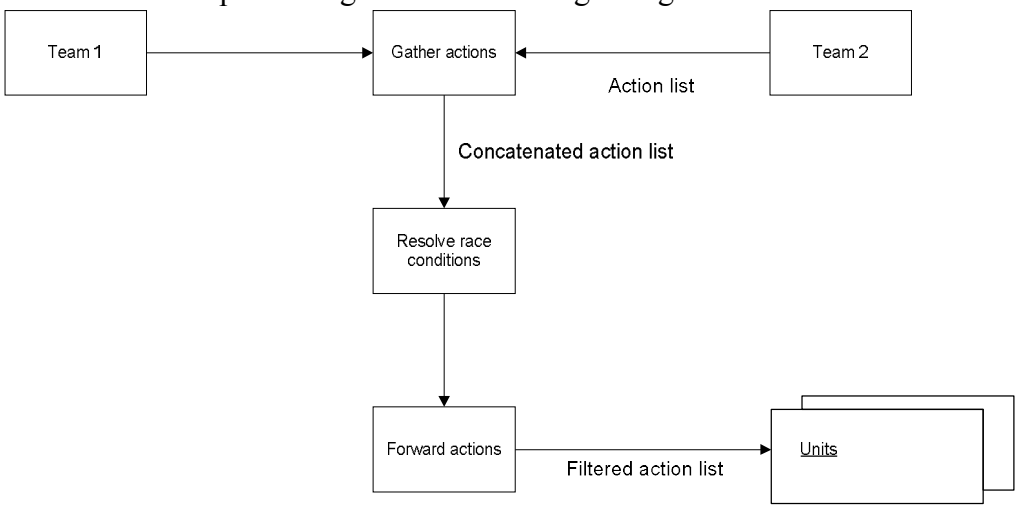
- Encircle: The goal of this command is to stall the opponent group and prevent it from joining the others group for reinforcement. After executing the Encircle strategic action, the expected outcome is that the groups participating in the execution of the Encircle command move closer to the targeted opponent group, and they block the directions in which the opponent group can move as much as possible.
- Retreat: The goal of the Retreat strategic level command is to increase the distance between the groups owned by the executor of the command and the opponent groups. The expected outcome of this strategic level action is that the groups move as far away as they can from the opponent groups, even if the opponent groups are executing some kind of chasing maneuver, during which they try to decrease the distance before the groups.
- Advance: The goal of the Advance strategic level command is to decrease the distance between the controlled groups and the opponent groups. The expected outcome of this command is that the controlled groups move as close to the opponent groups as possible, thus decreasing the distance between them. The groups should be

able to decrease the distance even if the groups belonging to the opponent are executing some kind of retreating maneuvers.

- Destroy: The goal of the Destroy command is to decrease the health point of the units in the opponent group. The expected outcome of this strategic level command is that the average health point of the opponent group is decreased as much as possible, the ideal outcome is when all of the units in the opponent group are destroyed, meaning that their health point is decreased to zero.

A score is maintained for each of the teams, which is initially zero, and it is increased in every timestep by the number of control points that are owned by a team at the actual timestep.

The teams are the highest level entities in the game from the point of view of the simulator; the actual action processing is done according to Figure 4.



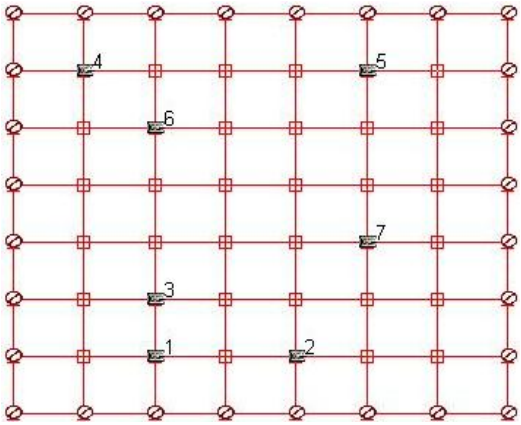
4. figure. Action processing in the simulator

Groups

The maximum number of units in a group was two units. The action list available to a group contained the Left, Right, Forward and Shoot actions. A group level action is sent to a smaller group of units, and it is further broken down to unit level actions. The meaning of these group level actions is:

- Left: The group turns left, meaning that the individual units in the group change their orientation by +90 degrees.
- Right: The group turns right, meaning that the individual units in the group change their orientation by -90 degrees.
- Forward: The group moves forward, meaning that every unit in the team advances one node in the direction of the orientation of the group leader unit. If the orientation of the units is not the same in a group, a group leader is selected and the other units modify their orientation to match the orientation of the leader. If the orientation of every unit in the team is the same, the forward command is executes. The leader of the group is selected by choosing the unit that was first assigned to the group.
- Shoot: Every unit in the group executes the shoot action.

An example partitioning of the units into groups is shown in Figure 4:



5. figure. Example state of the game

The groups created by the group creator module (the group creator module is described in detail in Section 3.3.1) for this state of the game were:

- 1st group: units indexed by 1 and 3, the group leader is unit indexed by 1
- 2nd group: units indexed by 2 and 7, the group leader is unit indexed by 7
- 3rd group: units indexed by 4 and 6, the group leader is unit indexed by 4
- 4th group: the unit indexed by 5, which is also the group leader. Note that there are no more units in this group.

Results

The concrete demonstration game contained two teams, all teams consisting of four units. The teams are placed on opposite sides of the map. The goal of a team is to destroy as many adversary units as possible while keeping as many own units alive as possible. The performance of a strategy is measured by playing against an opponent with a fixed strategy, for example an opponent using random strategy. The performance value is calculated according to the following formula:

$$\text{moreUnit} = \frac{\#\text{own units}}{\#\text{opponent units} + \#\text{own units}}$$

This formula returns relatively high values if the team has more units than its opponent and relatively low values are returned if the opponent has more units. If the number of units in the two teams is the same, the formula returns the neutral 0.5 value (note that values closer to 1 means that the team of the learning agent outnumbers its opponent team, and values closer to 0 means its opposite). The actual value of the performance is dependant of the starting number of units in each of the teams, but changes in the value show the changes in the power relations.

The state of the game is described as the joint state of the individual units (the state of a unit contains its position, orientation and healthpoint) extended with other global features (like the value of the moreUnit feature).

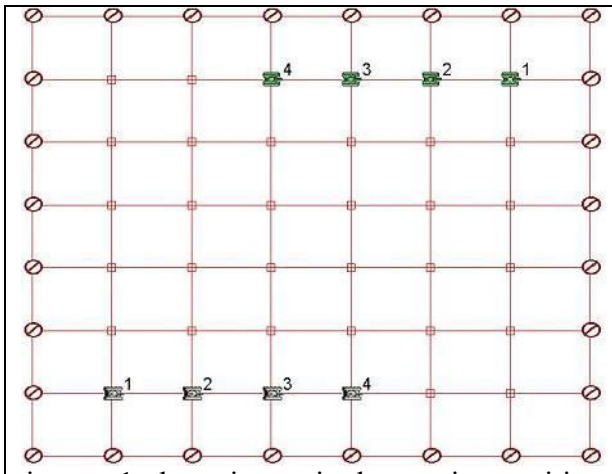
The learning parameters used during learning at the strategic level are shown in Table 1.

name	*value*
α	0.25
δ^l	0.1
δ^w	0.004
β	0.8
λ	0.5
γ	0.99
ε	0.05

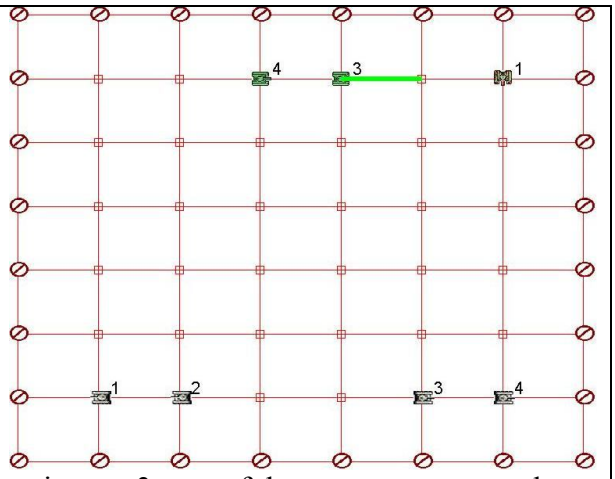
1. table. Parameters of GraWoLF during strategic level learning

The detailed description of the parameters can be found in Section 3.1.

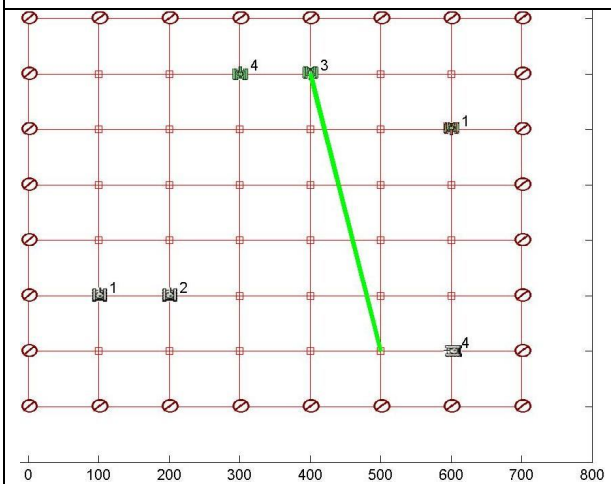
Some snapshots from a battle against a random opponent are shown in Table 2.



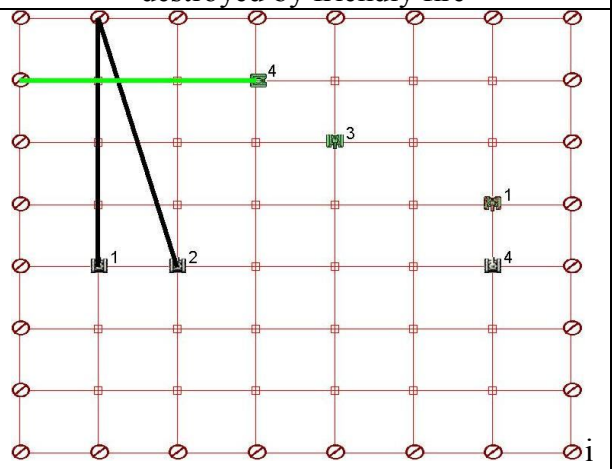
in step 1, the units are in the starting position



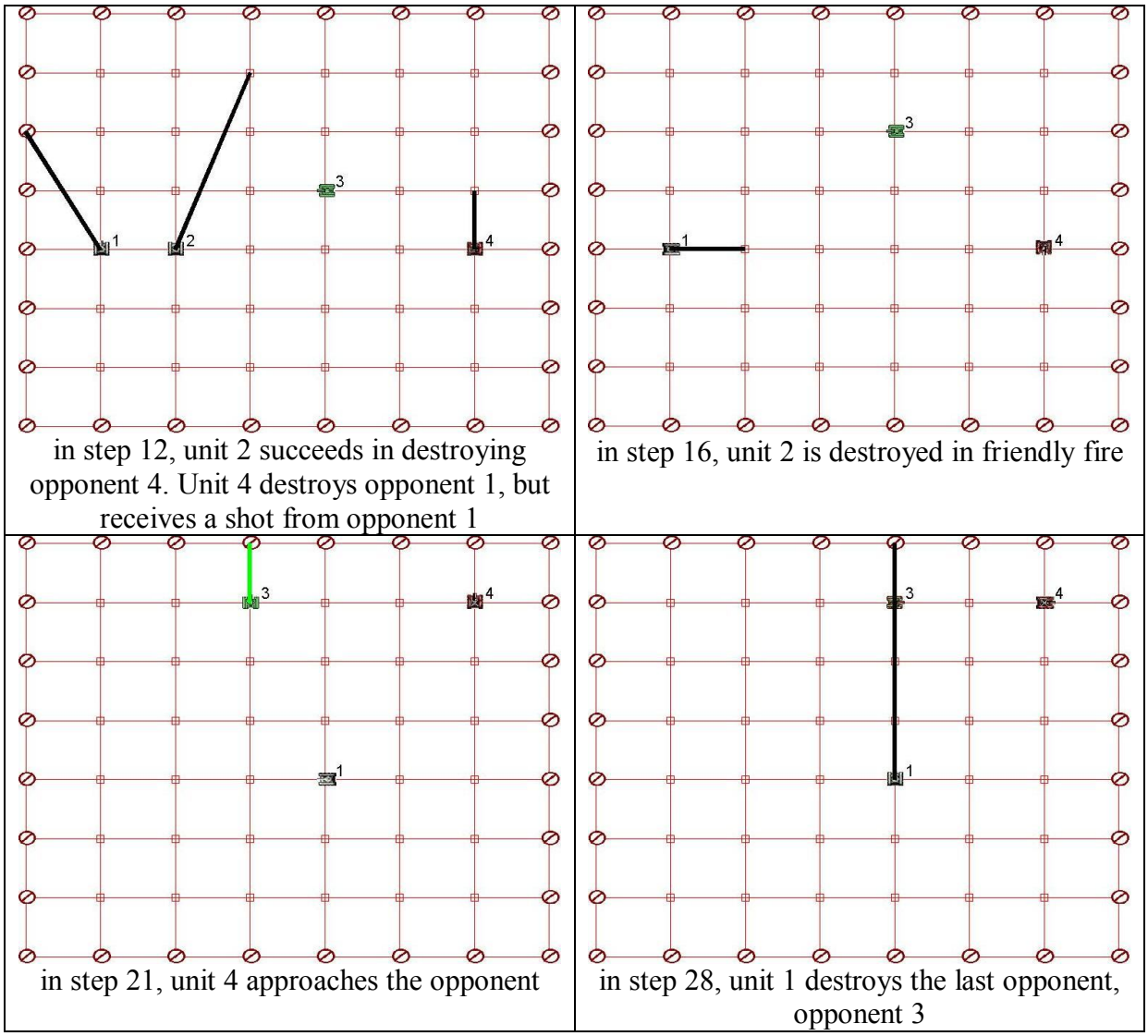
in step 3, one of the groups moves to the right side of the map. An opponent unit is destroyed by friendly fire



in step 7, a unit is destroyed by the enemy. Unit 1 and 2 starts to move upwards



in step 10, unit 1 and 2 are shooting but they hit nothing. Unit 4 approaches opponent 1

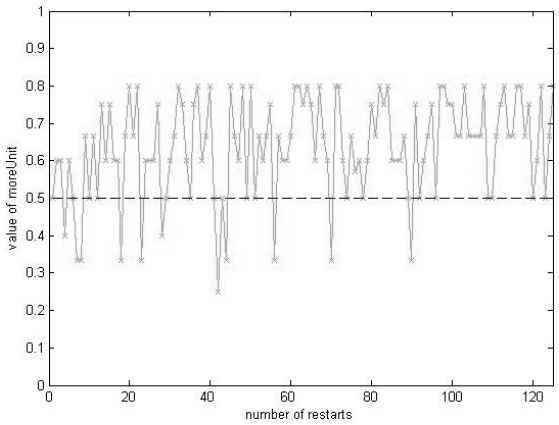


2. table. Battle against a random opponent [10]

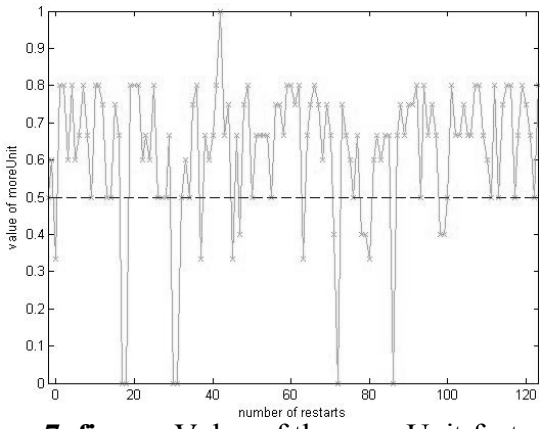
The performance of the learning agent is measured by the moreUnit feature, and as in the initial position the number of units in all teams is the same, the neutral value of the moreUnit feature is at 0.5. Three resulting learning curves are shown in the following figures (figure 6, 7 and 8), two of them correspond to a battle against a random opponent, and one corresponds to a battle against a static opponent.

These learning curves indicate that the learning team agent is able to find a locally optimal strategy against either a randomly acting or a static opponent. A policy is said to be good if it outperforms the initial policy (which is the random policy at the start of the learning sessions).

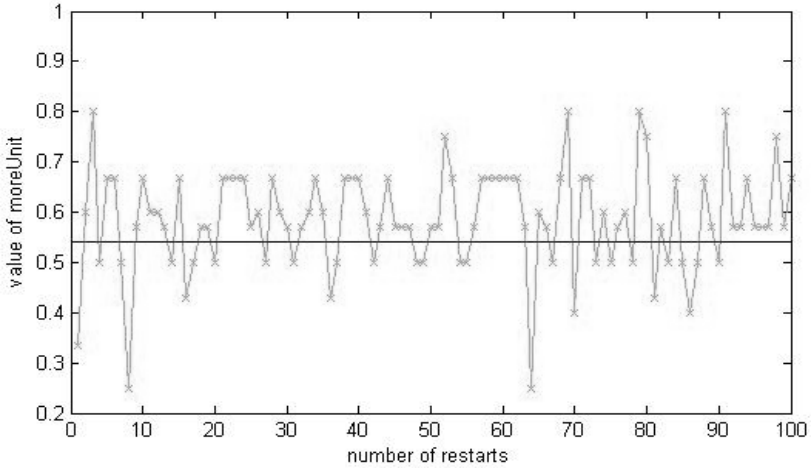
The performance of a final strategy can be measured by the average number of battles that are won by using that strategy. This performance value of a random policy against a random opponent is around 50%. If the learning agent can find a final policy that has a better average winning number, the strategy is better than the initial, which means that the learning session was not useless.



6. figure. Value of the moreUnit feature against a random strategy [10]



7. figure. Value of the moreUnit feature against a random strategy [10]



8. figure. Value of the moreUnit feature against a random strategy [10]

Figure 8:

CONCLUSION

The proposed solution for military operation planning was able to win an average of 60-65% of the games in the demonstrational domain. The solution relies on a spatial relationship between the agents and reduces the complexity of the learning algorithms by defining a hierarchy amongst the agents.

The solution efficiently reduces the complexity of the aggregated agent when there are a limited number of groups defined in a team. The solution assumes that a locally optimal policy can still be found if the communication between the agents is restricted and only the agents in the same group coordinate their actions. The experimental results show that the agent can learn a policy with which it can outperform a rather strong opponent, but in some cases it is possible that the team agent cannot adapt its parameter vector to beat its opponent (this is the case for example when the team agent finds a locally optimal solution that has poor performance).

The original form of GraWoLF is able to find a locally optimal policy, and as this algorithm is used at both levels of learning in the proposed solution, the hierarchical solution guarantees only finding a locally optimal solution. As it can be seen from experiments, if the algorithm converges to a local optimum, it usually get stuck in there and the parameter vector changes only slightly during consecutive learning steps and cannot move away from the local optimum. Therefore the learning has to be restarted several times and strategies with poor performance should be eliminated.

The GraWoLF technique could be improved by using such a technique that is capable of finding a global maximum; and instead of tuning the parameter vector in the direction of the gradient, the global maximum finding method can be used.

The whole learning process could be sped up by reducing the size of the feature vector describing the state of the game, because thus the size of the parameter vector will also be reduced. This can be done by defining fewer features (but this way information will be lost) or by using some compression technique, like hashing [7]. The run time of the learning algorithm can be reduced by doing the hierarchical decomposition less frequently (instead of creating groups in every timestep, the creation of groups can be done in say every ten timesteps, because agents in the same group tend to remain together).

A more intelligent group coordination behavior could be achieved using distributed rewards [8]. This means that a group of agents does not only observe the global reward signal, but they observe also an individual reward. This way the groups will know whether their individual performance is influencing the global reward in a positive or a negative way and they can individually adapt their behavior to increase the local (individual) reward, and thus hopefully increasing the global reward too. If there is only a global reward signal available to the groups in the team, one well performing group can make the others believe that they are performing well too (or one poorly performing group can reduce the global reward in such a way that the other groups believe that they are performing poorly), but by using local rewards this problem is solved.

REFERENCES

[1] I. Harmati, K. Skrzypczyk. Robot team coordination for target tracking using fuzzy logic controller in game theoretic framework. : Robotics and Autonomous Systems 57(1):75-86, 2009.

[2] Y. Liu, M. A. Simaan, J. B. Cruz. An application of dynamic Nash task assignment strategies to multi-team military air operations. : Automatica, 39:1469-1478, 2003.

[3] Russel, S. J., Norvig, P. Artifical Intelligence A Modern Approach. 1995.

[4] R. E. Precup, S. Preitl. Optimisation criteria in development of fuzzy controllers with dynamics. : Engineering Applications of Artificial Intelligence 17(6):661-674, 2004.

[5] von Neumann, J., Morgenstern, O. Theory of Games and Economic Behavior. 1944.

[6] J. B. Cruz, M. A. Simaan, A. Gacic, Y. Liu, Y. Moving horizon game theoretic approaches for control strategies in a military operation. : IEEE Transactions on Aerospace and Electronic Systems 38(3):989-999, 2002.

[7] Bowling, Michael. Multiagent learning in the presence of Agents with Limitations. 2003. Vols. CMU-CS-03-118.

[8] Bagnell, J. A., Ng, A. Y. On Local Rewards and Scaling Distributed Reinforcement Learning. 2005.

[9] Shapley, L.S. Stochastic Games. 1953.

[10] Kisfaludi, Peter. Strategy planning in multiagent robot systems. 2011.

[11] Kok, J. R., Vlassis, N. Collaborative Multiagent Reinforcement Learning by Payoff Propagation. 2006.

[12] T. Basar, G. J. Olsder. Dynamic noncooperative game theory. : SIAM, 2nd edition, 1999.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kassai Károly
kassai.karoly@hm.gov.hu

A KATONAI ELEKTRONIKUS ADATKEZELŐ KÉPESSÉGEK INCIDENSKEZELÉSÉRE VONATKOZÓ ÁLTALÁNOS KÖVETELMÉNYEK

Absztrakt

Az elektronikus adatkezelés fontos és egyben sérülékeny szolgáltatás a katonai üzemeltetési környezetben. A különböző formában jelentkező információs fenyegetések, mint a vírusok vagy rosszindulatú programok általi fertőzés, jogosulatlan rendszer vagy szolgáltatás hozzáférés, hoax fenyegetés, kiegészítve fizikai támadással, rendszer hibával vagy a nélkül, egyre hatékonyabb korlátozó hatásai vannak az információfüggő rendszerekre. A negatív hatások ellensúlyozás érdekében az IT üzemeltető szervezeteknek célszerű egy incidenskezelési keretrendszert kialakítani a kialakított folyamatok irányítására.

The electronic information handling is a very important and vulnerable service in military operational environment. The different information threats as a virus or malicious code infection, unauthorised system or service access, hoax, with or without physical attack, system error have more and more effective limitation impact of information dependent systems. To counterbalance this negative impacts the IT operating organisation should implement an incident handling framework for the control of established processes.

Kulcsszavak: *adat, információtechnológia, biztonság ~ data, IT, security*

BEVEZETÉS

Az elektronikus adatkezelő szolgáltatásokat fel kell készíteni az információs fenyegetések, meghibásodások ellensúlyozására. A gyakran csak statikusnak tekintett védelmi rendszabályokat úgy kell kialakítani, hogy a biztonság sérülése esetén is álljon rendelkezésre egy olyan eljárásrend, ami segíti a problémák érzékelését, a helyzet értékelését, a megfelelő reagálást.

A pontos értelmezés érdekében célszerű az alapvető kifejezések tisztázása a vonatkozó szabványnak megfelelően. E szerint:

- Információbiztonsági esemény (information security event): egy rendszer, egy szolgáltatás vagy egy hálózat állapotának azonosított előfordulása, amely az információbiztonsági szabályzat megszegését vagy a biztonsági ellenintézkedés hibáját, vagy egy addig nem ismert helyzetet jelez, amely biztonság vonzatú.
- Információbiztonsági incidens (information security incident): egyetlen, vagy egy sorozat nem kívánt vagy nem várt olyan információbiztonsági esemény, amely bekövetkezésének jelentős az üzleti műveleteket veszélyeztető és az információbiztonságot fenyegető valószínűsége van. [1]

A NEMZETI ÉS MÁS STRATÉGIAI SZINTŰ KÖVETELMÉNYEK

A minősített adat védelméről szóló jogszabályok szerint a minősített adat biztonságának sérülése esetén a biztonsági vezető feladata a kár felmérése, enyhítése, és lehetőség szerint a jogszerű állapot helyreállítása. A minősítő a Nemzet Biztonsági Felügyeletet tájékoztatja az esetről [2].

Elektronikus minősített adatkezelés esetén a rendszerbiztonsági felügyelet feladata a „hardver védelmét” rendszeresen ellenőrizni, és rendellenesség esetén annak kivizsgálása és a biztonság helyreállítása. A kivizsgálás támogatása érdekében a kormányrendelet naplózási kötelezettséget határoz meg, a naplófájlok időszakonként történő, dokumentált ellenőrzését rendeli el; a naplózási adatokról biztonsági mentéseket kell készíteni és azokat meg kell őrizni [3].

A Nemzet Biztonsági Felügyelet a vonatkozó törvény alapján kivizsgálja a minősített adatok védelmét érintő bejelentéseket és a biztonság megsértésével kapcsolatos eseményeket [4.].

A fentiek mellett az idézett jogszabályok a minősített adat biztonsága érdekében csak általános követelményeket határoznak meg, így megállapítható, hogy incidenskezelésre vonatkozó részletes módszertan, eljárásrend a minősített adatkezelés területén nem azonosítható.

Az elektronikus kormányzati gerinchálózat, illetve a csatlakozó hálózatok biztonságát szabályozó jogszabály szerint a „biztonsági események kezelése” és az „incidens menedzsment” címszavak gyakorlatilag azonos feladatokat tartalmaznak. E szerint:

- az észlelés történhet a hálózatfelügyelet észlelése, vagy felhasználói bejelentés alapján;
- rögzíteni kell az összes beérkező adatot és meg kell kezdeni az elemzést, az elemzési eredményeket öt évig meg kel őrizni;
- dönteni kell a beavatkozásról és tervet kell készíteni;
- a kialakított tervet végre kell hajtani és folyamatosan ellenőrizni kell, hogy nem keletkeznek-e újabb események.

Az incidens menedzselésnél ezek mellett szerepel még az a követelmény, hogy az üzemeltető incidens követő rendszerének képesnek kell lennie az incidensek életciklusának nyomon követésére, a korábbi incidensek közötti keresés támogatására [5]. A másik kormányzati szintű rendszer – az egységes digitális rendszer (EDR) – szabályozására vonatkozó kormányrendelet az előbbiekkel megegyező követelményeket tartalmaz, és sajnálatosan nem világítja meg még azt sem, hogy a címben szereplő „esemény" és „rendkívüli esemény" között mi a különbség [6].

A fentiek alapján megállapítható, hogy jogszabályok az incidenskezeléssel kapcsolatosan csak általános követelményeket határoznak meg, még a rendszer-specifikus kormányrendeletek sem tartalmaznak pontos eljárásokat.

A katonai szervezetek adatkezelésére vonatkozó incidenskezelési eljárások meghatározásának szükségességét a következő rövid stratégiai szintű áttekintés szemlélteti.

A Nemzeti Biztonsági Stratégia megállapítja, hogy a rendszerek sebezhetősége olyan kockázati tényező, amelynek jellegzetessége, hogy kis erőösszpontosítás nagy távolságból is rendkívüli kárt képes okozni. A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű, biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére [7].

A Nemzeti Katonai Stratégia szerint a Magyar Köztársaság biztonsági környezetében biztonsági kockázatot jelenthetnek a kritikus infrastruktúra elleni támadások [8].

Az EU Biztonsági Stratégia megállapítja, hogy a kereskedelem, a befektetések, a technikai fejlődés erősítik Európa függőségét – így sebezhetőségét – az összekapcsolt szállítási, energetikai, információs és egyéb infrastruktúrákon keresztül [9].

Az új NATO Stratégiai Koncepció szerint a cyber-támadások egyre gyakoribbá, szervezettebbé vállnak és egyre nagyobb károkat okoznak a közigazgatásban, az üzleti életben és gazdaságnak, veszélyeztethetik a szállítást és az energia rendszereket és egyé kritikus infrastruktúrákat. A támadások elérték azt a küszöböt, amikor már a nemzeti és Euro-Atlanti jólétet, biztonságot és stabilitást fenyegetik [10.].

A stratégiai szintű megfogalmazások jó összegzik a fenyegetések és sebezhetőség szintjének emelkedését, az információs függőséget, illetve a kritikus infrastruktúra védelem (crtical infrastructure protection; CIP, magyarul: KIV) területén belül a kritikus információs infrastruktúra védelem fontosságát, ami kellő alapot kell, hogy adjon a kormányzati és alacsonyabb szintű szabályozásoknak.

A katonai szervezetek növekvő információfüggősége és az egyre veszélyesebb információs fenyegetések miatt célszerűnek látszik a honvédelmi tárca szervezetei számára az elektronikus adatkezelő képességek incidenskezelésére egy olyan általános követelmény kialakítása, ami szakmailag megfelelően támogatja a rendszer-specifikus szabályozások kialakítását.

AZ ÁLTALÁNOS INCINENSKEZELÉS KIDOLGOZÁSÁT TÁMOGATÓ FORRÁSOK

A nemzetközi és nemzeti információbiztonsági menedzsment szabványok [11][12] alapján készült nemzeti ajánlás [13] gyakorlatilag a szabványok ajánlásait tartalmazza, magyarázatokkal bővíti. Ezen kívül az informatikai szolgáltatás nyújtására vonatkozó szabvány nyújt segítséget a feladatok áttekintéséhez [14][14].

Az informatikai irányítás ellenőrzését célzó COBIT módszertan vonatkozó részeit szintén érdemes figyelembe venni, mert a kormányzati ellenőrzést végző szervezetek e módszertant követik [14]. A nemzetközi ajánlások, szabványok mellett más nemzeti vagy egyéb szakmai ajánlások adják a forrást, melynek feldolgozása képezi az incidenskezelés fontosabb feladatait [16][17].

Egy MH szintű szabályozásnak szükségszerűen keret-rendszerűnek kell lennie, így a cikk a helyi hálózatok, eszközök, valamint egy országos hálózat incidenskezeléséhez szükséges feladatok nem minősített adatokkal történő támogatását célozza az említett követelmények, ajánlások feldolgozásával, és nem helyezi előtérbe a központi szolgáltatások kérdését, melyet más formában célszerű rendszer-specifikusan kidolgozni.

AZ ESEMÉNYEK ÉS BIZTONSÁGI HIÁNYOSSÁGOK JELENTÉSE

A jelentésre kötelezett adatok formáját, tartalmát, a jelentési határidőket rendszerenként úgy kell meghatározni, hogy teljesüljenek a jogszabályokban és az állami irányítás egyéb jogi eszközeiben megfogalmazott követelmények. A jelentések rendjét a következő általános elvek szerint kell kialakítani:

- Helyi hálózat, vagy önálló telepítésű eszköz esetében alap biztonsági osztály esetében a rendszergazdát, vagy kijelölt szervezeti elemet kell értesíteni. MH szintű hálózat esetében a hálózatgazdát és az információvédelmi szakfelügyeletet végző szervezetet kell értesíteni.
- Minősített adat elektronikus kezelésére feljogosított rendszer esetében az incidenseket – beleértve a rejtjeltevékenység körébe tartozó incidenseket is – a honvédelmi szervezet biztonsági vezetőjének az információvédelmi szakirányítást végző HM szerv felé kell jelentenie.

Jelentési kötelezettség alá tartoznak minimum az alábbi esetek:

- felismert, vagy felismerni vélt biztonsági események vagy védelmi gyengeségek, biztonsági rések;
- a rendszer hibás működése (hardver, szoftverhiba), vagy engedély nélküli konfigurációváltozás, esetleges emberi hibák;
- a szabályzatoknak nem megfelelő működés, vagy hiányos, pontatlan szabályozás;
- a fizikai védelmi rendszabályok sérülése;
- engedély nélküli rendszerhez vagy adatokhoz való hozzáférés.

A kezdeti jelentésekben a következő adatokat kell jelenteni:

- jelentő személy, szervezet megnevezése;
- érintett rendszer, vagy önálló telepítésű eszköz megnevezése, helye;
- az incidens bekövetkezésének/észlelésének ideje;
- az incidens során: megtörtént/kísérlet történt rá/nem történt meg: bizalmasság, sértetlenség rendelkezésre állás elvesztése;
- az incidens hatásaként: zavart keletkezett a szervezet működésében, személyiségi jogok sérültek, pénzügyi/gazdasági veszteség keletkezett, minősített adat bizalmassága sérült (minősítési szint és kezelési utasítás és adatforma azonosításával);
- az érintett rendszer/hardverelem jellemzői;
- az incidens oka: katasztrófa/egyéb károsodás, hacker vagy egyéb külső behatolás, fizikai behatolás; rendellenes működés vagy technikai hiba, rosszindulatú szoftver, nem szabályos használat, személyi hiba vagy egyéb más ok;
- milyen művelet során derült ki az esemény;

- egyéb fontosnak tartott adatok.

A felhasználókat a jelentési kötelezettség megtételében formanyomtatványokkal, a segítségül hívható személyek nevének, telefonszámának azonosításával, help desk szolgáltatással kell támogatni.

A fenti eljárásrend ugyanígy vonatkozik a rendszer üzemeltető állományára is, tehát az ügyeletes adminisztrátor, technikus által érzékelt technikai paraméterek, riasztási jelzések ugyanezen rendben kell, hogy jelentésre kerüljenek.

A kezdeti jelentéseket nyílt formában kell megtenni, a szükséges védelmi intézkedések megtétele, együttműködő partnerek értesítése, illetékes hatóságok felé történő időbeni jelentés érdekében. A jelentési kötelezettséget nem lehet helyi kivizsgálás indokával késleltetni. Újabb tények felszínre kerülése esetén a kezdeti jelentések után további pontosítások, kiegészítések tehetők.

Az incidensekre történő reagálás rendszabályait, és azzal kapcsolatos egyéni feladatokat az információs rendszer sajátosságainak megfelelően rendszeresen, minimum évente oktatni kell a következő szempontok figyelembe vételével:

- ismertetni kell a helyes viselkedés szabályai az incidens bekövetkezésekor, vagy annak észlelésekor: minden lényeges adat feljegyzése (megsértett szabály, az előforduló rendellenes működés, képernyő üzenet);
- incidens észlelése esetén az egyéni beavatkozások tilalma, a jelentési, értesítési, valamint esetleges bizonyítékszolgáltatásra vonatkozó kötelezettségek.

Az oktatáson esettanulmányok, szimulált esetek feldolgozásával célszerű az incidens helyzetekre történő reagálás hatékonyságát növelni, a krízishelyzetek megoldását támogatni.

A rendszeradminisztrátorok, biztonsági felelősök és egyéb technikai feladatokat ellátó személyek esetében MH rendszerek és minősített adatkezelő rendszerek esetében automatizált mechanizmusokkal, valósághoz közeli tréning környezet biztosításával kell a hatékonyságot növelni.

AZ INCINDENSEK MEGOLDÁSÁNAK TÁMOGATÁSA

E cikkben részletes megoldási javaslatok nem dolgozhatók ki, így a továbbiakban csak a bejelentés (vagy automatikus jelzés) alapján történő megoldás fontosabb tényezőinek áttekintése történik.

A rendszerek üzemeltetői és biztonsági állományából azonosítani kell azokat a személyeket, szervezeti elemeket, akiknek feladata a bejelentett esemény vizsgálata (beleértve a kiegészítő adatok gyűjtését) és javaslattétel az incidensé nyilvánításra, valamint azt a felelős vezetőt, akinek feladata az incidenskezelés elrendelése, szükség esetén a működésfolytonossági tevékenységek beindítása.

A rendszerek sajátosságainak és a rendelkezésre álló erőforrások figyelembe vételével a kezelendő incidenseket fontosságuk szerint be kell sorolni, és azonosítani kell az elhárításhoz (megoldáshoz) szükséges előre látható lépéseket. Az esetek fontosságával arányosan azonosítani kell azokat a szervezeti elemeket, amelyek megerősítésül bevonhatók a feladatok megoldásába, beleértve a más szervezetektől kapott erő, eszköz lehetőségét, szakmai támogatást.

A rendszer-specifikus jellemzők szerint az üzemeltető állomány tevékenységének könnyítése, illetve a szubjektív hibák kizárása, a vezetői döntésekkel járó időveszteség elkerülése érdekében beavatkozási sablonokat kell kialakítani, tesztelni és jóváhagyatni. Így az egyedi döntésekre csak abban az esetben van szükség, ha a megoldás a sablonoktól való eltérést igényli.

A tapasztalatok értékelése és hasznosítása érdekében az incidensekről szóló jelentéseket meghatározott időszakonként összesíteni kell. A tapasztalatok gyűjtése, értelmezése és elemezése alapján az üzemeltetési és védelmi rendszabályokat, eljárásrendet pontosítani, szükség szerint fejleszteni kell. A rendszabályok pontosítása az adott tapasztalatnak megfelelően lehet a rendszerhez kötött technikai vagy adminisztratív jellegű változtatás, de az előfordulás súlyosságának és gyakoriságának függvényében magasabb szintű szabályozási változás sem zárható ki (információbiztonság politika, jogszabály).

Az incidens reagálásra irányuló képességeket a hatékonyság felmérése érdekében teszt, gyakorlások formájában időszakonként, a rendszer-specifikus sajátosságoknak megfelelően, dokumentálva kell ellenőrizni. A tesztek és ellenőrzések – mint kötelező jellegű, nem népszerű események – természetesen csak akkor érhetik el céljukat, ha a sematikus felszínes ismétlés, vagy ugyanazon mozzanatok sorozatos gyakorlása helyett az üzemeltető és biztonsági menedzsment pontosan kidolgozza és fejleszti a gyakorlásokat, a valósághoz közeli teszt feladatokat, gyakorlási lehetőségeket alakít ki, monitorozza az egyéni teljesítményeket, pótfoglalkozásokat szervez a hiányzóknak, gyakoroltatja a külső és belső szervezetek közötti együttműködési feladatokat is.

A későbbi visszakereshetőség, elemzés és feldolgozás érdekében az incidensekre vonatkozó adatokat, valamint a vizsgálati eredményeket rendszerenként, a biztonsági dokumentumokkal együtt kell tárolni.

Az MH szintű adatkezelő rendszerek külső csatlakozásainak, illetve rendszer belső védelmének emelt szintű biztonsága érdekében a detektálás, elemzés, értékelés, reagálás és bizonyítékszolgáltatás céljait szolgáló központi eseménykezelő rendszert a nemzetközi szabványok, és NATO ajánlások szerint kell kialakítani. A központi eseménykezelő rendszer felépítését, szervezeti kapcsolatait, működési rendjét egyedileg kell meghatározni.

A napjainkban egyre népszerűbb – de nemzetenként és szervezetenként egyedileg definiált – cyber-védelmi képesség nemzeti szintű kialakítása remélhetően nem sokáig várat magára. A központi követelmények mindenféleképpen hatással lesznek a fentiekben meghatározott általános követelményekre, de a katonai adatkezelő képességek egyedisége, specialitásai miatt mindenféleképpen szükség van a katonai sajátosságoknak megfelelő specializált eljárások kialakítására.

ÖSSZEFOGLALÁS

A fenti általános feladatok a helyi vagy rendszer-specifikus sajátosságok (adatkezelési jellemzők, minősítési szint, prioritások) alapján az incidens kezelés feladatai egyedileg kidolgozhatók, vagy a felhasznált irodalom alapján tovább bővíthetők. A NATO vagy EU minősített adatok kezelésére vonatkozó rendszabályokkal az incidenskezelés ugyanígy specializálható.

Az elektronikus adatkezelés egyre bonyolultabbá válása megalapozza azt a következtetést, hogy már a helyi rendszerek esetében sem lehet elégséges az emberi erőre támaszkodás. A hálózatok üzemeltetése közben normál esetben is hatalmas mennyiségű adat keletkezik, egy-egy esemény többszörös, különböző szempontú adatokat generál. Az e mellett megjelenő hálózati forgalmi vagy tűzfal adatok még elméletileg sem kezelhetők kézzel.

A napló adatok kezelése, mentése egyre bonyolultabbá válik, illetve az adatok szűrése, elemzése és a szükséges követelmények levonása további alkalmazásokat igényel, speciális szakértelmet követel. Az országos méretű hálózatoknál ezek a jellegzetességek nagyságrendekkel bonyolultabb helyzeteket okoznak.

E sajátosságok miatt a honvédelmi tárcánál szükség van a hálózati biztonsági kérdések erőteljes támogatására, és incidenskezelés esetén is a korszerű informatikai megoldások rendszerbe állítására. Ezt a szükségszerű igényt alátámasztja napjaink eseményei alapján az a

nemzetközi szinten is egyre többet hangoztatott jelenség, hogy a hálózatokat nem elégséges csak a külső támadásokra felkészíteni, azok belülről is sebezhetők. Nyilvánvaló, hogy a felügyelt pontok, a szenzorok számának növekedése az incidenskezelést is bonyolultabbá teszi.

A cikk alapján kijelenthető, hogy a tárca szintű információ biztonságpolitika általános követelményrendszere is bővíthető az incidenskezelésre vonatkozó irányelvek rögzítésével, ami az ellenőrizhetőséget erősítheti az üzemeltető katonai szervezeteknél.

Ugyanígy fontos annak megállapítása is, hogy a nemzeti és nemzetközi összekapcsolások miatt szükség van információbiztonság területén a menedzsment és a technikai szintű együttműködési megállapodásokra, melyek lehetővé teszik a korai előjelzést, segítséget nyújthatnak az incidensek felderítésben és az okozott károk helyreállításában, illetve a bizonyítékok összegyűjtésében és benyújtásában.

Felhasznált irodalom

[1] MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése, 3.2. p. és 3. 3. p.

[2] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 60. §. 1-2. bekezdés OK

[3] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1. §. 22. p. és 58-59.§.

[4] 2009. évi CLV. törvény a minősített adat védelméről, 20. §. (2) j-k) p.

[5] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról, 3. sz. melléklet, Az elektronikus kormányzati gerinchálózat informatikai biztonsági szabályzata, 2. 5. 8. p. OK

[6] 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, 2. sz. melléklet Az EDR használati szabályzata, 2. 2. 3. p. események és rendkívüli események jelentése, kezelése

[7] 2073/2004. (III. 31.) Korm. határozat, a Magyar Köztársaság nemzeti biztonsági stratégiája, II. 1. 6. és III. 3. 7. p.

[8] 1009/2009. (I. 30.) kormányhatározat a Magyar Köztársaság Nemzeti Katonai Stratégiájáról, I. fejezet

[9] A Secure Europe in a Better World, European Security Strategy 2003, „The global challenges" fejezet

[10] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010

[11] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, „A" melléklet, A 14. 1 – 14. 1. 5. p.

[12] ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 14. 1.1 – 14. 1. 5. p.

[13] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v. 1.1. 2008, 14. fejezet

[14] Informatika. Szolgáltatásirányítás 1. rész: Előírás (MSZ ISO/IEC 20000-1: 2007), 6. 3. fejezet

[15] Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések (COBIT 4.1) DS-6, DS-8, és DS-10. fejezetek

[16] A Chief Information Officer kézikönyve, 2003, Management Kiadó Kft. ISBN 963 86190 9 0; 3/3. 1. 2.

[17] Computer Security Incident Handling Guide (SP-61 revision 1), 3- 8. fejezet

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kuris Zoltán
Zoltan.Kuris@bm.gov.hu

A MOBILKOMMUNIKÁCIÓ DETERMINÁNSAI ÉS DILEMMÁI A NEMZETI MINŐSÍTETT ADATOK TOVÁBBÍTÁSÁVAL ÖSSZEFÜGGÉSBEN

Absztrakt

A nagy sávszélességű, nagymennyiségű és gyors adatelérésű megoldások és eszközök elterjedése, a publikus hálózatokon való kommunikáció ma már triviális. Ugyanakkor egy érdekes és feltáratlan terület a szenzitív, vagy nemzeti minősített adatok, a fenti elvek szerinti mobilkommunikációját megvalósító „teljes életciklusában hazai felügyeletű" szakszerűen és jogszerűen alkalmazható eszközök (rendszerek) rendszeresítési és rendszerengedélyeztetési folyamatának vizsgálata. A szerző publikációjában kifejti a témával kapcsolatos determinánsokat, elemzi a dilemmákat, összehasonlító elemzés módszerével bemutat néhány - általa alkalmasnak ítélt – technológiát és ajánlást, irányelveket fogalmaz meg a nemzeti akkreditációval összefüggésben.

The high-bandwidth, large and rapid date access solutions and the proliferation of public communication networks are now trivial. However, an interesting and unexplored area is the investigation of sensitive, or classified national information in accordance with these principles, mobile communication implementing "full life cycle of domestic supervision" properly and lawfully applied tools, and the system permission and the systematic process. The author explains the most relevant determinants in his publication, analyzing the dilemmas. He also shows some technologies and a recommendation determines guidelines in concern with national accreditation.

Kulcsszavak: *érzékeny adat, minősített adat, adatkapcsolati lefedettség, titkosítás, rejtjelzés, VOIP kommunikáció, TEMPEST ~ stacioner, encrypted phones, encryption keys, Low audio latency*

BEVEZETÉS

Az információbiztonsági szakemberek alapvető küldetése annak hangsúlyozása, hogy a biztonság minden korban alapvető szükséglete volt a társadalmaknak, az államoknak, az egyéneknek. Ebből következik az a felismerés is, hogy a fejlődésnek, a társadalom működésének és a túlélésnek egyik döntő feltétele hogy a környezetről, a másik társadalomról, a másik államról, a másik emberről folyamatosan valós idejű és autentikus, használható információkat szerezzünk annak érdekében, hogy optimalizált döntéseket hozzunk. Ne legyenek illúzióink azzal összefüggésben, hogy az államok - és a nem állami szervezetek - ma is ugyanúgy folytatnak hírszerzést (információszerzést), mint akár évszázadokkal korábban, azzal a különbséggel, hogy a technikai és a tudományos fejlettség, magasabb színvonalon áll, és ennek minden előnyét, eredményét azonnal felhasználják a saját céljaik elérése érdekében. Az is axióma, hogy a hírszerzés az állam elemi szükségletei közé tartozik. A régi mondást („Navigare necesse est! = Hajózni pedig kell!") a hírszerzés és az információbiztonság nyelvére lefordítva annyit jelent: „információt szerezni pedig kell! Az információbiztonsági szakemberek igaznak tartják ezt napjainkban is és a jövőt illetően is.

A vezetésnek (így a kritikus infrastruktúrákat üzemeltető vezetőknek is) egymástól elválaszthatatlan két funkciója a szükséges információk beszerzésére és elemzésére alapozott döntés. A hatékony, jól működő hírszerzés önmagában nem vezet hatékony, bölcs döntésekhez. , de az információk hiánya, a hamis vagy félrevezető információk biztosan csak rossz döntéseket eredményeznek. Ugyanakkor, ha a vezető döntéskényszerben van, akkor a kevés, nem hiteles, nem időszerű információkra utaltan is dönteni kell. Ebből ered a hírszerzői körökben evidenciaként kezelt mondás, hogy „sohasem tudhatsz eleget".

A fentiekben kifejtett fenyegetésekkel szembeni hatékony védelmi intézkedések az defenzív hírszerzési tevékenység hatókörébe tartozó feladatok, amely alapvetően befolyásolják a kritikus infrastruktúra szektorainak – és ezen keresztül az állam működését is. A defenzív hírszerzés fontosságát és szükségességét részletesebben már diplomamunkában és előző publikációimban is kifejtettem. A defenzív terület hatékony működésének okán szükséges biztosítani a kritikus infrastruktúra szektorait irányító vezetők részére a szenzitív és/vagy minősített adatokat tartalmazó információ továbbítására alkalmas mobilkommunikációs eszközök alkalmazását, ugyanis ez egy hatékony eszköze az offenzív hírszerzés elleni védekezésnek. Figyelemre méltó szempont az is, hogy a védett mobil kommunikációs eszközök hiányában a vezetés operativitása és hatékonysága kérdőjeleződik meg. Ennek fontosságát a mai felgyorsult információs társadalmi fejlődéssel összefüggésben nem lehet elégszer hangsúlyozni.

A kutatási témámhoz kapcsolódóan, előző publikációimban már kifejtettem, – és feltehetően igazoltam is – hogy az információs társadalmak létfontosságú (kritikus) infrastruktúráinak hatékony és optimális működését meghatározzák a kritikus információs infrastruktúrák. Irányadó tudományos kutatási eredmények igazolták, hogy a kritikus információs infrastruktúrák működésében bekövetkezett zavarok kihatnak más szektorokra és kritikus infrastruktúra elemekre, illetve ezen keresztül a társadalom működésére is. Különösen igaz ez a fejlett információs társadalmak esetén, amelyek éppen az információs társadalmi fejlődésük kapcsán sebezhetővé válnak. Irányadó információbiztonsági szakemberek szerint egy adott információs társadalmi fejlettségi szinten lévő társadalom, az információs hadviselés dimenzióiban indított összehangolt támadással „visszavethető" az információs társadalmi fejlettségi szint alacsonyabb fokára. Előző publikációimban kutattam a komplex információbiztonság rendszerét, alrendszereit és elemeit is, annak okán, hogy - irányadó szakemberekkel egyetértve – fontosnak tartom a kritikus információs infrastruktúra területén alkalmazott védelmi intézkedések komplexitását.

A fenyegetésekkel szembeállított, megfelelően alkalmazott komplex védelmi intézkedések a kritikus szint alá csökkentik a maradvány kockázatot és megfelelően egyenszilárdá teszik a kritikus információs infrastruktúra rendszereit. Kutatási témámon belül meglehetősen markánsan jelenik meg a szenzitív, és minősített adatok védelmével összefüggő kutatási terület. Előző írásomban részletesen kifejtettem a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) [1] jótékony hatását a kutatási területemre. A Mavtv. kiadását követően megjelent kormányrendeleteket [2],[3],[4] is elemeztem, és kimutattam a NATO biztonsági szabályzatával [5] és az EU biztonsági szabályzatával [6] összefüggő koherenciát. Megállapítottam, hogy a minősített adatok védelmével összefüggő - nemzetközi törvényekben és szabályzatokban megfogalmazott irányelvek megfelelően átvezetésre kerültek a nemzeti jogszabályokba. Ez megteremtette annak lehetőségét, hogy a nemzeti minősített adatok kezelésére alkalmas elektronikus rendszereket lehessen akkreditálni és alkalmazni.

DETERMINÁNSOK, DILEMMÁK ÉS HIPOTÉZISEK

A fentiekben leírt szabályozók determinálták a rendszerek fejlesztésének rendszeresítési és rendszerengedélyezési eljárásainak szabályait. Ezeket a szabályokat a „stacioner" rendszerek esetén jól lehet alkalmazni, különösen abban az esetben, ha a minősített adatot kezelő elektronikus rendszer fogalmát a klasszikus értelemben vett informatikai rendszer irányából közelítjük meg. Ebben az esetben ugyanis a minősített adatok előállításáról gyűjtéséről, tárolásáról és továbbításáról van szó. Az ilyen rendszer teljes életciklusában előforduló tevékenység és az azzal összefüggésben alkalmazott személyi, adminisztratív, fizikai és elektronikus védelmi intézkedések halmaza – nemzetközi jogszabályokkal koherensen - többé kevésbé jól meghatározhatóak. Ugyanakkor, ha az „absztrakt" részben megfogalmazott „mobilproblematikát" vizsgáljuk, az információbiztonsági szakemberekben felmerülhet néhány megválaszolatlan (vagy félig megválaszolt) kérdés. A védett mobilkommunikáció értelmezési tartományában kutatva olyan érdekfeszítő témák elemzésére nyílik lehetőség, mint például a szóbeli közlés információtartalmának és az információtartalom minősített adatokkal összefüggő kapcsolatrendszerének vizsgálata. Ezzel összefüggésben a modellezésnél figyelemmel kell lenni arra, hogy az így értelmezett szenzitív, esetenként minősített adattartalommal is rendelkező információ mobilkommunikációs védett átviteli úton, - a kor színvonalának megfelelő infokommunikációs eszközök igénybevételével – történő átvitelére a felhasználói igények egyre markánsabban fogalmazódnak meg. Ezt az igény nem is olyan nehéz igazolni, hiszen az információs társadalom kritikus infrastruktúráinak biztonságos üzemeltetésének alapvető feltétele az operativitás, ennek pedig egyik előfeltétele az azonnali (védett mobilkommunikációs) eszközök) alkalmazása. Ezt felismerve a nemzetközi kutatási eredményeket és a nemzetközi sajtóban megjelent híreket, a közelmúltban a külföldi kritikus infrastruktúrák szektoraiban tapasztalható – a saját nemzeti hatóságaik által engedélyezett – a védett mobilkommunikációs eszközök megjelenése, elsősorban a védelmi és kormányzati szektoron belül [18]-[20].

Kiindulva tehát abból, hogy vannak determinált védelmi intézkedések, célszerű (mert az információs társadalmi fejlődés szakaszában a felhasználói igények kikényszerítik) kutatásokat végezni a nemzeti minősített adatok mobil kommunikációját biztosító lehetőségek és eszközök jogszerű és szakszerű alkalmazhatóságának területén. Publikációmban bemutatom a területet szabályozó jogszabályi környezetet, a jelenleg tapasztalható dilemmákat, kutatom a jelenlegi jogszabályi környezetben rejlő lehetőségeket, a szakszerű és jogszerű alkalmazás érdekében új – a jogszabályi környezetbe való beillesztésre alkalmas – irányelveket, javaslatokat fogalmazok meg. Összehasonlító elemzés módszerével bemutatok néhány „általam alkalmasnak talált" technológiát. Ezen túl leíró jellegű folyamatként

bemutatom a minősített információ továbbítására alkalmas mobil kommunikációs rendszer rendszeresítési és rendszerengedélyeztetési eljárásának főbb állomásait és dilemmáit.

AZ ÁLTALÁNOS SZABÁLYOZÁSI KÖRNYEZET LEHETŐSÉGEI ÉS KORLÁTAI

Mielőtt a védett mobil kommunikáció hazai lehetőségeinek elemzésére sor kerülne, szükségszerű néhány alapvető fogalom és a fogalmak közötti kapcsolatrendszer összehasonlító elemzését elvégezni. Ezzel összefüggésben, alapvetően szükséges helyesen értelmezni – illetve különbséget tenni – a közérdekű adat [17] 2.§ (4), a közérdekből nyilvános adat [17] 2.§ (5), nem nyilvános adat [17]19/A. § , a minősítéssel védhető közérdek [1] 5.§, az üzleti titok [16] 81.§ (2), és a minősített adat [1] 3. § (1) a) fogalmakat és azok tartalmát. Ugyanis az alkalmazható eljárásokat nagyban befolyásoló tényezőkről van szó. Tapasztalati tény, hogy a fogalmak helytelen értelmezéséből fakadóan –gyakran az információbiztonsági szakemberek is – téves következtetésekre juthatunk.

Ha a kritikus információs infrastruktúra elemek (szervezetek) irányából közelítjük meg a problémát, megállapíthatjuk, hogy az „adatbiztonság” érvényesítésével összefüggésben elmondhatjuk, hogy az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezeti intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek [17].

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik [17]. A védett mobil kommunikációs eszközöket illetően szögezzük le, hogy a továbbiakban a”védett mobil kommunikációs eszközök” fogalma alatt olyan eszközöket és alkalmazásokat értünk, amelyek olyan magas biztonsági szintű hardveres és szoftveres titkosítási algoritmusokat alkalmaznak, amelyek lehetővé teszik a hang és adat alapú információk adatátviteli úton történő magas titkosítási szintű nagy egyenszilárdságú továbbítását, kihasználva a publikus mobilkommunikációs hálózat adta lehetőségeket.

Figyelemmel arra, hogy adatkezelő természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet is lehet, az adatvédelem alanyát illetően igen széleskörű értelmezési tartomány határozható meg. Ugyanakkor az alkalmazott védelmi intézkedések kialakítását illetően egészen a minősítéssel védhető közérdek eléréséig nem találkozunk kötelező érvényű és megfelelően szankcionált szabályozókkal. Ebből az következik, hogy a nem nyilvános és üzleti titkoz képező adatok tekintetében nincsenek kötelező érvényűen meghatározva a személyi, fizikai, adminisztratív és elektronikai védelmi intézkedések, illetve a büntetőjogi szankciók sem jelennek meg egyértelműen. Ebből az következik, hogy ezeken az adatterületeken a védett mobilkommunikációs eszközök alkalmazását és alkalmazási szabályait az adatkezelő határozza meg, de ez az adatkezelőt illetően a közérdekű nem nyilvános és az üzleti titkot képező adat tekintetében nem kötelező érvényű. Ezzel összefüggésben született meg a Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszere (MIBIK). Természetesen az információbiztonsági irányítási rendszer szabvány szintű szabályozásának [9], [10] alkalmazása megfelelő ismereteket és alapokat ad a szervezetek részére, de jegyezzük meg, hogy az irányítási rendszer alkalmazása a szervezetek részére nem kötelező.

A védett mobilkommunikációs eszköz használata (rendszeresítése) a fent említett adatterületeken nincs hatósági engedélyezési eljáráshoz kötve és az alkalmazásukkal

összefüggésben nincs szabályozva az alkalmazandó személyi adminisztratív, fizikai és elektronikai védelmi intézkedések köre. Ez az anomália a nem nyilvános adatok és az üzleti titkok továbbítására alkalmas rendszerek használata esetén kétséget kizáróan (a szabályozás hiányából eredő) problémákat jelenthet, ugyanakkor az információs társadalmi fejlődés jelen szakaszában a kritikus információs infrastruktúrákat üzemeltető természetes és jogi személyek, illetve jogi személyiséggel nem rendelkező szervezetek részére ezen a szinten lehetővé teszik, (megengedik) a kor színvonalának megfelelő elektronikai rendszerek (ezen belül a mobilkommunikációs rendszerek) alkalmazását.

A MINŐSÍTÉSSEL VÉDHETŐ KÖZÉRDEK HATÓKÖRÉBE TARTOZÓ SZABÁLYOZÁSI KÖRNYEZET BEMUTATÁSA

Az előzőekben kifejtett adatkörökkel összefüggésben megállapíthatjuk tehát, hogy a védett mobil kommunikációs eszközök, eljárások alkalmazhatósága nem esik jelentős korlátozás alá, gyakorlatilag az adatkezelő belső szabályokban meghatározott védelmi intézkedések alkalmazása mellett igénybe veheti a védett mobilkommunikációs eszközök nyújtotta szolgáltatásokat.

Feltételezve azt, hogy a kedves olvasó már ismeretekkel rendelkezik ezen a szakterületen és a minősítéssel védhető közérdek hatókörébe tartozó szabályozási környezetet vizsgáljuk, azt tapasztaljuk, hogy a minősített adat védelméről szóló 2009. évi CLV törvény[1] és annak végrehajtási rendeletei[2], [3], 8] részletesen és szinte teljes körű szabályozást jelentenek a védelmi intézkedések teljes vertikumában. Megállapítható az is, hogy a nemzetközi törvényekkel meglévő koherencia jól érzékelhető akkor, ha részletesen tanulmányozzuk és összehasonlítjuk a NATO biztonsági szabályzatát, az EU Tanács biztonsági szabályzatát a fent említett Mavtv-el és végrehajtási rendeleteivel. Ez kétség kívül pozitív eredmény, de egyben statikussá teszi a hazai szabályozási környezetet, annak ellenére, hogy szakmai körökben vannak törekvések a hazai szabályozás módosításával összefüggésben. Irányadó szakmai körök véleményével azonosulva kisebb, módosítások (a védett mobil kommunikáció területén is) alkalmasak lennének optimális elektronikus rendszerek szakszerű és jogszerű bevezetésének elősegítésére. A jelenlegi hazai szabályozás kisebb anomáliáit jól példázza egy védett mobil kommunikációs rendszer bevezetésének modellezése, amelyre az alábbiakban gondolatkísérletet teszek.

Nemzeti minősített adat (információ) továbbítására alkalmas védett mobil kommunikációs rendszer hazai jogszabályi környezetbe illeszkedő bevezetésének lehetőségei (gondolatkísérlet)

Ha a külföldi minősített adatok továbbítására alkalmas védett mobilkommunikációs eszközök nemzetközi tapasztalatait elemezzük, arra a következtetésre jutunk, hogy számos eszköz és rendszer áll rendelkezésre a kritikus információs infrastruktúrát üzemeltető felhasználók igényeinek kielégítésére. Ezt a későbbiekben igazolom néhány NATO és EU tanúsítvánnyal is rendelkező „encrypted phone” bemutatásával(GoldLock 3G, SecuVOICE, SecuGATE, Silentel SecureCall, TigerXS,). De a hazai piacon is találhatóak hasonló fejlesztési irányok, (NETIPHONE) amelyek ígéretes nemzeti megoldásokat jelenthetnek.

Gondolatkísérletünk első fázisa az, hogy a nemzeti minősített adatok (szóbeli információk) továbbításával összefüggésben tisztázzuk azt, hogy mikor is beszélhetünk minősített adatról és milyen feltételek teljesülése esetén beszélünk nemzeti minősített adatról.

A mavtv. [1] 3.§ (1) bekezdés a) pontja szerint „ nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn

belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;"

A fenti szakaszban megfogalmazottakkal összefüggésben – azon túl, hogy a „formai követelményeknek megfelelően tartalmazó olyan adat" szóhasználat zavaróan hat (és talán nem is helyes). Elgondolkodtató az, hogy ha a fenti szakasz értelmében a formai követelményeknek megfelelő és minősítési eljáráson keresztül esett adat minősül minősített adatnak, akkor a – nem tárgyiasult formában – egy adott „Bizalmas!" minősítési szint fölötti adathoz kapcsolódóan szóban elhangzott (de nyilvánvalóan a formai követelményeknek nem megfelelő és minősítési eljáráson keresztül nem esett), mobilkommunikációs, vagy stacioner eszközön, illetve rendszeren továbbított szóbeli információ milyen elbírálás alá esik. Ugyanis, különösen a „Bizalmas!" minősítési szint fölött szigorú feltételeknek megfelelően magas szintű személyi, adminisztratív, fizikai és elektronikai védelmi intézkedéseket kell kötelező érvényűen alkalmazni, és ha ez a terület szabályozatlan a minősített adatok védelmével összefüggő (jól felépített) komplex védelmi rendszer egyenszilárdsága csökkenhet.

Egyetértve és elfogadva a nemzetközi törvényekből is eredő (magas szintű egyenszilárdságot biztosító) hazai szabályozással is koherens követelményrendszert, a felhasználói igényeknek megfelelő védett mobilkommunikációs rendszerek szakszerű és jogszerű üzemeltethetősége érdekében is szükségesnek mondható a „nem tárgyiasult formában" szóban elhangzó és elektronikus rendszereken továbbított minősített adatok megjelenítése a hazai szabályozásban.

Gondolatkísérletünk következő fázisa az, hogy a hazai (nemzeti) minősített adatok továbbítására alkalmas elektronikus rendszerek használatbavétele és használata során nem kerülhetjük meg azt az Mavtv. végrehajtási rendeletében [8] 42.§ (3)-(5) bekezdésében megfogalmazottakat, miszerint:

„(3) A rejtjeltevékenységet folytató szerv rejtjeltevékenysége során csak olyan rejtjelző eszközt alkalmazhat, amelyre vonatkozóan az NBF rendszerengedélyt adott ki.

(4) Nemzeti minősített adat rejtjelzésére csak olyan rejtjelző eszköz alkalmazható, amelynek fejlesztője, illetve gyártója rendelkezik a minősített adat kezeléséhez szükséges, jogszabályban meghatározott személyi és tárgyi feltételekkel, és amely szerv esetében az NBF a rejtjelző eszközre vonatkozóan – a létrehozására vonatkozó döntéstől a tervezést,

a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást is érintően, a rendszer egyes elemeinek vagy egészének a kivonásáig és megsemmisítéséig – megbízhatóan meggyőződött arról, hogy nem áll fenn a bizalmasság elve sérülésének veszélye.

(5) Nemzeti minősített adat rejtjelzésére külföldi eszköz csak akkor alkalmazható, amennyiben a (4) bekezdésben meghatározott rejtjelző eszköz nem áll rendelkezésre, vagy a katonai műszaki követelmények nem teszik lehetővé külön nemzeti és külföldi rejtjelző eszköz együttes alkalmazását katonai műveletekben."

A fentiekben megfogalmazott követelmények a szakértő olvasó számára többé -kevésbé egyértelmű szabályokat fogalmaz meg, melynek lényege (kissé leegyszerűsítve) az alábbiakban összefoglalásra is kerül. Ugyanakkor a rendelet értelmezését követően arra a következtetésre is juthatunk, hogy nemzeti minősített adat továbbítására külföldi eszközt is igénybe lehet venni [42 § (5)]. A kutató számára bizonytalanul megválaszolható „nyitott kérdés" marad az, hogy vajon ebben az esetben - amennyiben a (4) bekezdésben meghatározott eszköz nem áll rendelkezésre – milyen szabályokra kell figyelemmel lenni a külföldi rejtjelző eszköz nemzeti minősített adat továbbítására való használatbavételét illetően.

- Hazai nemzeti minősített adat továbbítására csak hazai rejtjelző eszköz használható (és külföldi rejtjelző eszköz csak akkor használható ha hazai eszköz nem áll rendelkezésre). Ebből az következik, hogy „általában" minősített adatot rejtjelző eszközzel kell továbbítani, ami rejtjelzésnek minősül és a rejtjeltevékenységgel összefüggő előírásokat kell alkalmazni.
- Rejtjelző eszközök rendszeresítési engedélyezését a Nemzeti Biztonsági Felügyelet (mint hatóság) végzi. Minősített adat továbbítására alkalmas rejtjelző eszközt az NBF engedélye nélkül nem lehet fejleszteni és használni.
- Rejtjelző eszközt fejleszteni csak Telephely Biztonsági Tanúsítvánnyal rendelkező, többségi magyar tulajdonban lévő gazdasági társaság végezhet [3].
- Az NBF-et a rejtjelző eszköz engedélyezésének teljes életciklusába be kell vonni. Ez azt jelenti, hogy a fejlesztés megkezdését megelőzően a fejlesztő kérelemmel fordul az NBF felé, az NBF rendelkezésére bocsájtja a fejlesztési célt megfogalmazó műszaki dokumentációt, majd ezt követően a szabályoknak megfelelően rendszeresítési engedély kérelemmel fordul az NBF felé aki közigazgatási eljárás keretében a fejlesztési ciklus befejezését követően rendszeresítési engedély ad ki. A fentieket még akkor is alkalmazni kell, ha esetlegesen külföldi eszköz használatbavételéről beszélünk.
- A rendszeresítési engedély csak a rejtjelző eszköz jogszerű használhatóságát teszi lehetővé Ennek birtokában a fejlesztő a hazai piacon forgalomba hozhatja a rejtjelző eszközt. Az üzemeltető szervezet ezen túl egy rendszerengedélyeztetési (akkreditációs) folyamat keretében (a megfelelő tartalommal) rendszerengedély kérelmet kell előterjeszteni az NBF részére, aki a kérelem elbírálását követően közigazgatási eljárás keretében hatósági rendszerengedély ad ki.

Összefoglalva: Adott minősítési szintnek megfelelő minősített adat továbbítására alkalmas nemzeti védett mobilkommunikációs eszköz fejlesztőjének (a nemzeti hatósággal szorosan együttműködve) rendszeresítési eljárás keretében rendszerengedélyt kell beszerezni az adott rejtjelző eszközre. Majd ezt követően a védett mobilkommunikációs rendszer üzemeltetője rendszerengedélyeztetési eljárás keretében rendszerengedélyt kér és kap a nemzeti hatóságtól (NBF). A fenti két közigazgatási eljárás lebonyolítását – annak eredményességét – lényegesen meghatározza az alkalmazni kívánt minősítési szint, ezért ennek megfontolása (a védelmi intézkedések költségeit is figyelembe véve) a projekt sikerét, vagy bukását alapvetően meghatározza. Ezért is fontos egy feltételezett célprojekt végrehajtása esetén az irányadó információvédelmi szakemberek által (nem elégszer hangsúlyozott) kockázatelemzés elkészítése és a projektszerű (ahol van projekt szponzor, megfelelő projektszervezet és ehhez rendelkezésre állnak a megfelelő emberi és anyagi erőforrások is) működési keretek közötti kockázatmenedzsment működtetése. Erre jó példát adnak (és természetesen megfelelő szakmai alapokat is jelentenek) a NATO és EU biztonsági szabályzatában megfogalmazódó irányelvek [4],[5] és például a NATO direktívákban részletesen meghatározott kockázatmenedzsment előírásai. Ezt a hazánkban nem gyakran (és nem szívesen alkalmazott) módszertan olyannyira fontos eleme a sikeres projekt végrehajtásának, hogy külön publikáció keretében kutatom és fejtem ki a témával kapcsolatos megállapításaimat.

A mobilkommunikációs eszközök bevezetésének és használatának dilemmái és azok feloldásának lehetőségei a minősített adatok védelmének tükrében.

Az előző fejezetben kifejtett alapállapotban a mobilkommunikációs rendszer fejlesztőjének és üzemeltetőjének, sok költségigényes feltételnek kell megfelelni. Különösen igaz ez abban az esetben, ha a minősítési szint eléri a „Bizalmas!" minősítési szintet, vagy azt meghaladja.

Ma a fejlesztők és az üzemeltetők legnagyobb dilemmája a „Költséghatékony” rendszer fejlesztése és üzemeltetése! Sok esetben a minősített adatot kezelő szervezetek vezetői túlzottan felülbecsülik az alkalmazott védelmi intézkedések anyagi terheit. Irányadó információbiztonsági szakemberek, a megfelelő ismeretek birtokában – ismerve a hazai szabályozás adta lehetőségeket – költséghatékony megoldásokat tudnak prezentálni a minősített adatot kezelő szervezet vezetőjének.

A fenti szempontrendszer alkalmazása mellett a védett mobil kommunikációs rendszer fejlesztésével és üzemeltetésével összefüggésben, szükség szerint az alábbiakra célszerű figyelemmel lenni.

Az előző fejezetben kifejtésre került, hogy minősített adatok továbbítására, általában rejtjelző eszközt kell alkalmazni. Ugyanakkor kiindulhatunk abból is, hogy a Mavtv. végrehajtási rendeletében [8] 2.§ (4)-(5) bekezdéseiben az alábbiak kerültek megfogalmazásra.

„(4) A felhasználó rendszer használata nem minősül rejtjeltevékenységnek, ha a minősített adatok kezelése vagy továbbítása olyan informatikai rendszeren történik, amelyben a rejtjelző eszköz, rejtjelző szoftver vagy rejtjelző eljárás is telepítésre került és a rendszer biztonsági beállítása nem teszi a felhasználó számára lehetővé a rejtjelzés biztonsági beállításainak módosítását vagy a minősített adatok rendszerben történő kezelése vagy továbbítása során

a rendszerben alkalmazott rejtjelzés kiiktatását.

(5) Nemzeti „Korlátozott terjesztésű!” minősítési szintű adatot – ha az elektronikus rendszer magasabb minősítési szintű adat kezelésére vonatkozó rendszerengedéllyel nem rendelkezik és a megvalósítási lehetőségek adottak – rejtjelzéssel védett virtuális magánhálózat útján kell továbbítani. „

A fenti információkat értelmezve a védett mobilkommunikációs rendszer fejlesztőjének és üzemeltetőjének van lehetősége megfontolni a (4) bekezdésben megfogalmazottaknak megfelelő rendszer kifejlesztését és üzemeltetését. Ebben az esetben lehetőség ként merül fel az a megoldás, hogy csak a VPN rendszer szerverparkjának biztonsági területén kell megteremteni a minősítési szintnek megfelelő fizikai és elektronikai biztonsági környezetet, és a végponti eszközök (mobiltelefonok) esetében nem kell kialakítani a fenti biztonsági környezetet. Ez különösen figyelemreméltó gondolatmenet akkor, ha tudjuk, hogy ugyanezen rendelet 28.§ (3) bekezdése szerint „A katonai, nemzetbiztonsági és bűnügyi műveletekben a személyi biztonsági tanúsítvánnyal rendelkező személy folyamatos személyes felügyelete alatt álló rendszer, valamint annak eleme a biztonsági vezető által meghatározott biztonsági intézkedések betartása mellett biztonsági területen kívül is használható.

Ebben az esetben a fenti rendelet kisebb módosításával - a 28.§ (3) bekezdés megfontolt kiterjesztésével - lehetséges megalapozni a minősített adatok beszéd és SMS alapú továbbítására alkalmas mobilkommunikációs rendszer jogszerű alkalmazásának lehetőségét, olyan kritikus infrastruktúrát, vagy kritikus információs infrastruktúrát üzemeltető szervezeteknél, ahol ez igazán indokolt. Amint azt a későbbiekben példákkal is igazolom, a fenti modellnek megfelelő alkalmazások, mind a nemzetközi, mind a hazai piacon elérhetőek.

A fenti feltételek teljesülése esetén lehetőség nyílhat hazai fejlesztők által fejlesztett rendszer rendszerengedélyeztetésére úgy, hogy csak a központi egység esetében kell a minősítési szintnek megfelelő rendszeresítési eljárást lefolytatni és a megfelelő rendszerengedélyt az NBF-től kérelmezni, melyet a hatóság közigazgatási eljárás keretében ad ki. Ha összehasonlító elemzésnek vetjük alá az EU-s és NATO-s szabályozásokat [4], [5] megállapítható hogy a hazai szabályozással ellentétben a „Korlátozott Terjesztésű!„ minősítési szintű minősített adat kezelését nem kötik adminisztratív zónához, csupán annyit írnak elő, hogy meg kell akadályozni az adathoz való illetéktelen hozzáférést (NATO információbiztonsági direktíva). Az EU, NATO szabályozás adminisztratív zónáról azt mondja ki, „hogy az a biztonsági terület körül alakíthatók ki és ott legfeljebb KT minősített

adat kezelhető". Ehhez a rendezőelvhez való igazodás tapasztalható az EU és NATO tagországok esetében amikor a védett mobilkommunikációs nemzeti eszközeiket tanúsítja a saját nemzeti hatóságuk. Ha tehát a nemzetközi szabályokkal összhangban a hazai védett mobilkommunikációs eszközök rendszeresítésének és használatbavételének során ehhez a rendező elvhez módjában állna igazodni a hazai fejlesztőnek, (illetve az üzemeltetőnek) nemzeti „korlátozott Terjesztésű!" minősítési szintig nem lenne akadálya a védett mobilkommunikációs eszközök használatbavételének.

NÉHÁNY KÜLFÖLDI ÉS HAZAI FEJLESZTÉSŰ MOBILKOMMUNIKÁCIÓS RENDSZER BEMUTATÁSA.

Hazai és külföldi fejlesztő és gyártó cégek a mobil hálózatokban folytatott szenzitív információkat tartalmazó kommunikáció védelmére alkalmas számos technológiai megoldást ajánlanak. Az általuk alkalmazott műszaki megoldások közül elsősorban az IP alapú technológiák biztosítanak hosszú távú megoldást.

Annak igazolására, hogy a közelmúltban a nemzetközi kritikus infrastruktúrák szektorain belül – az operatív irányítás támogatása érdekében –előtérbe került a védett mobilkommunikációs (infokommunikációs) eszközök alkalmazása, ennek okán az alábbiakban néhány jellemző technológiai megoldási lehetőség kerül bemutatásra. Ennek keretében célszerűen bemutatásra kerül, hazai fejlesztésű alkalmazott technológia is.

Gold Lock TM PBX Gateway

A fenti izraeli védelmi minisztérium által tanúsított technológia, katonai titkosítási szintű titkosítási algoritmussal biztosít háromrétegű (laptop, Nokia telefon, Android készülék) költséghatékony védelmi lehetőséget VOIP beszélgetésekre, szöveges üzenetek küldésére és fájlátvitelre. A technológia megfelelő védelmet nyújt a celluláris információk elfogása és illetéktelenek általi feldolgozása ellen. Ez által költséghatékony védelmet nyújt magán személyek, állami szervezetek, és katonai és rendvédelmi szervek vezetőinek illetéktelen személyek általi lehallgatását illetően.

1. ábra.

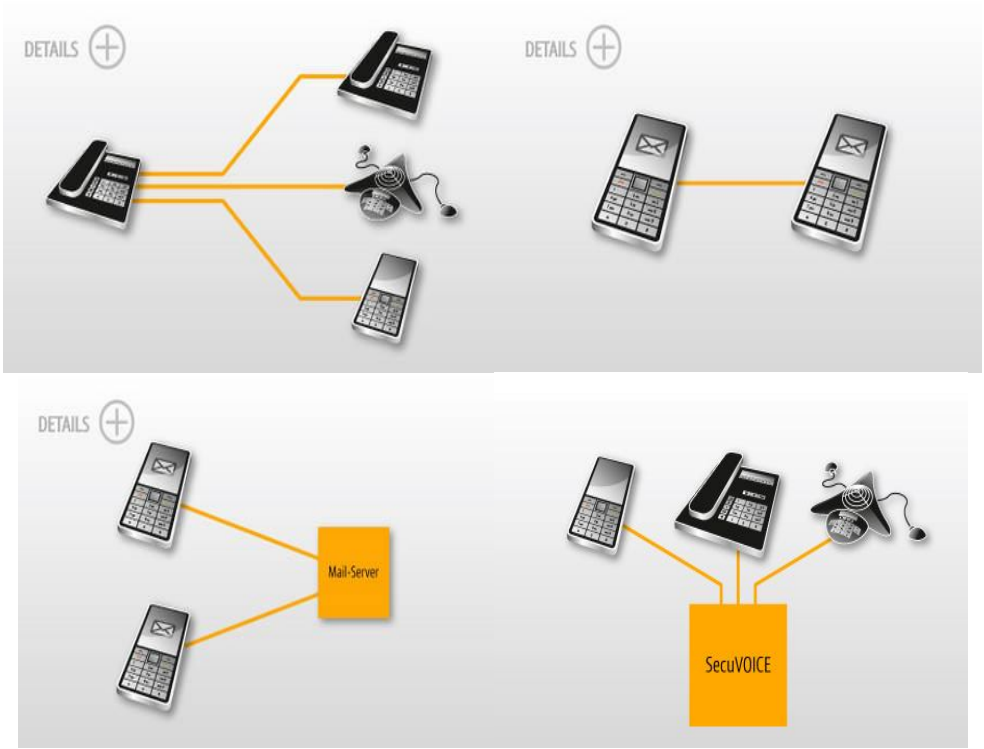
Jellemző tulajdonságok:

- A Gold Lock PBX Gateway-n keresztül egyszerűen kezelhetően végzi el a telefonos kapcsolat biztonságos meghosszabbítását.
- Egy audio jel erősíti meg a biztonságos kapcsolat létrehozását.
- Linux alapú stabil platform
- Jól skálázható, a biztonságos kommunikációt terjeszti ki a mobil eszközök felé.

- Kompatibilis a meglévő digitális alközpontokkal és kihasználja azok előnyeit.
- A rendszerhez egyaránt lehet csatlakoztatni analóg, digitális és IP készülékeket.
- A Gold Lock PBX Gateway kommunikál más Gold Lock PBX Gateway központi egységekkel.
- A Gold Lock PBX Gateway biztonságosan kummunikál 3G adatvonalon, más (Nokia, PC, BlackBery,iPhone) mobil eszközökkel.
- Biztonságos katonai szintű 256 bites (EAS) titkosítási algoritmus használata, megbízható hitelesítés.

Secuvoice [18] NATO KT (Német fejlesztő és gyártó)

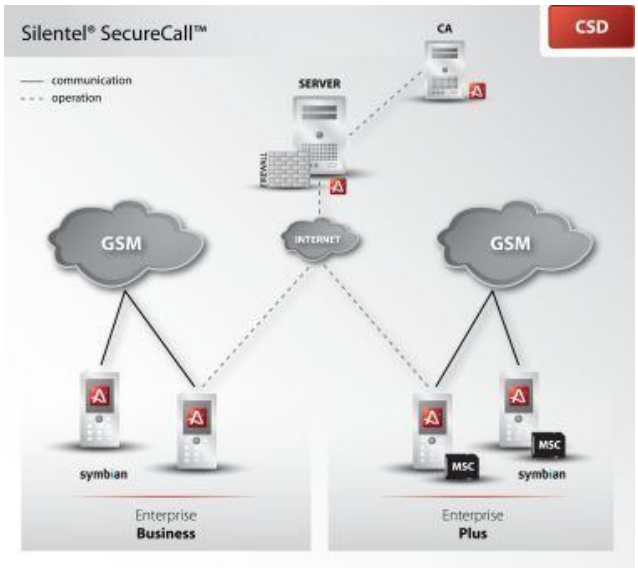
A rendszer jellemzően az egyedi Secusmart biztonsági kártyával biztosítja a hardveres titkosítás megvalósítását, annak minden előnyös tulajdonságát kihasználva. Ebből következően az egyedi azonosítás és a egységes kulcsmenedzsment is biztosított. A SecuSmart biztonsági kártya alkalmazása megfelelő egyenszilárdságú védelmet nyújt a mobil hang és adatátviteli funkciókban egyaránt. A rendszer NATO „Korlátozott Terjesztésű!" minősítési szintű minősített adatok továbbítására hatósági engedéllyel rendelkezik. A SecuSmart kártyát egyszerűen be kell helyezni egy kompatibilis mobiltelefonba. a kártya tartalmaz egy hamisíthatatlan kriptográfiai modult, amely titkosítja (128 bites EAS titkosítás) az adatátviteli útra kerülő (hang, SMS) adatokat. A kártya tartalmaz egy identitást, amelynek segítségével a „végponti eszköz" egyedi azonosítása (tanúsítvány alapú hitelesítése) megtörténik. Ez alapján kizárt a"Man int the Middle" támadás lehetősége. A fentiekből az következik, hogy titkosított kommunikációra azon készülékek képesek, akik rendelkeznek ezzel az identitással. Az alkalmazott hardveres megoldás jellemzően elliptikus kriptográfiai görbét biztosít. A rendszer alkalmas a rugalmas felhasználói igények (mobil-mobil; mobil-ISDN vezetékes; konferencia; SMS) kielégítésére.



2. ábra

Silentel SecureCall [19]

A Silentel SecureCall egy olyan megoldás, amely a dedikált kommunikációs résztvevők részére biztosít mobilkommunikációs lehetőséget. A rendszer architektúráját illetően alapvetően két változatban került forgalomba. Az „üzleti „és a „kormányzati változat között alapvető különbség, hogy az üzleti változat tisztán szoftveres titkosítást végez és a titkosító szoftver e mobiltelefon memóriájára van installálva, addig a kormányzati változat a titkosító szoftverből és egy Mobile Security micro SD (MSC) kriptográfiai chipből épül fel, amelyen egy belső titkosítási algoritmus fut (hardveres kulcsgenerátor és titkosító). A szlovák Nemzeti Biztonsági Felügyelet (Národný Bezpečnostný Úrad) által szlovák nemzeti „Bizalmas!" legmagasabb minősítési szintre tanúsított Silentel SecureCall Plus rendszert használják minősített adatok mobilkommunikációjának megvalósítására a szlovák kormányzati szervek. A „NATO Bizalmas!" szintre történő akkreditációja jelenleg folyamatban van.



3. ábra

A megoldás előnye, hogy könnyű és relatívan olcsó a bevezetése és üzemeltetése. A rendszer architektúrája lehetővé teszi kommunikációs végpontként Android, Symbian, Windows Mobile/Windows Phone, Windows platformú eszközök (smartphone, PDA, Tablet PC, számítógép) együttes alkalmazhatóságát. Lehetőséget teremt arra is, hogy mobil eszközökről titkosított adatátvitellel elérhetők legyenek központi adatbázisok szolgáltatásai (pl. térinformatikai rendszer). Silentel rendszer GSM hálózat áramkörkapcsolt adatátvitel (CSD) technológia alkalmazása helyett standard IP protokoll alapúan is kialakítható, ez esetben egy rendszerben alkalmazhatók WiFi-s, WiMax-os, műholdas, vezetékes végpontok, a különböző Silentel rendszerek összekapcsolhatók.

A fentiekben kifejtett kétségtelen előnyös tulajdonságok miatt rendkívül figyelemreméltó megoldásnak tekinthető a Silentel SecureCall kormányzati és katonai verziója is, amely mindenképpen további részletes tanulmányozást érdemelne és talán ezt követően költséghatékony, felhasználóbarát és megfelelően egyenszilárd megoldás bontakozhat ki a hazai információbiztonsági szakemberek számára.

Sectra [19] (Holland fejlesztő és gyártó NATO, EU Titkos)

4. ábra. Sectra TigerX készülék és asztali kiegészítő terminálja (Tiger XS Office)

A Tiger XS rendszerről a NATO katonai bizottsága tanúsítványt állított ki, amelyben igazolta, hogy a rendszer lehallgatás mentes biztonságos kommunikáció lefolytatására alkalmas „NATO Titkos!" Minősítési szintig. Ugyanezt a rendszert a közelmúltban az EU-ban is tanúsították"EU Titkos!" minősítési szintig. Ebből következik, hogy az eszköz jelen pillanatban kettős tanúsítással rendelkezik (NATA; EU), ezért egyedülálló helyzetben van az európai piacon. A fentiekből következik, hogy a szövetségi rendszeren és az Európai Unión belül lehetőség nyílt a minősített adatok mobilkommunikációjára „Titkos!" minősítési szintig. A rendszer alapvető jellemzője, hogy ugyanazon eszköz egyaránt lehetőséget biztosít a védett vezetékes és mobilkommunikáció megvalósítására. A NATO tagországok katonai vezetőinek és az EU 27 tagországának döntéshozóinak több mint fele rendelkezik a rendszer által biztosított minősített adatok mobilkommunikációs lehetőségével. A rendszer fő funkciója a beszédkommunikáció védelme, de lehetőséget biztosít védett SMS, Fax továbbítására és egyéb adatátviteli lehetőségegek is támogat.

A Sectra Tiger XS személyi titkosító eszközt (n. számú ábra) alkalmazásához felhasználójának bluetooth-szal kell csatlakoztatnia mobil készülékhez, vagy behelyeznie a vezetékes vonalra csatlakoztatott terminájába (Tiger XS Office), az azonosítás kártyával és kóddal történik, ezután a Tiger XS készülékről fogadható, vagy kezdeményezhető a hívás. A rendszer kiépítésétől függően alkalmazhat offline és online kulcsmenedzsmentet, míg előbbinél a kiosztott kulcsokat manuálisan kell telepíteni és időszakosan frissíteni a készüléken, addig online kulcsmenedzsment esetén ezek a hálózaton levő készülékeken automatikusan frissülnek.

5. ábra. Sectra Tiger biztonságos mobiltelefon

A Sectra új fejlesztése [23] a Tiger biztonságos mobiltelefon (n. sz. ábra), mely a Sectra Tiger XS technológiáján alapul. A készüléket úgy tervezték, hogy az mindenhol használható

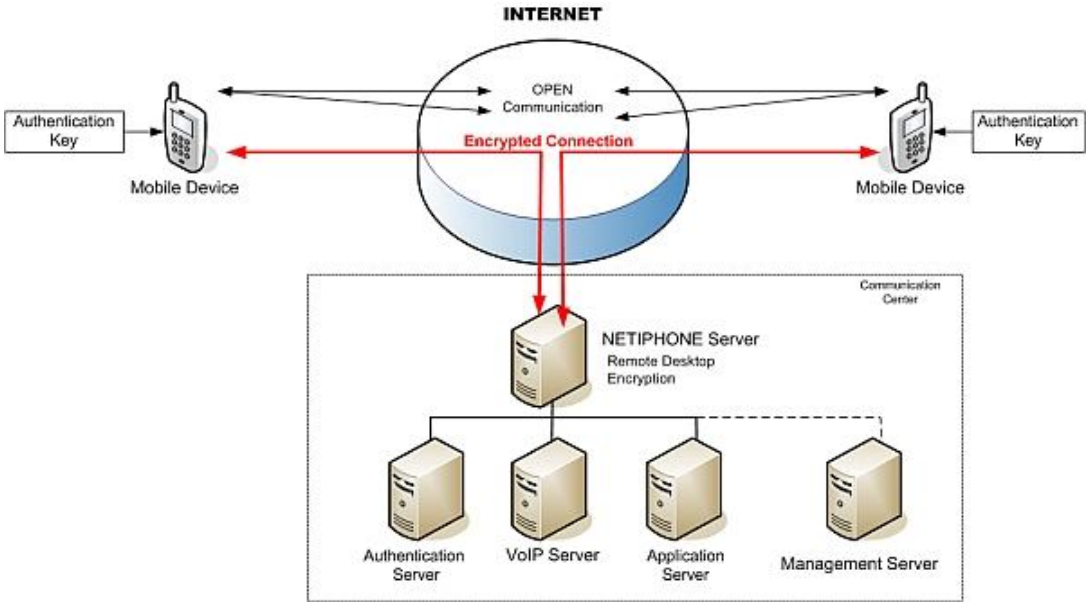
legyen, cellás és műholdas mobilhálózaton egyaránt alkalmazható (GSM, 3G, Iridium, Inmarsat, Thuraya). A készülék kompatibilis a Tiger XS készülékkel és a Tiger XS Office kiegészítő modullal. A svéd-holland fejlesztésű terméknek jelenleg folyamatban van a svéd és holland nemzeti „Titkos!" minősítési szintre történő engedélyezési eljárása, melyet követően EU és NATO „Titkos!" szintre kívánják tanúsítatni.

NETIPHONE [21]

Az állami szervezetek, és a gazdasági társaságok felhasználói részéről igény mutatkozik a belső, bizalmas információkat tartalmazó, publikus hálózatokat használó kommunikációs csatornák – legyen az hang, multimédiás vagy adatkommunikáció – titkosítására. A kommunikációs lehetőségeken túl cél a központi alkalmazások, illetve a levelezés elérése is Mindezt úgy kell megvalósítani, hogy a lehető legkevesebb információ hagyja el a biztonsági területet és az adatok ne kerüljenek tárolásra a külső, nem biztonsági területen elhelyezkedő felhasználói terminálokon. Amint azt a fentiekben láthattuk, az igényeket részben és egészében kielégítő software komponensek már léteznek a piacon. A NETIPHONE™ viszont, amely teljes egészében magyar fejlesztés, tartalmazza a fent említett összes szolgáltatást. Mindemellett felhasználóbarát, könnyen kezelhető és számtalan kényelmi funkcióval ellátott megoldás, amely a titkosított kommunikációt ugyanolyan egyszerűvé teszi, mint a hétköznapi mobiltelefon használatot.

A rendszer felépítése

A NETIPHONE™ alkalmazás a mobil készülékek és a központi NETIPHONE™ szerver között létrehozott titkosított adatcsatornán biztosít megbízható kommunikációt, a nyilvános mobil adathálózatot használva. A hangkommunikációt a központi oldalon található VoIP központ alkalmazás biztosítja a hálózathoz csatlakozó terminálok között. Ezen felül a rendszer lehetőséget nyújt elektronikus levelezésre, illetve központi szolgáltatások használatára is, mint például fájlok küldése és fogadása. Lehetőség van a titkosított csatornán keresztül folytatott kommunikáció központi megfigyelésére, illetve a használat és a működés, rendszer logok alapján történő felügyeletére.



6. ábra.

A rendszer szolgáltatásai:

- Központi alkalmazások távoli desktop-on keresztüli elérése
- Titkosított hangkommunikáció
- Automatikus SMS alapú híváskezdeményező értesítés, a rendszerhez pillanatnyilag nem csatlakozó hívott fél irányába
- Központilag tárolt Telefonkönyv
- Központilag tárolt Hívásnapló a nem fogadott, fogadott, indított hívásokról
- Rendszerüzenetek nem fogadott hívásról, illetve új e-mail beérkezéséről

Biztonság:

- Központilag tárolt érzékeny információk. A kliensen tárolt azonosító adatok védelme jelszóval
- AES 256 bites titkosítás használata
- Szeparált külső és belső hangkommunikáció – nyílt hálózat alkalmazásakor blokkolt titkosított hangkommunikáció funkciók
- A kulcs és beállítási információk jelszavas védelme a készülékben
- Központilag futtatott applikációk, a felhasznált adatok kizárólag központban történő tárolása

Menedzselhetőség, megfigyelhetőség:

- A rendszerkomponensek hibaeseményeinek naplózása
- A kommunikációs események naplózása
- A rendszerben folytatott kommunikációk rögzítése és tárolása, visszakereshetőségük biztosítása
- A rendszerkomponensek központi menedzselhetősége, konfigurálhatósága

A NETIPHONE rendszer előnye, hogy kliens oldalon nem igényel speciális eszközt, a titkosítást megvalósító kliensalkalmazása minden Symbian S60 platformú mobiltelefonra telepíthető. Használatához csomagkapcsolt adatátviteli (GRPS, EDGE, 3G/HSDPA) mobilszolgáltatás szükséges. A készüléket egy hónapig módomban állt tesztelni, tapasztalataim azt mutatják, hogy 3G adatkapcsolat esetén a készülék jól használható, ugyanakkor jelenleg ez még az ország területének nagyobbik részén ez még nem elérhető, 2G adatkapcsolat esetén a beszédhang gyakran volt szakadozott, késleltetett, a problémás helyeken a hagyományos GSM hívások minősége lényegesen jobb volt.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A Mav. végrehajtási rendeleteinek (90/2010. Korm. rendelet és a 161/2010. Korm. rendelet) KT minősített adat kezelését illető rendelkezései nincsenek teljesen összhangban az EU-s és NATO-s szabályozással, ugyanis az utóbbiak nem kötik adminisztratív zónához a KT minősített adatok kezelését. Ugyanakkor a hazai jogi szabályozás katonai, nemzetbiztonsági és bűnügyi műveletekben biztonsági területen kívül is a megfelelő szabályok mellett akár nemzeti SZT minősített adat kezelését is biztosítják, melyet viszont a NATO és EU szabályozás nem enged meg. (Megj: biztonsági terület jármű belsejében is kialakítható). Ahhoz hogy védett mobilkommunikációs rendszereken legalább nemzeti KT minősített

adatokat lehessen kezelni, szükséges hogy azt az EU-s és NATO-s szabályozással összhangban a hazai szabályozás is lehetővé tegye.

Széleskörű (hazai) kormányzati és államigazgatási felhasználásra a nemzeti KT minősítési szint megcélzása a célszerű, személyi, fizikai, adminisztratív, elektronikai biztonsági szempontból a biztonság és a felhasználhatóság, egyenszilárdság (személyek köre, felhasználás helyei, ár-érték) közt „optimális középút „megválasztása mellett.

A NETIPHONE mint hazai kezdeményezés ígéretesnek tűnik, de a megfelelő lefedettség biztosítása mellett a továbbfejlesztésére lenne szükség, melyhez a szlovák fejlesztésű SecureCall szolgáltatja a legjobb követendő mintákat. A legprofesszionálisabb megoldás kétségtelenül a SECTRA, ennek viszont hátránya az egyedi készülékek magas ára lehet.

Az ideális nemzeti védett mobilkommunikációs rendszer paraméterei:

- hazai fejlesztésű (jogszabályok, nemzetbiztonság)
- mobilhálózaton áramkörkapcsolt (GSM hívás) és csomagkapcsolt (GPRS, EDGE, 3G/HSDPA) adatátviteli módban is alkalmazható
- kereskedelmi forgalomban kapható mobilkészülékkel alkalmazható
- készülékei MicroSD formátumú hardveres titkosító kártyát alkalmaznak, GPS modult tartalmaznak
- PKI alapú authentikációt és titkosítást alkalmaz
- Végpont-végpont közti titkosított adatcsatornát alkalmaz
- Tanúsítványok online kezelését biztosítja (központi tanúsítvány szerverrel)
- központi adatbázisokkal alkalmazható (pl. katasztrófavédelmi, rendvédelmi)
- TETRA állomásokkal tud kommunikálni
- + műholdas mobilkészülékekkel is alkalmazható

Az EU-s és NATO viszonylatban a minősített adatok védett mobilkommunikációval történő kezelése, egyértelműen a SECTRA megoldása az egyetlen szóba jöhető lehetőség.

Felhasznált irodalom

[1] A minősített adat védelméről szóló 2009 évi CLV. törvény

[2] A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet. (58.§ (1),(2))

[3] A telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet.

[4] C-M (2002) 49 A NATO Biztonsági szabályzata

[5] A Tanács 2001. március 19-i 2001/264/EK határozata a Tanács Biztonsági szabályzatának elfogadásáról.

[6] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV törvény.

[7] Az államtitkot, vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdekeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. (IV.29.) Korm. rendelet.

[8] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet. 49§-51§

[9] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; A mellék-let, A 8.1- A 8.3. p.

[10] MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002), 8.1 – 8-3. p.

[11] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, p. 76-87.

[12] ISO/IEC 20000-1 Information technology – Service management - Part 1: Specification; 3.3. p. és 6.6. p.

[13] Kassai Károly Az elektronikus adatkezelés során szükséges személyi biztonság kérdései.(Hadtudományi Szemle 3. évfolyam 3. szám 2010. 1. oldal)

[14] A Nemzeti Biztonsági Felügyelet elnökének (NBF bemutatása biztonsági vezetőknek.ppt 2010.11.12) előadása.

[15] 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (49.§, 55.§, 55.§6A, 116.§, 137.§/A, 189.§)

[16] Az 1959. évi IV. törvény a polgári törvénykönyvről (81.§ (2)-(3) bekezdései)

[17] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

[18] http://www.secusmart.com/home.html (2011.05.10)

[19] http://www.ia.nato.int/niapc/category/mobile-communications_51 (2011.05.10)

[20] http://www.sectra.com/global/news/press_releases/security/2009-2010/pdf/Sectra%20Panthon.pdf (2011. 05.10.)

[21] http://www.neti.com/products/neti-phone (2011. 05.10.)

[22] http://www.ardaco.com/downloads/doc/SGDIS_leaflet.pdf (2011.05.20)

[23] http://www.sectra.nl/Data/Sites/1/Sectra%20Folders/Tiger%207401%20101101.pdf (2011.05.20.)

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Horvayné Fehér Judit
feherjenator@gmail.com

Munk Sándor
munk.sandor@zmne.hu

A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT FOGALMA, RENDELTETÉSE

Absztrakt

A korszerű informatika szolgáltatásait napjainkban már egyetlen alkalmazási terület, így a rendőri alkalmazás sem nélkülözheti. Napjaink informatikája a hálózati megoldások informatikája, amely a különböző informatikai eszközök, rendszerek, alkalmazások összekapcsolódására, egymás szolgáltatásainak igénybevételére, egymás képességeit kölcsönösen erősítő együttműködésére épül. Az informatikai hálózatok által nyújtott előnyök hátrányokkal, biztonsági kockázatokkal is párosulnak. A hálózatokhoz kapcsolódó fogalmak és értelmezéseik heterogenitása akadályát képezi az eredményes tudományos-szakmai tevékenységnek, a hálózatok biztonsága kutatásának. Jelen publikáció összegzi a hálózatok alapfogalmait; bemutatja az informatikai hálózathoz kapcsolódó fogalmak alkalmazását a rendőrségi szakmai dokumentumokban; végül összeveti a különböző értelmezéseket és megfogalmaz egy javasolt fogalmat és értelmezést.

In our days none of the application areas, including police applications can neglect modern IT services. Today's informatics is informatics of network solutions, that is built on interconnection of various IT devices, systems, and applications, use of services of each other, and their cooperation mutually reinforcing each other's capabilities. Benefits of IT networks are coupled with disadvantages, security risks too. Heterogeneity in network related concepts and their interpretations are an obstacle to effective scientific-technical activities, and network security research. Recent publication summarizes the conceptual basics of networks; presents the use of IT network concepts in police documents; and finally compares the different interpretations, and lays down a suggested police IT network concept, and interpretation.

***Kulcsszavak**: fogalmi alapok, informatikai hálózatok, rendőrségi informatikai hálózat ~ conceptual basics, IT networks, police IT network.*

BEVEZETÉS

A korszerű informatika szolgáltatásait napjainkban már egyetlen alkalmazási terület sem nélkülözheti. Nincs ez másként a rendőri területen sem, az eredményes és hatékony bűnügyi, közrendvédelmi, határrendészeti, közlekedés- és igazgatásrendészeti tevékenység egyre növekvő jelentőségű feltételrendszerét képezik az informatika által nyújtott szolgáltatások. Informatikai eszközök, rendszerek, alkalmazások támogatják többek között a szervezeten belüli általános információáramlást; a Rendőrség által is használt nyilvántartások kezelését; valamint az egyes szaktevékenységeket (bűnügyi vizsgálatok, okmányellenőrzés, közterület-megfigyelés, határellenőrzés, stb.).

Napjaink informatikája már a hálózati megoldások informatikája, amely a különböző informatikai eszközök, rendszerek, alkalmazások összekapcsolódására, egymás szolgáltatásainak igénybevételére, egymás képességeit kölcsönösen erősítő együttműködésére épül. Hálózati lehetőségek nélkül az informatikai szolgáltatások jelentős része egyáltalán nem, vagy csak korlátozottan, szűkített funkciókészlettel működőképes. Hálózati megoldásokra épül többek között a Rendőrség Robotzsaru ügykezelő rendszere, a HERMON körözési információs rendszer, a HIDRA idegenrendészeti alkalmazás, az AFIS ujj- és tenyérlenyomat azonosító rendszer, a NEKOR okmány-minta nyilvántartó rendszer, vagy a HERR határellenőrzési rendszer és a SIS schengeni információs rendszer.

Az informatikai hálózatok által nyújtott előnyök, mint az életben minden lehetőség, hátrányokkal is párosulnak. A hálózatok lényegi sajátosságai önmagában; az önálló (sok esetben külső) szolgáltatásként megjelenő globális és nagykiterjedésű hálózatok kialakulása; ezen keresztül az informatikai rendszerekhez történő hozzáférés könnyebbé válása jelentős és újszerű sebezhetőségeket, biztonsági kockázatokat hordoz magában. Napjainkra a hálózatok biztonsága, a hálózati biztonság az informatikai biztonság lényeges összetevőjévé, jelentős szakterületévé vált, ami természetszerűleg érvényes a rendőri alkalmazásra is.

A szakirodalom és a szakmai dokumentumok tanulmányozása azt mutatja, hogy az informatikai eszközöket, rendszereket összekapcsoló hálózatok fogalmi alapjaival kapcsolatban a szakmai, szakértői körökben még sem általában, sem a rendőri szakterületen nem alakult ki egyetértés, egységesen elfogadott értelmezés. Egymás mellett találkozhatunk az informatikai hálózatok, számítógép-hálózatok, távközlési hálózatok, kommunikációs hálózatok, infokommunikációs hálózatok kifejezésekkel, sok esetben a tartalmat leíró meghatározások nélkül. Ez a terminológiai sokféleség akadályát képezi az eredményes tudományos-szakmai tevékenységnek; a kutatók, szakemberek együttműködésének.

A fentiek alapján jelen publikáció alapvető célja, hogy egységes hálózati fogalmi alapot alakítson ki, határozzon meg a rendőrségi informatikai hálózat biztonsági kérdései vizsgálatához. Ennek érdekében:

- összegzi az informatikai hálózatok alapvető fogalmait;
- bemutatja a kapcsolódó hálózat fogalmakat, kifejezéseket a rendőrségi szakmai dokumentumokban és megfogalmazza a rendőrségi informatikai hálózat javasolt fogalmát, rendeltetését.

INFORMATIKAI HÁLÓZATOK FOGALMI ALAPJAI

Az informatikai hálózat fogalom értelmezésének, tartalmának vizsgálata során kiindulásképpen megfogalmazható az a széles körben – bármely nézőpont, megközelítés mellett – elfogadható általános megállapítás, hogy az informatikai hálózat olyan technikai (valós, működő) hálózat, amelynek rendeltetése információs szolgáltatások nyújtása, információs tevékenységek támogatása, megvalósítása, és amelynek elemei technikai

eszközök (rendszerek), az elemek között pedig információcserét biztosító valós fizikai, vagy absztrakt logikai kapcsolatok állnak fent.

A fenti általános körülhatároláson belül az informatikai hálózat fogalom tartalmát és ezzel egy időben a különböző megközelítések, értelmezések közötti eltéréseket legmagasabb szinten az határozza meg, hogy van-e és milyen szűkítés a hálózat rendeltetésében (vagyis hogy a hálózat milyen szolgáltatásokat nyújt, milyen tevékenységeket támogat), illetve van-e és milyen szűkítés a hálózatot alkotó eszközökre, vagy az információcsere során alkalmazott megoldásokra vonatkozóan.

Az *információs szolgáltatásokat nyújtó technikai hálózatok* témaköréhez kapcsolódóan számos különböző általános tartalmú kifejezéssel találkozhatunk, amelyek között kiemelt szerepet töltenek be a következőek: távközlési hálózatok, műsorszóró hálózatok[1] és számítógép-hálózatok. Ezek közül a gyakorlatban elsőként az információtovábbítást támogató távközlési, illetve műsorszóró hálózatok jelentek meg, a későbbiekben alakultak ki az információcsere mellett a feldolgozási és tároló-képességek megosztását, összekapcsolását támogató számítógép-hálózatok is, napjainkban pedig már a különböző információs szolgáltatásokat nyújtó hálózatok integrálódásának korszakát éljük. A fenti fogalmakhoz a különböző szakmai dokumentumokban különböző meghatározások tartoznak.

A *távközlési* (távközlő, kommunikációs, híradó) *hálózatok*[2] különböző meghatározásainak alapvető összetevője, hogy alaprendeltetésük információk eltérő helyek közötti átvitele. A továbbított információk formája (beszéd, hang, írott szöveg, álló és mozgókép, adat, technológiai folyamatok vezérlő jelei, stb.) alapján különböztethetőek meg a hálózatok által nyújtott távközlési szolgáltatások.

Kezdetben az egyes (pld. távíró, távbeszélő) távközlési hálózatok egy konkrét szolgáltatást nyújtottak, a végberendezések és az ezeket hálózatba kapcsoló vonalak, kapcsolóelemek szorosan egymáshoz tartoztak. A későbbiekben olyan távközlési (pld. géptávíró/telex, fax) hálózatok jelentek meg, amelyekhez már nem tartozott önálló technikai hálózati megoldás, az információk továbbítását megfelelő átalakítások után más létező (elsősorban a távbeszélő) hálózatok biztosították. A modemes átalakítás segítségével a hagyományos távközlési (távbeszélő) hálózatok egy meghatározott átviteli sebességig adatátviteli szolgáltatásra is alkalmassá váltak. Végül megjelentek a tervezetten több szolgáltatást nyújtó (pld. ISDN) távközlési hálózatok is. A távközlési szakterületen így az idők során fokozatosan szétváltak a végfelhasználói (előfizetői) és a hálózati (hordozó) szolgáltatások.

A *számítógép-hálózatok*[3] alaprendeltetése nem elsősorban az információtovábbítás, információcsere, ez valójában csak egy szükséges feltétel az azonos, vagy hasonló információs képességeket, szolgáltatásokat nyújtó eszközök összekapcsolásához, az összetevők képességeinek egyszerű összegzését meghaladó, magasabb szintű, vagy akár új képességek kialakításához: különböző információs (rész)képességekkel rendelkező eszközökből meghatározott információs szolgáltatásokat nyújtó, egységes egészként működő – elosztott architektúrájú – eszközrendszerek felépítéséhez.

A számítógép-hálózatok meghatározásának alapja lehetne, hogy számítógépeket kapcsolnak össze. Ez azonban az egyes definíciók, értelmezések szerint ma már nem ilyen egyértelmű. Egyes meghatározások számítógépeket (vagy autonóm számítógépeket) tartalmaznak, mások számítógépeket és más eszközöket említenek, végül a harmadik csoport definícióiban adatfeldolgozó rendszerek, eszközök szerepelnek. A legszűkebb értelmezés esetében tehát a hálózat kizárólag (általános célú) számítógépekből állhat, a legtágabb értelemben pedig csomópontjai lehetnek bármilyen, adatfeldolgozási képességgel rendelkező eszközök.

[1] Ezek részletesebb vizsgálatáról jelen publikáció célkitűzései figyelembevételével eltekintünk.
[2] Telecommunication[s] network.
[3] Computer network.

A fenti értelmezési kérdéseket csak tovább árnyalja a számítógép fogalmának tartalma, amely alatt sokan a mindenki által használt általános célú számítógépeket értenek, pedig a fogalom meghatározásai (amelyek lényege: automatizált adatfeldolgozó eszköz) ennél sokkal tágabb körre kiterjedő értelmezést írnak le: magukban foglalják például a célszámítógépeket is. Ráadásul napjainkban már olyan, információs tevékenységeket támogató, integrált funkciójú technikai eszközök jelentek meg (okostelefonok, GPS-készülékek, médialejátszók, stb.), amelyek csoportjának általános megnevezésére az informatikai eszköz kifejezés kínálkozik.

A híradástechnikai, távközlési, illetve a számítástechnikai, szűkebb értelemben vett informatikai *szakterületek, megoldások, eszközök konvergenciája, integrációja* egyre kevésbé teszi lehetővé a távközlési és a számítógép-hálózatok megkülönböztetését. Bár ez a megkülönböztetés a két szakterületen még létezik (az előbbi a számítógép-hálózatokat egy speciális típusnak, távközlő adathálózatnak tekinti, az utóbbi pedig a távközlési hálózatokat a számítógép-hálózatok fizikai összeköttetést megvalósító részeként kezeli), de alapjául már csak az egyes hálózatok eredete, kialakulása szerepel és egyes típusok esetében meg is fogalmazódik, hogy a besorolás szubjektív. A két hálózat-típus összefoglaló fogalmára, illetve az integrálódott hálózat-típus megnevezésére a BME távközlő hálózatok tantárgya az információközlő hálózatok, illetve infokommunikációs hálózatok kifejezéseket használja. [1, 3., 17. o.] Ezek a kifejezések az informatikai szakterületen nem használatosak.

Az *informatikai hálózatok* fogalma szűkebb és tágabb tartalmakkal is értelmezhető. Ezek között a legszűkebb értelmezés: általános célú számítógépek, illetve számítógép-hálózati kapcsolóelemek[4] és a köztük fennálló valós, vagy absztrakt (fizikailag távközlési hálózatok által megvalósított) összeköttetések összessége. Eszerint az értelmezés szerint a hálózat szolgáltatásai közé csak az operációs rendszerek által biztosított képességmegosztó és információcsere szolgáltatások tartoznak. Mindezek csak alapot képeznek a felhasználók számára összetettebb, speciális szolgáltatások megvalósítására (hasonlóképpen ahhoz, ahogy egy számítógép és operációs rendszere csak egy platform az érdemi felhasználói szolgáltatásokat nyújtó alkalmazások számára).

Tágabb értelmezés szerint az informatikai hálózat részét képezik a számítógépeken futó alkalmazások is, amelyek így már speciális (hálózati) szolgáltatásokat nyújtanak felhasználóik számára. A legszűkebb, technikai jellegű értelmezéstől eltérően ez a megközelítés már felhasználói nézőpontú, szolgáltatásközpontú. Egy ilyen értelmezésű informatikai hálózat képes hagyományos távközlési (pld. távbeszélő, videokonferencia, fax, stb.) szolgáltatások nyújtására. Szolgáltatás-alapú megközelítésben tehát nincs ok a (hagyományos) távközlési és (hagyományos) számítógép-hálózatok megkülönböztetésére, ez gyakorlatilag technikai megvalósítási kérdéssé válik, ami a felhasználó számára érdektelen.

A legtágabb értelmezés esetében az informatikai hálózat elemei nem kizárólag számítógépek, hanem bármilyen információs tevékenységet támogató rendeltetésű (tágabb értelemben vett informatikai), vagy egyszerűen csak más rendeltetésű, de információs képességekkel rendelkező (informatizált) technikai eszközök is lehetnek. [2, 17. o.] Eszerint az informatikai hálózatok közé tartoznak többek között a tárolóhálózatok, a térfigyelő rendszerek (hálózatok), a vezetéknélküli szenzorhálózatok, vagy a felügyeleti, irányító és adatgyűjtő rendszerek (hálózatok).

Az informatikai hálózat fogalmának vizsgálata során nem hagyható figyelmen kívül az informatikai rendszer fogalma és nem kerülhető meg a *hálózat és rendszer fogalmak* viszonyának elemzése sem. Sok esetben a szóhasználatban is keveredik a két kifejezés, lényegében azonos tartalomhoz kapcsolódóan találkozhatunk a rendszer és a hálózat kifejezésekkel (pld. távbeszélő rendszer és távbeszélő hálózat), más esetekben viszont a jelzős

[4] Elosztók-erősítők (hub), kapcsolók (switch), útválasztók (router), átjárók (gateway).

kifejezések egyértelműen eltérő tartalmakat jelölnek (pld. felügyeleti irányító és adatgyűjtő rendszer, illetve hálózat).

A következőkben informatikai rendszer alatt eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására (információs szolgáltatások nyújtására) létrehozott (működő, technikai) rendszerét értjük. [3, 21. o.] Az informatikai rendszer fogalmába általában beleértjük a valamilyen szintű formális körülhatárolást és a működési, illetve irányítási, felügyeleti (működtetési, fejlesztési) autonómiát. Ezek a jellemzők különböztetik meg – bár természetesen nem matematikai pontossággal – az egymástól független rendszereket, az alrendszerekből felépülő rendszereket, az egymással tervezetten, szorosabban együttműködő rendszereket (rendszerek rendszere), valamint az egymással dinamikusan változó módon, lazábban együttműködő rendszereket (rendszerek szövetsége).

Az informatikai hálózatok tartalmilag minden tekintetben megfelelnek a rendszerfogalom kritériumainak (működő technikai rendszerek), így elvileg minden informatikai hálózat egyben – egy speciális – informatikai rendszernek is tekinthető. Ennek megfelelően egy informatikai hálózat (mint rendszer) más informatikai rendszerekhez (hálózatokhoz) viszonyítva lehet:

- önálló (autonóm) rendszer;
- egy rendszer viszonylagos önállósággal rendelkező, de annak részét képező alrendszere;
- szolgáltatásokat nyújtó (ehhez esetleg további szolgáltatásokat felhasználó) önálló rendszer;
- szolgáltatások megvalósítása érdekében további rendszerekkel (hálózatokkal) együttműködő. összekapcsolódó rendszer.

Az informatikai hálózat fogalma értelmezhető, sőt értelmezendő egy adott szervezet esetében is. A *szervezet informatikai hálózata* a szervezeten belüli információáramlás támogatásának, a szervezeti informatikai rendszerek, eszközök összekapcsolásának, valamint a szervezet és a környezet informatikai rendszerei, eszközei összekapcsolásának eszköze.

Szervezeti nézőpontból célszerű meghatározni a *szervezet informatikai hálózata és informatikai infrastruktúrája* viszonyát is. Az infrastruktúra tartalmi jellemzői, hogy szolgáltatásai alapvető igényeket elégítenek ki és széles körben, térbelileg kiterjedt módon, illetve időben stabilan férhetők hozzá. [4, 60. o.] Ennek megfelelően a szervezeti informatikai infrastruktúra a szervezet egészének érdekeit szolgáló, többek által közösen használt informatikai erőforrások összessége, amelynek alapvető részét az informatikai rendszer további összetevőit rendszerbe integráló hálózat, a kiszolgáló eszközök nagyobb része, valamint a széles körben felhasználható alkalmazások és adathalmazok (adatállományok, adatbázisok, adattárházak, stb.) képezik [3, 28. o.]

Összességében a továbbiakban – az informatikai biztonsági kérdések által megkövetelt átfogó megközelítés alapján – az informatikai hálózat fogalmát tág értelemben (a számítógép-, távközlési és egyes információs rendeltetésű technikai hálózatokat is magában foglaló módon) használjuk. Vagyis informatikai hálózat alatt olyan információs szolgáltatásokat nyújtó technikai hálózatokat értünk, amelyek csomópontjai információs tevékenységeket támogató eszközök, illetve kapcsolóelemek, amelyeket információcserét biztosító valós fizikai, vagy absztrakt logikai kapcsolatok kötnek össze.

Egy szervezet informatikai hálózata alatt szűkebb értelemben a szervezet informatikai rendszerének részét, a szervezet informatikai infrastruktúrájának alapvető összetevőjét, a hálózat csomópontjait alkotó informatikai eszközöket, valamint a szervezet felügyelete, irányítása alatt álló hálózati kapcsolóelemek és összeköttetések együttesét értjük. Tágabb

értelemben a szervezet informatikai hálózatának részét képezik a külső szolgáltatók által biztosított – részben a szervezet által felügyelt, esetleg virtuális – kapcsolóelemek és összeköttetések is.

A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT ÉRTELMEZÉSE

A 'rendőrség informatikai hálózata' fogalom értelmezéséhez meg kell határozni e kifejezés tartalmát. Az értelmezés egyik alapvető célja a hálózat határainak kijelölése, annak meghatározása, hogy mely összetevők, elemek tartoznak a hálózathoz és melyek nem. A fogalomalkotás, az alkalmazott szakkifejezések tartalmának, értelmezésének vizsgálata nem elsősorban elméleti játék, hanem a szakmai párbeszédet lehetővé tevő és a szakmai tevékenységet alapvetően meghatározó feladat. Amennyiben nem rögzítjük, hogy mit értünk a rendőrség informatikai hálózata alatt, nincs körülhatárolva például az sem, hogy e hálózat fejlesztésének, üzemeltetésének, felügyeletének, vagy védelmének követelményei, feladatai mire terjednek ki.

Fontosnak tarjuk annak hangsúlyozását is, hogy a fogalmi kérdések vizsgálata során nem az alkalmazott kifejezés az elsődleges, hanem a tartalom. A megfogalmazott tartalomhoz különböző megnevezések rendelhetőek, amelyek között érdemben csak a szakterületi-tudományos közösség elfogadott 'szóhasználatai', illetve a kifejezéseknek a szakterületen kívüliek számára 'sugallt' tartalma képezhet célszerűségi különbségeket.

A fogalom értelmezése céljából a következőkben:

- összegezzük a hálózat terjedelemére, határaira vonatkozó alapvető kérdéseket;
- röviden bemutatjuk a Rendőrség hálózatai fejlődését;
- áttekintjük a kapcsolódó hálózatfogalmakat a szakmai dokumentumokban;
- meghatározzuk a rendőrségi informatikai hálózat javasolt határait, összetevőit;
- meghatározzuk a hálózat működéséhez szükséges külső hálózatokat;
- bemutatjuk a hálózattal együttműködő legfontosabb külső hálózatokat.

A *rendőrségi informatikai hálózat tartalmának, határainak értelmezése* – más hálózatokhoz hasonlóan – szükségessé teszi olyan szempontok meghatározását, amelyek alapján egyes elemekről, összetevőkről eldönthető, hogy az adott hálózat részét képezik-e, vagy annak környezetéhez tartoznak. Ezen szempontok közé többek között irányítási/felügyeleti, szolgáltatási és technológiai kérdések tartoznak. A különböző megközelítések sok esetben az alkalmazott hálózat-megnevezésekben is jelentkezni szoktak.

Az *irányítás/felügyelet központú megközelítés* szerint a hálózat határait az irányítási, felügyeleti jog- és feladatkör határai jelölik ki. Mindez megvalósítható mind alkalmazó, mind szolgáltató szervezetek szempontjából. Ennek megfelelően egy elem, összetevő akkor tartozik egy adott hálózathoz, ha afölött egységes irányítás érvényesül. Ez választ el egy adott informatikai hálózatot az általa felhasznált, de más irányítása, felügyelete alatt álló hálózatoktól. Az egységes irányítás meghatározott szabályozási keretek közötti követelménytámasztási, fejlesztési, felügyeleti, üzemeltetési szabadságot, egyben felelősséget tartalmaz. A határok kiszervezett feladatok, igénybevett szolgáltatások esetében nem mindig könnyen jelölhetők ki. Esetünkben tehát vizsgálni kell, hogy a szóba jöhető hálózati elemek, összetevők körül mire terjed ki a Rendőrség irányítása, felügyelete.

A *szolgáltatások oldaláról történő megközelítés* alapját egy kiválasztott szolgáltatási kör meghatározása képezi. Ennek megfelelően egy elem, összetevő akkor tartozik egy adott hálózathoz, ha hozzájárul a hálózati szolgáltatás megvalósulásához és nem tartozik oda, ha léte nincs hatással a nyújtott szolgáltatásra. E megközelítés nehézségei a különböző

szolgáltatások egymásra épüléséből fakadnak. Ennek megfelelően a későbbiekben meg kell határozni, hogy miket kívánunk a rendőrségi informatikai hálózat szolgáltatásai közé sorolni.

A *technológiai szempontú megközelítés* az alkalmazott hálózati – fizikai, átviteli, kapcsolási, stb. – technológiákra épít. Ennek megfelelően egy hálózathoz azon elemek, összetevők tartoznak, amelyek egy adott technológia alkalmazására épülnek. A felsorolt három megközelítés közül felhasználói szempontból ennek van a legkisebb jelentősége. Ugyanazon (pld. távbeszélő) szolgáltatás számos különböző (pld. számítógép-, vagy műsorszóró) hálózati technológia segítségével, vagy ezek vegyes alkalmazásával is megvalósítható. Az elmondottak alapján véleményünk szerint ez a legkevésbé alkalmas a rendőrségi informatikai hálózat határainak kijelöléséhez.

Az *információs szolgáltatásokat nyújtó rendőrségi hálózatok* előzményei közé a belügyi ágazat távközlési hálózatai[5] tartoztak. Ezek üzemeltetése 1993-tól került át a Rendőrség (akkor az ORFK Híradástechnikai Szolgálata) feladatkörébe. 1999-ben jelent meg a Rendőrség és más rendvédelmi, rendészeti szervek számára szolgáltatásokat nyújtó Egységes Belügyi Digitális Hálózat (EBDH), mint a szolgáltatóktól lehetőség szerint független, a meglévő alrendszerekre építkező zártcélú hálózat koncepciója, amely támogatja a hagyományos beszéd- és adatátviteli alkalmazások igénybevételét. Ennek alapinfrastruktúráját egy 1990 és 2003 között kialakított önálló országos transzporthálózat képezte, amely mikrohullámú és Budapesten optikai, illetve vezetékes összeköttetésekre épült. A BM Távközlési Szolgálat felügyelete alá tartozó hálózat üzemeltetése 2007 elején Zártcélú Rendészeti Hálózat (zRH) megnevezéssel átkerült az akkor megalakult Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalához, majd 2011 tavaszán a kormányzati hírközlési szolgáltatóhoz (Kopint-Datorg Zrt.). [5, 27., 54., 90. o.]

A *rendőrségi szakmai dokumentumokban előforduló hálózatfogalmak* áttekintéséhez feldolgoztuk a Rendőrséggel kapcsolatos jogszabályokat és ORFK utasításokat. Ezek között több hálózat kifejezéssel is találkozhatunk.[6] E fogalmakra egységesen igaz, hogy értelmezésüket, meghatározásukat a dokumentumok nem tartalmazzák és nem is hivatkoznak más olyan dokumentumra, forrásra, ahol ezek meghatározása megtalálható, tehát gyakorlatilag a kifejezések értelmezését ismertnek tekintik. A publikációnk címében szereplő '*informatikai hálózat*' kifejezéssel csak egyetlen ORFK utasításban (meglepő módon a kutyás és lovas szolgálati szabályzatban) [6, 443. pont] találkoztunk.

A leggyakrabban előforduló fogalom a különböző jelzőkkel (belső, országos belső zárt) ellátott '*intranet*', vagy 'intranetes hálózat', amelynek egységesen elfogadott értelmezése: internet protokollokat használó, zárt – vagy csak biztonsági funkciókkal rendelkező eszközökön (tűzfal, átjáró) keresztül elérhető – számítógép-hálózat ("belső internet"). A '*számítógépes hálózat*' kifejezés önmagában is szerepel az ügyeleti szolgálattal, illetve az iratkezeléssel kapcsolatos szabályozásokban. [7, 35. és 106. pontok; 8, 15. pont]

Több szabályozóban megtalálható az '*adatátviteli hálózat*' fogalom, esetenként 'országos számítógépes' és 'rejtjelezett' jelzőkkel. [9, 10 pont] Ennek elfogadott értelmezése: adatátviteli szolgáltatások ellátására tervezett és optimalizált távközlő hálózat, amely hatékonyan képes adatok közvetítésére a hálózat végződései között, ahol adatátvitel alatt – a hagyományos analóg átvitellel szemben – digitális bitsorozatok, folyamok átvitelét értendő. Találkozhatunk még a '*táv-adatátviteli hálózat*' kifejezéssel is [10, 20. pont], amely a nagyobb távolságra történő adatátvitelt biztosító hálózatok megnevezése, azonban megítélésünk szerint használata napjainkban a lehetőség általánossá válásával már idejétmúlt.

[5] BM távhívó-távbeszélő hálózat, BM országos géptávíró hálózat, BM országos mozgószolgálati rádióhálózat, BM MRKB mobil rádiótelefon hálózat.

[6] A következőkben a több dokumentumban is előforduló hálózat kifejezések esetében csak egy, vagy néhány dokumentumra fogunk hivatkozni.

A hagyományos távközlési fogalmak közül a dokumentumokban a '*távbeszélő hálózat*' és a '*távhívó hálózat*' kifejezésekkel találkozhatunk. [11, 4. pont; 12] Ez utóbbi esetében a távhívás a helyi (egyetlen kapcsolóközpont segítségével lebonyolított) hívás ellentéte, más távbeszélő hálózatba irányuló – helyi központokat összekapcsoló távhívó központ(ok)on is átmenő – hívás. Ehhez a körhöz kapcsolható a távbeszélő hálózattal lényegében azonos értelmű '*hang-átviteli hálózat*' kifejezés is, ami a hangok (ezen belül beszéd) átvitelét lehetővé tévő – eredetileg analóg, később már digitális – hálózat. A kifejezés a 'hang- és távadat-átviteli hálózat' összetételben fordul elő [10, 20. pont], ami így gyakorlatilag egy integrált szolgáltatású hálózat megjelölése. Egy helyen szerepel a '*hír-összeköttetési hálózat*' kifejezés is [13, 2.e pont], amelyben a jelző a híradás, kommunikáció, információkapcsolat egyes rendvédelmi területeken korábban alkalmazott szinonimája.

A következő feladatunk ***a*** *rendőrségi informatikai hálózat határai, összetevői* körének kijelölése, vagyis annak meghatározása, hogy milyen kritériumok alapján mely összetevőket sorolunk a rendőrségi informatikai hálózathoz és melyeket tekintjük azon kívül állónak. A megnevezéstől (az 'informatikai' jelzőtől) ideiglenesen eltekintve, tartalmi szempontból a hálózat határainak meghúzásánál megítélésünk szerint csak a felhasználó-központú, szolgáltatás-alapú kritérium lehet megfelelő megoldás.

Általában és a hálózatok biztonságának vizsgálata szempontjából is a lényeg a nyújtott szolgáltatások biztonsága, amelyek különböző – egymástól függetlenül működő, de napjainkban inkább már egymással együttműködő – technológiai megoldásokra épülhetnek. Ennek megfelelően a meghatározandó hálózat-fogalomnak magában kell foglalnia minden, információs szolgáltatást nyújtó hálózatot, köztük a hagyományos távközlési, számítógépes és más (pld. térfigyelő, érzékelő, stb.) hálózatokat. Az ily módon körülhatárolt hálózat megnevezése az informatikai mellett lehetne más (pld. infokommunikációs, információtechnológiai = IT) is, ennek azonban megítélésünk szerint másodlagos a jelentősége.

A szolgáltatás-alapú megközelítés mellett dönteni kell abban is, hogy milyen kritérium kerüljön alkalmazásra a 'rendőrségi' jelző érvényesítése során. Az első, magától értetődő lehetőség, hogy a határ az ORFK irányítása, felügyelete szerint kerüljön meghúzásra. Ennek megfelelően a rendőrségi informatikai hálózat az ORFK irányítása, felügyelete alá tartozó hálózatokat, hálózati összetevőket foglalja magában és nem tartoznak bele a más (kormányzati és társ-) szervezetek által felügyelt hálózatok.

Egy tágabb értelmezés szerint a rendőrségi informatikai hálózat keretei közé sorolhatóak a következő – a rendőrségi tevékenységhez szorosan kapcsolódó jellegű, de nem a Rendőrség szervezetében, hanem a Belügyminisztérium irányítása, felügyelete alá tartozó – szervezetek (belügyi szervek): a Szervezett Bűnözés Elleni Koordinációs Központ, a Nemzeti Védelmi Szolgálat, a Terrorelhárítási Központ és a Rendőrtiszti Főiskola. E tágabb értelmezést indokolhatja a szervezeti informatikai hálózatok kiterjedt együttműködési kapcsolatrendszere, illetve a hálózatbiztonsági követelmények, kockázatok, megoldások jelentős hasonlósága, esetenként azonossága.

A rendőrségi informatikai hálózat – mint ráépített (átfedő) hálózat[7] – működése során *felhasznált külső hálózatok* közé tartozik mindenekelőtt a Zártcélú Rendészeti Hálózat (zRH), az Elektronikus Kormányzati Gerinchálózat (EKG), az Egységes Digitális Rádiótávközlő Rendszer (EDR), a BM országos távhívó távbeszélő hálózata, valamint egyes távközlési szolgáltatók hálózatai. A rendőrségi informatikai hálózat országos infrastruktúráját, gerinchálózatát gyakorlatilag a fenti hálózatok, ezek közül is elsősorban a zRH biztosítja.

A fizikailag önálló *Zártcélú Rendészeti Hálózat* egy technikai megoldással[8] az *Elektronikus Kormányzati Gerinchálózat* virtuális kiegészítő gerinchálózatát, annak

[7] Overlay network.
[8] MPLS VPN Carrier Supporting Carrier.

melegtartalékát is képezi, egyben az EKG is nyújthat szolgáltatást a zRH-nak oly módon, hogy a két hálózat önállóan felügyelhető, működésük egymást nem befolyásolja. [5, 94. o.] Az *Egységes Digitális Rádiótávközlő Rendszer* keretein belül egy rendészeti virtuális magánhálózat (VPN) működik, amely a rendőrség, a büntetésvégrehajtás és a Nemzeti Védelmi Szolgálat felhasználói körére terjed ki. Az EDR hálózat erőforrásainak több mint 80%-át a rendészeti VPN használja. A *BM országos távhívó távbeszélő hálózata* két budapesti főgyűjtő gócközpontot, mintegy 30 kormányzati és rendészeti célú objektum távbeszélő alközpontját, valamint az érintett épületek strukturált kábelhálózatát foglalja magában.

Végül röviden – csak felsorolásszerűen – számba kell vennünk, melyek azok a legfontosabb, *együttműködő külső hálózatok*, amelyek szorosabban kapcsolódnak a rendőrségi informatikai hálózathoz, amelyek jelentősebb szerepet játszhatnak a rendőrségi informatikai hálózat biztonsági kérdéseinek elemzése, gyakorlati megvalósítása során. Ezek körének meghatározása részletesebb vizsgálatot igényel és attól is függ, hogy az érintett hálózatokkal a rendőrségi informatikai hálózat milyen módon – közvetlenül, vagy más, felhasznált hálózatokon keresztül – áll kapcsolatban. Az azonban megfogalmazható, hogy az együttműködő külső hálózatok főbb csoportjait a kormányzati/közigazgatási hálózatok, a védelmi szféra más szervezeteinek (honvédség, katasztrófavédelem, nemzetbiztonsági szolgálatok, mentőszolgálat, büntetésvégrehajtás, vám- és pénzügyőrség, stb.) hálózatai, valamint egyes nemzetközi (elsősorban európai úniós és NATO) hálózatok alkotják.

JAVASLAT A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT FOGALMÁRA

Az előzőekben foglaltakra építve a rendőrségi informatikai hálózat fogalma a következő formában határozható meg: *a Rendőrség, az ORFK felügyelete, irányítása alatt álló, információs szolgáltatásokat nyújtó technikai hálózatok összessége.* A fenti meghatározásnak megfelelően a rendőrségi informatikai hálózat magában foglalja a hagyományos távközlési (vezetékes és mobil távbeszélő, géptávíró, rádiótávközlő, stb.) hálózatokat, a számítógépes hálózatokat, valamint a speciális rendeltetésű térfigyelő, érzékelő és más hálózatokat.

A hálózat megnevezésére más szakkifejezés is használható lehetne, erre a magyar (szak)nyelvben elvileg több jelzős kifejezés – pld. információs, informatikai, infokommunikációs, információtechnológiai, stb. – található, azonban ezekhez a különböző szakterületeken, a különböző szakmai körökben, iskolákban eltérő értelmezések kapcsolódnak és közülük egyik sem nyert széleskörű, megkerülhetetlen elfogadást. A hálózatbiztonság szempontjából az 'informatikai' jelző 'információs tevékenységeket támogató, megvalósító technikai [megoldás]' tartalmú használatát indokolja az is, hogy a Magyar Informatikai Biztonsági Ajánlások is ezt a jelzőt tartalmazzák.

A rendőrségi informatikai hálózat tehát olyan hálózat, amelynek rendeltetése a rendőrségi feladatok során felmerülő információs tevékenységek támogatása, megvalósítása, elemei technikai eszközök (rendszerek) és az elemek között információcserét biztosító valós fizikai, vagy absztrakt – más hálózatok szolgáltatásaira épülő – logikai kapcsolatok állnak fent.

Felhasznált irodalom

[1] HENK Tamás-NÉMETH Krisztián: Távközlő hálózatok. Jegyzet. – BME Távközlési és Médiainformatikai Tanszék, 2005.

[2] MUNK Sándor: Katonai informatika III. A katonai informatika eszközrendszere. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003.

[3] MUNK Sándor: Katonai informatika II. Katonai informatikai rendszerek, alkalmazások. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006.

[4] MUNK Sándor: Katonai informatika I. A katonai informatika alapjai. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003.

[5] PÁNDI Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-, katonai- és közigazgatási kommunikációs rendszerek megszervezésére és irányítására. Doktori (PhD) értekezés. – ZMNE, Budapest, 2005.

[6] 17/2009 (OT 10.) ORFK utasítás a Rendőrség Kutyás és Lovas Szolgálati Szabályzatáról.

[7] 53/2010 (OT 31.) ORFK utasítás a Rendőrség ügyeleti szolgálata és a közreműködésével teljesítendő jelentési és tájékoztatási kötelezettség rendjéről.

[8] 12/2009 (OT 7.) ORFK utasítás a Kriminalisztikai Archiváló Rendszer üzembeállításával és működtetésével kapcsolatos egyes feladatokról.

[9] 5/2009 (OT 3.) ORFK utasítása Rendőrség szervei hivatásos, köztisztviselői, közalkalmazotti állománya és a nyugállományba vonulók igazolványának, valamint a hivatásos állomány szolgálati azonosító jelvényének és hímzett azonosítójának kiadásáról és nyilvántartásának rendjéről.

[10] 4/2008 (OT 4.) ORFK utasítás az Országos Rendőr-főkapitányság Szervezeti és Működési Szabályzatáról.

[11] 23/2007 (OT 16.) ORFK utasítás az Országos Rendőr-főkapitányság telekommunikációs eszközökkel történő ellátásának rendjéről, valamint a távközlési szolgáltatások igénybevételének szabályairól.

[12] ORFK Gazdasági Főigazgatóság, Informatikai Főosztály, Kommunikációs és Adatátviteli Osztály információi.

[13] www.police.hu/content/organization?contentid=1996664; (letöltés: 2011.05.19.)

[14] 2009 (OT 15.) az Országos Rendőr-főkapitányság és a Magyar Barlangi Mentőszolgálat között kötött együttműködési megállapodás.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Munk Sándor
munk.sandor@zmne.hu

INFORMÁCIÓS SZOLGÁLTATÁSOKAT NYÚJTÓ HÁLÓZATOK ALAPJAI

Absztrakt

Napjaink társadalmának leírására széles körben elfogadottak az információs társadalom, hálózati társadalom kifejezések. Az információs társadalom technológiai alapját az információs szolgáltatásokat nyújtó hálózatok képezik. Napjaink másik, senki által nem vitatott jelensége az információs tevékenységeket támogató technológiák konvergenciája, integrációja. Tényként fogadható el az is, hogy az egymással egyre szorosabb kapcsolatba kerülő szakterületek fogalomrendszere nincs egymással harmóniában, ami egyre növekvő mértékben akadályozza a hatékony együttműködést. Jelen publikáció meghatározza az információs szolgáltatásokat nyújtó hálózatok fogalmát, szerepét; bemutatja kialakulásuk okait; elemzi a hálózatok és rendszerek viszonyát; végül meghatározza felépítésük, összekapcsolódásuk alapvető kérdéseit.

Society of our age is widely described as information society, and networked society. Information society is technologically based on networks providing information services. Other unquestioned phenomenon of our age is convergence, integration of technologies supporting information activities. It is also a fact that concepts, and ideas of professional areas, building more and more strong connections with each other, are not in harmony and that increasingly impedes the efficient cooperation. Recent publication defines the concept, and role of networks providing information services; presents the reasons for their formation; analyses the relationships between networks and systems, and finally determines fundamental issues of their architecture, and interconnections.

***Kulcsszavak**: információs (informatikai) hálózatok, hálózati alapfogalmak, elosztott rendszerek, hálózatok felépítése, hálózatok összetevői ~ I(T) networks, foundational network concepts, distributed systems, network architectures, network components*

BEVEZETÉS

A napjaink társadalmának leírására széles körben használt fogalmak között leggyakrabban az *információs társadalom, hálózati társadalom* kifejezésekkel találkozhatunk. A témakörrel átfogó módon foglalkozó Manuel Castells megfogalmazása szerint "… a kialakuló társadalmi struktúrák domináns funkciói és folyamatai az információs korban egyre inkább hálózatokba szerveződnek." [1., 598. o.], "… társadalmi szerveződésünk kulcsfontosságú összetevője az információ, és az üzenetek és képek áramlásai a hálózatok között társadalmi struktúránk alapvető összekötő fonalát alkotják." [1, 608. o.] A fentiekkel jellemzett információs társadalom technológiai alapját értelemszerűen mindenekelőtt az információs szolgáltatásokat nyújtó, információs tevékenységeket támogató és megvalósító hálózatok képezik.

Napjainkra a hálózatok a társadalom, a gazdaság, a kultúra és a magánszféra alapvető elemeivé váltak, a korszerű közlekedési, közmű és kommunikációs hálózatok nélkül ma már elképzelhetetlen az élet. Ezen belül az *információs szolgáltatásokat nyújtó hálózatok* szerepe, jelentősége az élet minden területén (a közigazgatásban, a gazdaságban, védelmi illetve katonai alkalmazásban és a magánéletben) folyamatosan nő. A Magyar Köztársaság esetében az infokommunikációs ágazat középtávú cselekvési terve ezt a következőképpen fogalmazza meg. "Az egyre magasabb szintű fogyasztói elvárások és a folyamatos technológiai fejlődés eredményeként – a világ legfejlettebb országaihoz hasonlóan – hazánkban is kialakulóban van egy összetett, felhasználók millióit és eszközök tízmillióit egyre nagyobb kapacitású hálózatokkal összekötő és egyre magasabb szintű szolgáltatásokkal kiszolgáló, folyamatosan fejlődő rendszer." [2, 8. o.]

Az információs korszak, az információs társadalom alapját képező technológiák másik széles körben felismert jelensége a különböző szakterületek, többek között az *információs, kommunikációs és média technológiák*[1] *konvergenciája, integrálódása*. A konvergencia alapját egyrészt funkcionális, másrészt technológiai tényezők képezik. Valamennyi érintett szakterület közös jellemzője, hogy rendszerei, eszközei, eljárásai információs tevékenységeket támogatnak, vagy valósítanak meg, illetve hogy technikai alapjait egyre növekvő mértékben a folyamatosan fejlődő mikroelektronika képezi. A technológiai fejlődés következményeiként fokozatosan elmosódnak a határok a korábban önálló szakterületek között és jelennek meg több szakterület szolgáltatásait, megoldásait ötvöző integrált rendszerek, eszközök.

Mint azt egy korábbi publikációban már megfogalmaztam: az egyes "szakterületek fogalomrendszere a sajátos igények, megközelítések és a saját múlt, szakmai fejlődés következtében nincs egymással harmóniában. Ezek a *különbözőségek, fogalmi heterogenitás* egyre növekvő mértékben akadályozzák és fogják akadályozni a hatékony együttműködést, az egyes szakterületek ismeretanyagának összehangoltságát, egységes rendszerbe történő integrálódását. A mind az elmélet, mind a gyakorlat oldaláról növekvő mértékben jelentkező igények szükségessé, elkerülhetetlenné teszik egy közös, átfogó, az egymással szoros kapcsolatba kerülő szakterületek számára is megfelelő fogalomrendszer kialakítását". [3, 52. o.]

A fentiek alapján jelen publikáció alapvető célja, egy nagyobb kutatás részeként, az információs szolgáltatásokat nyújtó hálózatok általános kérdéseinek, alapfogalmainak összegzése, rendszerezése, a kapcsolódó részterületek ismeretanyagával, fogalomrendszerével harmonizáló formában történő, azok számára keretként felhasználható meghatározása. Ennek érdekében:

- meghatározza az információs szolgáltatásokat nyújtó hálózatok fogalmát, helyét, szerepét;
- bemutatja az információs szolgáltatásokat nyújtó hálózatok kialakulásának okait, célját;

[1] Tágabb értelemben az említettek mellett ide tartoznak a következők is: nyomdatechnika, méréstechnika, irányítástechnika, irodatechnika, oktatástechnika, stb.

- elemzi az információs szolgáltatásokat nyújtó hálózatok és rendszerek viszonyát, fogalmi alapjait;
- végül meghatározza az információs szolgáltatásokat nyújtó hálózatok együttműködésének, összekapcsolódásának alapvető kérdéseit.

INFORMATIKAI HÁLÓZATOK: A TECHNIKAI HÁLÓZATOK EGY TÍPUSA

A bevezetésben már megfogalmazottak alapján vizsgálatainkat az információs szolgáltatásokat nyújtó hálózatokra összpontosítjuk. Ezzel a fogalommal a szakirodalomban gyakorlatilag nem találkozhatunk. Az egyes kapcsolódó szakterületek saját fogalmakat használnak, mint a távközlő hálózatok, kommunikációs hálózatok; számítógép-hálózatok, adat(átviteli) hálózatok; illetve műsorszétosztó-, műsorszóró és műsorelosztó hálózatok. Különböző megközelítések, iskolák összefoglaló fogalmaiként csak a következő kifejezések jelennek meg: informatikai, infokommunikációs, (elektronikus) hírközlő és műsorközlő hálózatok.[2] Ezek egyikének tartalma sem öleli fel az információs szolgáltatásokat nyújtó hálózatok teljes körét.

A következőkben a fogalomalkotás általános szabályait felhasználva teszünk kísérletet a vizsgálat tárgyát képező hálózatok fogalmának, valamint a hálózatok rendszerében elfoglalt helyük és szerepük meghatározására. A tudományos fogalomalkotás alapja a bővebb terjedelmű legközelebbi nem-fogalom (genus proximum), valamint a megkülönböztető jegy, jellegzetes különbség (differentia specifica) meghatározása. Esetünkben a magasabb szintű fogalomnak a hálózatot és azon belül a technikai hálózatot, megkülönböztető jegyként pedig a rendeltetést, a nyújtott szolgáltatásokat választjuk. Ennek keretében hálózat alatt meghatározott tulajdonságokkal rendelkező elemek (csomópontok) és az ezek között fennálló, meghatározott tulajdonságokkal rendelkező kapcsolatok összességét értjük [4, 183. o.].

A *technikai szféra hálózatai* [lásd 4, 180. o.] célirányosan, meghatározott szükségletek kielégítésére kerülnek létrehozásra, a természetben, az élővilágban megfigyelt, vagy a társadalomban kialakult hálózatokkal szemben mindig van rendeltetésük, meghatározott szolgáltatásokat nyújtanak. Ennek megfelelően technikai hálózat alatt olyan hálózatot értünk, amelynek elemei technikai eszközök (rendszerek) és amelyek között valós fizikai, vagy absztrakt logikai kapcsolatok állnak fent. Az egyes hálózatok rendeltetését, szolgáltatásait természetesen alapvetően meghatározzák a hálózat elemei és köztük fennálló kapcsolatok. Ennek megfelelően a technikai hálózatoknak három nagyobb csoportja különböztethető meg: a közlekedési hálózatok; az energiát, vagy anyagot továbbító hálózatok; valamint az információs szolgáltatásokat nyújtó hálózatok.

A közlekedési hálózatok rendeltetése a technikai eszközökkel végzett személy- és áruszállítás infrastrukturális feltételeinek (utak, pályák és kapcsolódó létesítmények) a biztosítása. A villamos energia hálózatok rendeltetése az erőművekben előállított áram eljuttatása a fogyasztókhoz, a különböző csővezetékes hálózatok pedig elsősorban folyadékokat (kőolaj, víz, szennyvíz, iszap, stb.), vagy gázokat (földgáz, más szénhidrogének, stb.), ritkábban szilárd anyagokat szállítanak. Végül a hálózat csomópontjai közötti információáramlásra épülő hálózatok rendeltetése információs tevékenységek támogatása, vagy megvalósítása.

A továbbiakban a vizsgálat tárgyát ez utóbbi csoportot alkotó *információs szolgáltatásokat nyújtó technikai hálózatok* képezik, amelyek rendeltetése információs tevékenységek támogatása, megvalósítása, elemei technikai eszközök (rendszerek) és az elemek között információcserét biztosító valós fizikai, vagy absztrakt – más hálózatok szolgáltatásaira épülő – logikai

[2] Ezek részletesebb vizsgálatával, értelmezésével egy későbbi publikációban fogunk foglalkozni.

kapcsolatok állnak fent. Ezek közül elsőként az információtovábbítást támogató távközlő, illetve műsorszóró hálózatok jelentek meg. A későbbiekben alakultak ki a további információs tevékenységtípusokat – információfeldolgozást-előállítást, információszerzést és információtárolást – támogató hálózatok is. A technológiai fejlődés következtében az idők során aztán folyamatosan előtérbe kerültek és kerülnek a több információs tevékenységet támogató, integrált információs szolgáltatásokat nyújtó hálózatok.

Az információs kapcsolatokra épülő technikai hálózatok esetében megkülönböztethetünk mikro- és makro-hálózatokat. A mikro-hálózatok esetében – amelyekkel elsősorban technikai eszközökön, berendezéseken belül találkozhatunk – a hálózat csomópontjai egymáshoz "viszonylag közel" (nanométerestől kb. a centiméteresig terjedő távolságban) vannak. A makro-hálózatok csomópontjai viszont egymástól távolabb, jellemzően földrajzi értelemben is távol helyezkednek el. A két csoport hálózatait hasonlóságaik mellett jelentős különbségek is jellemzik. A továbbiakban vizsgálódásainkat már csak a makro-hálózatokra szűkítve végezzük.

Az információs szolgáltatásokat nyújtó hálózatok összefoglaló fogalmának rövidebb megnevezésére a magyar (szak)nyelvben elvileg számos jelzős kifejezés – pld. információs, informatikai, infokommunikációs, információtechnológiai, stb. – lehetséges lenne, azonban ezekhez a különböző szakterületeken, a különböző szakmai körökben, iskolákban eltérő értelmezések kapcsolódnak. Egy adott tartalom megnevezése sok esetben nem vezethető le logikai alapon, ugyanazon tartalom különböző megnevezései között pedig általában nem állítható fel 'jobb-rosszabb', 'alkalmasabb-kevésbé alkalmas' reláció.

Jelen publikációban az információs szolgáltatásokat nyújtó hálózatok megnevezésére az informatikai hálózat kifejezést használjuk, aminek alapját az 'informatikai' jelző 'információs tevékenységeket támogató, megvalósító technikai [megoldás]' tartalmú értelmezése képezi. Ugyanezen értelmezés jelenik majd meg az informatikai eszköz, informatikai rendszer fogalmak értelmezésében is. Természetesen egy meghatározott tartalom megnevezése megállapodás kérdése, így ez a kifejezés/megnevezés a későbbiekben tetszőleges, egységesen elfogadott szakkifejezéssel felváltható.

INFORMATIKAI HÁLÓZATOK KIALAKULÁSA

Az információs szolgáltatásokat nyújtó hálózatok vizsgálatának első lépéseként érdemes áttekinteni, hogy milyen okok vezettek ezen hálózatok kialakulásához, milyen céllal került sor információs képességekkel rendelkező eszközök hálózatba kapcsolására, kapcsolódására. Az okok első nagy csoportja az információtovábbítást támogató, megvalósító távközlési hálózatokhoz kapcsolódik.

Az információk[3] (beszéd, hang, írott szöveg, álló és mozgókép, adat, technológiai folyamatok vezérlő jelei, stb.) továbbítására létrehozott hagyományos távközlési és műsorközlő hálózatok esetében a cél az *információtovábbítás támogatása*, az információ(k) egy adott helyről más hely(ek)re történő eljuttatása. Ennek megfelelően a hálózat kiemelt csomópontjait az információk küldését és fogadását biztosító technikai eszközök (végberendezések) képezik, amelyek között az információáramlás technikai támogatás – átviteli vonalak és kapcsolóelemek – nélkül gyakorlatilag nem lenne, vagy nem megfelelő hatékonysággal lenne lehetséges. Ebben az esetben tehát a hálózat kialakításának indokát elsősorban a különböző szolgáltatási pontok (végpontok) térbeli elhelyezkedése és a köztük megvalósítandó információtovábbítási igény képezi. A hálózat további csomópontjai már az információtovábbítás megvalósításának technológiai, szervezési, gazdaságossági és más belső szempontjai figyelembevételével jelen-

[3] Pontosabban az információkat hordozó különböző reprezentációk.

nek meg, többnyire a hálózati (távközlési) szolgáltatásokat igénybevevők számára átlátszó, számukra érdemi jelentőséggel nem bíró módon.

A távközlési hálózatok kezdetben egy konkrét szolgáltatást nyújtottak (pld. távíró, távbeszélő), a végberendezések és az ezeket hálózatba kapcsoló vonalak, kapcsolóelemek szorosan egymáshoz tartoztak. A későbbiekben olyan távközlési (pld. géptávíró/telex, fax) hálózatok jelentek meg, amelyekhez már nem tartozott önálló technikai hálózati megoldás, az információk továbbítását megfelelő átalakítások után más létező (elsősorban a távbeszélő) hálózatok biztosították. A modemes átalakítás segítségével a hagyományos távközlési (távbeszélő) hálózatok egy meghatározott átviteli sebességig adatátviteli szolgáltatásra is alkalmassá váltak. Végül megjelentek a tervezetten több szolgáltatást nyújtó (pld. ISDN) távközlési hálózatok is.

Az információs szolgáltatásokat nyújtó hálózatok kialakulása okainak második nagy csoportja a számítógép-hálózatok megjelenéséhez kapcsolható. Ezek eredeti rendeltetése nem elsősorban az információtovábbítás, információcsere volt, kialakulásuk valójában az *információk, információs képességek megosztásának támogatása* feltételeit biztosította. Ez elsőként a más számítógépeken található információk elérését, kezelését; más számítógépek feldolgozóképességének felhasználását; valamint a más számítógépekhez kapcsolódó speciális eszközök (perifériák) használatának lehetőségét foglalta magában. A hálózat csomópontjait ebben az esetben az egyes felhasználók számítógépei (a hálózati szolgáltatásokat nyújtó 'végberendezések'), az esetleges kiszolgáló eszközök, valamint a hálózati kapcsolóelemek képezik.

A távközlési hálózatokkal ellentétben a számítógép-hálózatok 'végberendezései' önmagukban, hálózatba kapcsolódás nélkül is képesek információs szolgáltatásokat nyújtani (információt szerezni, tárolni, előállítani, vagy rendelkezésre bocsátani), legfeljebb korlátozottabb mértékben, vagy hatékonysággal. A hálózati szolgáltatás lényege ebben az esetben tehát az adott eszköz képességeinek külső erőforrásokkal történő kiegészítése.

A számítógép-hálózatok lehetőségeinek további kihasználására épült a hálózatba kapcsolódás okainak harmadik csoportja, amelynek lényege az azonos, vagy hasonló információs képességeket, szolgáltatásokat nyújtó eszközök összekapcsolása révén az összetevők képességeinek egyszerű összegzését meghaladó, *magasabb szintű,* vagy akár *új képességek kialakítása*. A hálózatba kapcsolódás révén különböző információs (rész)képességekkel rendelkező eszközökből meghatározott információs szolgáltatásokat nyújtó, egységes egészként működő eszközrendszerek épülhetnek fel. Ez tulajdonképpen a részegységekből felépülő eszközök kialakításának analógiájára, de új szemléletmódra – az úgynevezett hálózatközpontú, hálózatalapú[4] megközelítésre – épülő megvalósítás, amelynek lényege az egyes részképességeket szolgáltató összetevők szétválasztása, önálló, általában földrajzilag is eltérő helyen történő kialakítása.

A hálózatközpontú megközelítés, a hálózatba kapcsolódás nem csak a különböző képességek, szolgáltatások egymáshoz kapcsolására, hanem azonos, vagy hasonló képességek egymást erősítő együttműködésére épülő megoldásokra is biztosít lehetőséget. Azonos, vagy hasonló információs képességek, szolgáltatások összekapcsolása az összetevők képességeinek egyszerű összegzését meghaladó, magasabb szintű, vagy akár új képességek kialakítását eredményezheti. Ezek a képességek épülhetnek többek között az együttműködő összetevők számára, feladatmegosztására, vagy térbeli elhelyezkedésére. Több azonos, vagy eltérő típusú érzékelő-eszköz együttműködése növelheti az információszerzés pontosságát (vagy egyáltalán megteremtheti lehetőségét). Több tárolóeszköz együttműködése javíthatja a tárolás biztonságát, a tárolt információk elérhetőségét, hozzáférhetőségét. Végül több információfeldolgozó

[4] Network centric, network based.

eszköz együttműködése (az elosztott, vagy grid-alapú számítások) az önálló eszközök által megvalósíthatatlan számítási kapacitást biztosít.

Napjainkban a szakterületek konvergenciája és integrációja következtében, illetve az előzőekben elmondottak alapján ma már egyre kevésbé lehetséges és célszerű a hagyományos távközlési és számítógép-hálózatok (vagy például a kábeltévé hálózatok) megkülönböztetése, elkülönítése. Emiatt is szükség van egy minden korábbi és újonnan megjelenő, szakterületi hálózat-fogalmat keretbe foglaló átfogó fogalom, az informatikai hálózat fogalmának bevezetésére.

Az *eltérő, kibővülő tartalmú értelmezések* miatt különösen a számítógép-hálózatok megnevezése ad alkalmat félreértésre, így alkalmazása egyre inkább kerülendő. A szakirodalomban található meghatározások a számítógép-hálózatok elemeiként:

- számítógépeket (vagy autonóm számítógépeket) tartalmaznak [5, 22. o.];
- számítógépeket és más eszközöket említenek [6, 732-01-03];
- vagy bennük adatfeldolgozó rendszerek, eszközök szerepelnek [7, 01.01.45, 11. o.].

A legszűkebb értelmezés esetében tehát a hálózat kizárólag (általános célú) számítógépekből állhat, a legtágabb értelemben pedig csomópontjai lehetnek bármilyen, adatfeldolgozási képességgel rendelkező eszközök.

A fenti értelmezési kérdéseket csak tovább nehezíti a számítógép fogalmának tartalma, amely alatt sokan mindenki által használt általános célú számítógépeket értenek, pedig a fogalom meghatározásai (amelyek lényege: automatizált adatfeldolgozó eszköz) ennél sokkal tágabb körre kiterjedő értelmezést írnak le: magukban foglalják például a célszámítógépeket (így pld. a távközlési hálózatok kapcsolóközpontjait, kapcsolóelemeit) is. Ráadásul napjainkban már olyan, információs tevékenységeket támogató, integrált funkciójú technikai eszközök jelentek meg (okostelefonok, GPS-készülékek, médialejátszók, stb.), amelyek ennek a definíciónak teljes egészében megfelelnek, tehát számítógépnek 'tekinthetők'.

INFORMATIKAI RENDSZEREK ÉS HÁLÓZATOK, INFORMATIKAI HÁLÓZATOK HATÁRAI

Az információs szolgáltatásokat nyújtó hálózatok fogalmának vizsgálata során nem kerülhető meg az információs szolgáltatásokat nyújtó rendszerek fogalma és e két fogalom viszonyának elemzése sem. Már előzetesen megjegyezhető, hogy a szóhasználatban sok esetben keveredik a két kifejezés, lényegében azonos tartalomhoz kapcsolódóan találkozhatunk a rendszer és a hálózat kifejezésekkel (pld. távbeszélő rendszer és távbeszélő hálózat), más esetekben viszont a jelzős kifejezések egyértelműen eltérő tartalmakat jelölnek (pld. felügyeleti irányító és adatgyűjtő rendszer, illetve hálózat). A következőkben meghatározzuk az információs szolgáltatásokat nyújtó rendszer fogalmát.

Információs szolgáltatásokat nyújtó, vagyis *informatikai rendszer* alatt a továbbiakban eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására (információs szolgáltatások nyújtására) létrehozott (működő, technikai) rendszerét értjük. [8, 21. o.] A rendszer fogalmába általában beleértjük a valamilyen szintű formális körülhatárolást és a működési, illetve irányítási, felügyeleti (működtetési, fejlesztési) autonómiát. Ezek a jellemzők különböztetik meg – bár természetesen nem matematikai pontossággal – az egymástól független rendszereket, az alrendszerekből felépülő rendszereket, az egymással tervezetten, szorosabban együttműködő rendszereket (rendszerek rendszere), valamint az egymással dinamikusan változó módon, lazábban együttműködő rendszereket (rendszerek szövetsége).

Az informatikai rendszer fogalom fentiekben szereplő értelmezéséhez kapcsolódóan ki kell emelni, hogy a definícióban foglalt tartalom nem korlátozódik a számítástechnikai – 'számítógép(es)' – rendszerekre, amennyiben ezek alatt általános célú számítógépekre épülő technikai rendszereket értünk. A definícióban szereplő 'eszköz' bármely – tágabb értelemben vett – informatikai, vagyis olyan technikai eszköz lehet, amelynek rendeltetése információs tevékenységek támogatása, megvalósítása.[5] Az informatikai jelzőt eszközök esetében is a korábban bemutatott tartalommal használjuk, fenntartva azt a megjegyzést, hogy a körülhatárolt tartalom leírására bárki joggal használhat más kifejezést is.

Az információs szolgáltatásokat nyújtó hálózatok tartalmilag minden tekintetben megfelelnek a rendszerfogalom kritériumainak (működő technikai rendszerek), így elvileg, kellő önállóság esetén minden informatikai hálózat egyben – egy speciális – informatikai rendszernek is tekinthető. Ugyanakkor a két fogalom értelmezései számos esetben utalnak 'rész / egész', vagy 'szolgáltatást igénybe vevő / szolgáltatást nyújtó' viszonyra. A hálózatok és rendszerek viszonya alapvetően attól függ, hogy hol húzzuk meg a hálózat határait, mit tekintünk a hálózat részének és mit azon kívül álló összetevőnek.

Egy *hálózat határai, összetevőinek köre* megítélésünk szerint a hálózat által nyújtott szolgáltatások alapján határozhatóak meg. Ennek megfelelően azon összetevők tartoznak egy hálózathoz, amelyek hozzájárulnak a hálózati szolgáltatások megvalósításához és nem tartoznak oda azok, amelyek léte nincs hatással a nyújtott szolgáltatásokra. Ez a megközelítés elsősorban a csomópontok esetében jelent mérlegelési lehetőséget, hiszen a csomópontokat hálózatba kapcsoló logikai, vagy fizikai összeköttetések a hálózat lényegi részét képezik.

A hálózati csomópontok három nagy csoportját a hálózati szolgáltatások igénybevételét biztosító, illetve a szolgáltatásokat nyújtó csomópontok (végpontok), a hálózati információáramlást megvalósító, biztosító csomópontok (belső pontok), valamint az előző két funkcióval egyaránt rendelkező csomópontok képezik. Amennyiben ez utóbbiakat logikailag két összetevőre – egy végpontra és egy belső pontra – bontjuk és egy virtuális kapcsolattal kötjük össze, két alapvető csomópont-típussal kell számolnunk.[6] Ezek közül a belső csomópontok[7] egyértelműen a hálózat részét képezik, így a hálózathoz történő tartozás ténylegesen elsősorban a végpontok esetében vizsgálandó.

A *hálózati végpontok* információs szolgáltatásokat nyújtó technikai hálózatok esetében jellegüket tekintve két alapvető csoportba sorolhatóak. Az első esetben a hálózati végpont részét képezi a szolgáltatások igénybevételét, vagy nyújtását biztosító technikai eszköz, vagy rendszer, a másodikban viszont csak a csatlakozási lehetőséget biztosító felület (interfész) és szükség esetén az ezt biztosító csatolóeszköz, csatolóelem tartozik a hálózathoz.

A távközlési szakterületen, az ISDN hálózatok kialakulása során a fenti két értelmezésnek megfelelően jelent meg a távszolgáltatások és a hordozó szolgáltatások fogalma [9]. Erre építhetőek a megfelelő hálózat fogalmak is[8]. A távszolgáltató hálózat sajátossága, hogy részét képezi a végberendezés és alkalmazás (e nélkül a szolgáltatás nem lenne elérhető), a hálózat az átvitt jelet, adatot – az alkalmazáshoz illeszkedő módon – feldolgozhatja, egy adott repre-

[5] A meghatározás szerint ezek közé tartoznak pld. a távbeszélő, távíró, fax-készülékek, hagyományos és 'okos' mobiltelefonok, médialejátszók (MP3 player), GPS helymeghatározók és navigációs eszközök, bankjegykiadó automaták, bolti pénztárgépek, mérésadatgyűjtő eszközök, szenzor-berendezések, szórakoztató elektronikai eszközök, stb.

[6] Mint azt a Távközlő hálózatok jegyzet is teszi logikai (forgalmi) hálózatok esetében [9, 64-65.o.].

[7] Távközlő hálózatok esetében kapcsolók, rendezők, nyalábolók, számítógép-hálózatok esetében jelerősítők, passzív elosztók, kapcsolók, útvonalválasztók (csomagkapcsolók), átjárók, stb.

[8] Teleservice network, bearer network.

zentációról egy másikra[9] átalakíthatja. [10, 71. o.] Ezzel szemben a hordozó hálózat olyan hálózat, amely két vagy több pont között biztosít átlátszó – a hálózat által nem értelmezett, nem feldolgozott – adatátvitelt (jelátvitelt), nem csatlakozik hozzá közvetlenül végberendezés és nem tartozik hozzá alkalmazás sem.

A fenti két fogalom (megnevezés) a gyakorlatban széles körben nem terjedt el, azonban tartalmuk ma is alkalmas a hálózatok két nagy típusának elhatárolására. Ennek megfelelően megkülönböztethetünk a felhasználók által közvetlenül igénybe vehető, végszolgáltatásokat nyújtó hálózatokat és más rendszerek, hálózatok számára átviteli, hordozó szolgáltatásokat nyújtó hálózatokat.

A hálózatok vizsgálhatóak az informatikai rendszerek 'irányából' is. Informatikai rendszerekhez kapcsolódóan a hálózatok elsőként a ma már kihalóban lévő *távadatfeldolgozó rendszerek* esetében jelentek meg, amelyek lényege központi számítógép(ek) szolgáltatásainak elérése távolról, speciális – kezdetben kizárólag be- és kiviteli funkciókat megvalósító – technikai eszközök, végberendezések (ún. terminálok) segítségével. A távadatfeldolgozó rendszerek hálózatai egyszerű felépítésű, csillagtopológiájú hálózatok voltak, amelyek csomópontjait a központi számítógép, a terminálvezérlő eszköz és az ehhez kapcsolódó – közeli és távoli – terminálok alkották. A távoli terminálkapcsolatot biztosító adatátviteli vonalak az akkori távközlési rendszerek (telefon, telex, rádió) szolgáltatásaira épülve[10] kerültek megvalósításra.

A számítógépek közötti adatátvitel – ezen belül a távoli számítógépek közötti távadatátvitel – lehetőségeinek bővülésével, elterjedésével a távadatfeldolgozó rendszereket az *elosztott rendszerek* követték. Az elosztott rendszerek fogalmának különböző meghatározásaival találkozhatunk, amelyek közül az egyik legelterjedtebb értelmezés Tanenbaum professzoré: önálló számítógépek együttese, amely felhasználói számára egyetlen koherens rendszernek tűnik. [11, 15. o.] Más, általánosabb megfogalmazás szerint egy elosztott rendszer több autonóm feldolgozó elem rendszere, amelyek együttműködnek egy közös rendeltetés megvalósítására, vagy egy közös cél elérésére. [12, 523. o.] Tágabb értelmezésben tehát az elosztott rendszerek összetevői nem feltétlenül számítógépek, hanem információcsere és más sajátos információs képességekkel rendelkező eszközök.

Az elosztott rendszerek két nagy csoportját a szorosan összekapcsolt és a lazán összekapcsolt[11] típusok alkotják. Az előbbiek jellemzője, hogy a feldolgozó elemek (csomópontok) rendelkeznek közös, osztott memória-hozzáféréssel, míg az utóbbiaknál ez nem lehetséges, így esetükben a csomópontok közötti információcsere üzenetalapú. A szorosan csatolt rendszerek a gyakorlatban egymáshoz fizikailag közeli – egy rack szekrényben, egy eszközben, egy kártyán, vagy akár egy lapkán elhelyezett – elemekből állnak, amelyeket mikro-hálózatok kötnek össze. A továbbiakban – szűkebb értelmezés szerint – az elosztott rendszerek közül csak a lazán kapcsolt rendszerekkel foglalkozunk.

Sokan hagyományos értelemben a távadatfeldolgozó és az elosztott rendszerek fogalmait – kimondva, kimondatlanul – számítógépekhez, mégpedig általános célú számítógépekhez kapcsolják és nem tekintenek ebbe a csoportba tartozónak számos más, információs tevékenységet támogató rendszert, amelyek rendeltetése például *távirányítás/távvezérlés, távfelügyelet, vagy távmérés*[12] vagy ezek együttese. Az ilyen rendszerek sajátossága eredetileg az volt, hogy végberendezéseik jelentős része nem autonóm számítógép, hanem speciális beavatkozó, vagy érzékelő eszköz. Ezek azonban tágabb értelemben szintén az informatikai – rendeltetésük sze-

[9] Például 4 kHz sávszélességű analóg jelről 64 kbit/s digitális adatfolyamra és vissza.
[10] Az adatátviteli összeköttetést kapcsolt, vagy bérelt távközlési vonalak biztosították.
[11] Tightly coupled és loosely coupled.
[12] Remote control, remote monitoring, telemetry.

rint informatikai tevékenységet támogató, megvalósító – eszközök közé tartoznak és ugyanezen okból tágabb értelemben az említett rendszerek is informatikai rendszerek. Ebből következően az informatikai rendszerek és a hálózatok kapcsolatát vizsgálva ezen rendszereket is figyelembe kell venni.

A hálózatba kapcsolt, hálózatra épülő informatikai rendszerek[13] szempontjából a hálózatok két nagy csoportba sorolhatóak. Az első csoportot az egyes (szervezeti, vagy funkcionális) *informatikai rendszerek saját, 'dedikált' hálózatai* alkotják, amelyek:

- az adott informatikai rendszer integráns részét képezik;
- szolgáltatásaikat kizárólag az adott informatikai rendszer számára nyújtják;
- irányításuk, felügyeletük az adott informatikai rendszer irányításának, felügyeletének részét képezi.

A dedikált hálózatok lehetnek autonóm (önmagukban is teljes körűen működőképes, minden kapcsolóelemet és átviteli vonalat magukban foglaló), vagy más hálózatok szolgáltatásaira (is) épülő hálózatok. Ez utóbbi esetben a külső szolgáltatások köre egyes átviteli utak (néhány, vagy több) külső megvalósításától az átviteli szolgáltatások teljes körének külső megvalósításáig terjedhet. A két végletet így a hálózat teljes mértékben saját fizikai megvalósítása, illetve az adott rendszer szempontjából teljes mértékben virtuális hálózat képezi.

A szervezeti, vagy funkcionális informatikai rendszerek hálózatainak határait "alulról" tehát az irányítás, felügyelet határai jelölik ki. Az ezen kívül álló hálózati összetevőkre, pontosabban az igénybevett hálózati szolgáltatásokra vonatkozóan az adott informatikai rendszer irányítói csak szolgáltatási megállapodásban rögzített igényekkel, követelményekkel élhetnek, a megvalósítás eszközeire, módjára érdemi ráhatásuk nincs. A hálózatok és szolgáltatásaik egymásra épülésével részletesebben majd a következő pontban foglalkozunk.

A második csoportba *a több informatikai rendszer számára szolgáltatásokat nyújtó hálózatok*, más néven szolgáltatói hálózatok tartoznak. Ezek kezdetben a hagyományos távbeszélő hálózatokat felhasználó modemes adatátviteli szolgáltatásokra épültek, a későbbiekben viszont megjelentek a speciális digitális átviteli technológiákra épülő adatátviteli hálózatok[14]. A távközlési szakterület megfogalmazása szerint az adatátviteli hálózat "adatátviteli szolgáltatások ellátására tervezett és optimalizált távközlő hálózat, amely hatékonyan képes adatok közvetítésére a hálózat végződései között". [10, 24. o.] Napjainkra ez a fogalom (és ehhez kapcsolódóan még inkább a távadatátviteli hálózat fogalma) megítélésem szerint idejét múlta, használatuk megtévesztő és kerülendő. Korunk integrált szolgáltatású hálózatait már nem egy adott típusú, hanem számos különböző szolgáltatás ellátására tervezik és optimalizálják, így csak adatátviteli szolgáltatást nyújtó hálózatról és nem adatátviteli hálózatról beszélhetünk. Ráadásul napjaink korszerű hálózatai ma már a nyújtott (vezetékes és mobil távbeszélő, műsortovábbító, műsorszóró, stb.) szolgáltatástól függetlenül mind adatátviteli technológiára épülnek, tehát tulajdonképpen már minden hálózat "adatátviteli hálózat".

Összességében megállapítható, hogy egy információs szolgáltatásokat nyújtó (informatikai) hálózat kellő autonómia esetén maga is informatikai rendszernek tekinthető. Egy informatikai hálózat határai a hálózat által nyújtott szolgáltatások, illetve az egyes összetevők ehhez történő hozzájárulása alapján határozhatóak meg. Ebből a szempontból a két nagy csoportot a felhasználók által közvetlenül igénybe vehető, végszolgáltatásokat nyújtó hálózatokat és a más rendszerek, hálózatok számára átviteli, hordozó szolgáltatásokat nyújtó hálózatok képezik. Ez utóbbiak csak az információtovábbítást biztosító csatolóelemeket (interfészeket), kapcsolóelemeket és átviteli vonalakat foglalják magukban, míg a végszolgáltatásokat nyújtó há-

[13] Networked (IT) systems.
[14] Ritkábban, elsősorban a távközlési szakterületen: adathálózatok, adatközlő hálózatok.

lózatok részét képezik a szolgáltatások igénybevételét biztosító végberendezések, valamint a szolgáltatások nyújtásában részt vevő (kiszolgáló) eszközök, berendezések.

Az informatikai hálózat (mint rendszer) más rendszerekhez (hálózatokhoz) viszonyítva lehet:

- önálló (autonóm) rendszer;
- egy rendszer viszonylagos önállósággal rendelkező, de annak részét képező alrendszere;
- más rendszer(ek) számára szolgáltatásokat nyújtó (ehhez esetleg további szolgáltatásokat felhasználó) önálló rendszer.

Az elsőre példának tekinthetőek az első távíró, vagy távbeszélő hálózatok (rendszerek). A második típusba tartoznak például a térfigyelő rendszerek, vagy a felügyeleti, irányító és adatgyűjtő rendszerek dedikált hálózatai. Végül a harmadik csoportba sorolhatóak korunk integrált szolgáltatású távközlő hálózatai.

INFORMATIKAI HÁLÓZATOK EGYÜTTMŰKÖDÉSE, INFORMATIKAI HÁLÓZATOK FELÉPÍTÉSE, ÖSSZETEVŐI

Az információs szolgáltatásokat nyújtó technikai hálózatok alatt – mint azt a korábbiakban rögzítettük – olyan hálózatot értünk, amelynek elemei (csomópontjai) informatikai képességekkel rendelkező technikai egységek, eszközök, vagy rendszerek, és amelyek között információtovábbítást, információcserét biztosító kapcsolatok állnak fent. Az informatikai hálózatok – sőt minden hálózat – megfelelnek a rendszer-kritériumoknak, így esetükben is értelmezhető az alhálózat (alrendszer) fogalma, illetve hálózatok, mint összetevők összekapcsolódhatnak egy nagyobb hálózatban (amelynek így alhálózatait képezik).

A rendszerelméleti megközelítésnek megfelelően az informatikai alhálózat egy nagyobb informatikai hálózat olyan része (összetevője), amely önmagában is informatikai hálózatnak tekinthető. Csomópontjai és kapcsolatai közé az eredeti hálózat csomópontjainak és kapcsolatainak egy része tartozik. Összetett informatikai hálózat alatt pedig olyan hálózatot értünk, amelyen belül önálló alhálózatok különíthetőek el. Megjegyzendő, hogy egy informatikai hálózat lehet része, informatikai alhálózata más rendeltetésű (nem informatikai) technikai hálózatnak is, azonban ezzel a következőkben külön nem foglalkozunk.

Az *összetett hálózat, alhálózat* fogalmak használata során először arra kell választ adni, hogy mikor és milyen szempontok alapján tekinthető egy informatikai hálózati eszköz-együttes önálló hálózatnak (alhálózatnak), vagy egy hálózat összetett hálózatnak, vagyis összekapcsolódó, együttműködő hálózatok együttesének. Az önállóság kritériumai természetesen vizsgálati, gyakorlati szempontoktól függően különbözőképpen határozhatóak meg. A kritériumok közé tartoznak mindenekelőtt: a rendeltetés, a technológia, az irányítás/felügyelet, a biztonsági követelmények/megoldások, valamint a földrajzi elhelyezkedés. Ezek a tényezők sok esetben egymással összefüggésben állnak: eltérő rendeltetéshez, vagy eltérő földrajzi jellemzőkhöz (kiterjedéshez) többnyire eltérő technológiai megoldások is tartoznak. Elemi hálózatnak egy meghatározott rendeltetésű, valós fizikai kapcsolatokra épülő, egységes irányítás alatt álló hálózatot (erőforrás-rendszert) célszerű tekinteni. Ezen felül további kritérium lehet az alkalmazott technológiai megoldás (valamilyen szintű) azonossága is.

Az összetett hálózatok lényegét meghatározott szempontok szerint elkülöníthető *(al)hálózatok összekapcsolódása, együttműködése* képezi, amelyek így a felhasználók számára, szolgáltatási szempontból egyetlen hálózatnak 'látszanak'. Hálózatok összekapcsolásának alapvető célja az általuk nyújtott szolgáltatások körének, elérhetőségének kibővítése. Ennek első lehetősége a szolgáltatásokat igénybevevők, az egymással "egy hálózaton lévő" – így egymással információt cserélni (kommunikálni) képes – felhasználók körének bővítése volt, ami a föld-

rajzilag, vagy szolgáltatók szempontjából elkülönült hálózatok összekapcsolódásában jelentkezett. Erre elsőként a hagyományos távbeszélő hálózatok esetében került sor, majd ezt követte a számítógép-hálózatok globális hálózattá kapcsolódása.

A hálózatok összekapcsolódása során a felhasználói kör bővítése mellett cél lehet az azonos, vagy hasonló szolgáltatások különböző megoldásokkal, technikai módszerekkel történő elérésének biztosítása, illetve a szolgáltatások körének, vagy lehetőségeinek bővítése. Az előbbire példa a vezetékes, a mobil- és a számítógépes (pld. Skype-alapú) beszédkommunikációt biztosító hálózatok összekapcsolása. Az utóbbihoz sorolható a számítógépen elérhető SMS-szolgáltatás, illetve számítási képességeket biztosító hálózatok (gridek), számítási felhők, továbbá érzékelő, vagy tároló-hálózatok összekapcsolása.

A hálózatok összekapcsolódása gyakorlatilag a hálózatok közötti információcsere lehetőségének megteremtését, biztosítását jelenti. Ez a távközlési szakterület szakkifejezéseit felhasználva [részletesebben lásd 10, 71-73. o.], azt tágabban értelmezve megvalósulhat egyenrangú és hierarchikus összekapcsolás révén.

Egyenrangú összekapcsolás alatt két hálózat közötti olyan közvetlen kapcsolatot, információcsere megoldást értünk, amelyet egy – mindkét hálózat csomópontját képező – csatlakoztató egység valósít meg. A csatlakoztató egység feladata az összekapcsolt hálózatok közötti különbözőségek feloldása, a hálózatok között kicserélt információk és szolgáltatások szükség szerinti, interoperábilis átalakítása. A csatlakoztató egységet távközlési hálózatokban általában együttműködtető egységnek, számítógép-hálózatokban pedig a feloldandó technológiai eltéréstől függően átjárónak, hídnak, kapcsolónak, elosztónak, jelismétlőnek nevezik.[15]

A gyakorlatban több hálózat összekapcsolása a páronkénti, egyenrangú megoldás helyett hatékonysági szempontokból már általában egy e célra kialakított – összekapcsoló – hálózat segítségével történik, ami szükség esetén több szinten megismételhető. A *hierarchikus összekapcsolás* tehát hálózatok közötti olyan közvetett kapcsolat, megoldás, amelyben az információcsere lehetőségét egy másik hálózat biztosítja. Ebben az esetben az összekapcsolandó hálózatok egy-egy csatlakoztató egységgel kapcsolódnak az őket összekapcsoló, más néven gerinchálózathoz, amely gondoskodik a továbbítandó információk az érintett hálózatok (csatlakoztató egységeik) közötti átjuttatásáról.

A hierarchikus összekapcsolás során a páronkénti összekapcsolások (átalakítások) nagyobb számával szemben csak egy, vagy néhány közös közvetítő megoldásra (szabályrendszerre és formátumra, protokollra) történő át- és visszaalakításra van szükség. Az információcsere a gerinchálózatban az összekapcsolandó hálózatok szempontjából átlátszó módon valósul meg. Megjegyzendő, hogy a végfelhasználói szolgáltatásokat nyújtó hálózatok hierarchikus összekapcsolása ezen hálózatok és a gerinchálózat egyenrangú összekapcsolásai révén valósul meg.

Az egyenrangú és hierarchikus összekapcsolás fogalmaira építve az összetett hálózatokat is *egyenrangú és hierarchikus felépítésű hálózatok* típusaiba sorolhatjuk. A hierarchikus (felépítésű, architektúrájú) hálózat olyan összetett hálózat, amelyben az alhálózatok hierarchikus módon, egy gerinchálózat segítségével kapcsolódnak össze. Hangsúlyozni érdemes, hogy hierarchikus felépítésű hálózatról és gerinchálózatról csak összetett hálózat esetében van értelme beszélni, egyébként minden hálózatot gerinchálózatnak tekinthetnénk.

Egyenrangú (összetett) hálózat alatt olyan összetett hálózatot értünk, amelyben az alhálózatok között csak egyenrangú, páronkénti kapcsolatok léteznek. Az egyenrangú összetett hálózat fenti fogalma nem keverendő össze az egyenrangú hálózat[16] széles körben haszná-

[15] Interworking unit (IWU), gateway, bridge, switch, hub, repeater.
[16] Peer-to-peer network.

latos értelmezésével. Ez utóbbi olyan hálózat (ellentéte a kiszolgáló-alapú hálózat), amelynek összetevői az erőforrás-megosztás szempontjából egyenrangúak, egyaránt lehetnek a szolgáltatások központi koordináció nélküli nyújtói és igénybevevői.

A *gerinchálózat*[17] egy összetett hálózat azon alhálózata, amely a hálózat más részeit, alhálózatait legmagasabb szinten kapcsolja össze, biztosít köztük információcserét. A gerinchálózat nélkül az összetett hálózat önálló, egymástól elszakított alhálózatokra esik szét. Mivel a hierarchikus összekapcsolás több szinten is lehetséges, így összetett hálózatban a gerinchálózat által összekapcsolt alhálózatok maguk is lehetnek hierarchikus felépítésűek, rendelkezhetnek – az összetett hálózat szempontjából alacsonyabb szintű – gerinchálózattal. Számítógép-hálózati terminológiában ennek a nagy kiterjedésű hálózatok[18], illetve ezek együttese – maga az Internet – fogalma felel meg.

A gerinchálózat kifejezés mellett a szakirodalomban – sok esetben szinonim értelemben – találkozhatunk a *törzshálózat*[19] kifejezéssel is. Az előbbi inkább szervezeti, az utóbbi inkább szolgáltatói hálózatok esetében használatos. A hagyományos távíró- és távbeszélő hálózatok esetében a törzshálózat (központközi hálózat) a kapcsolóközpontok közötti rész megnevezése volt, gerinchálózat alatt pedig a törzshálózat primer (saját körzetszámmal rendelkező) központjai közötti hálózatrészt értették. [10, 17. o.]

Szolgáltatói hálózatok esetében, amelyek jellemzően nagykiterjedésű hierarchikus felépítésű összetett hálózatok, a felhasználói szolgáltatások elérését biztosító hálózati elemek (végberendezések) a gerinchálózatnak nem képezik részét, ahhoz vagy a gerinchálózathoz csatlakozó alhálózatok, vagy egyedi összeköttetések segítségével kapcsolódnak. Ennek megfelelően a szolgáltatói hálózatok további alhálózatai[20] a végberendezések csatlakoztatásában, a hálózati szolgáltatások elérésében játszott szerepük alapján a távközlési szakterület megnevezésével hozzáférési és körzeti (felhordó) hálózatok közé sorolhatóak. A hozzáférési, körzeti és törzshálózatokat – bár valójában egyenrangúan összekapcsolt hálózatok – sokszor hierarchikusan egymásra épülő, úgynevezett hálózati síkokba rendezve jelenítik meg.

A *hozzáférési (elérési) hálózat*[21] egy összetett hálózat azon része, amelyhez a felhasználói végberendezések közvetlenül kapcsolódnak (vagy annak részét képezik) és amely közvetlenül, vagy más hálózaton keresztül kapcsolódik a szolgáltatást (internet, távbeszélő, műsorszétosztó, stb.) nyújtó hálózatrészekhez (a törzs-, vagy gerinchálózathoz). Hagyományos távközlési hálózatok esetében ez a végberendezések (előfizetők) és a helyi kapcsolóközpontok közötti hálózatrész, számítógép-hálózatok esetében ezt a szerepet a helyi hálózatok valósítják meg, kábeltévé hálózatok esetében pedig a hozzáférési hálózat(ok) megnevezése házhálózat és bekötőhálózat.

A *körzeti (felhordó, nagyvárosi, aggregációs) hálózat*[22] általában nagyobb hálózatok esetében megjelenő olyan hálózat, amelynek rendeltetése a hozzáférési hálózatok és a gerinchálózat közötti hatékony és gazdaságos kapcsolat megteremtése, a hozzáférési hálózatok forgalmának összefogása (rendszerezése, rendezése, kapcsolása). Számítógép-hálózatok esetében ezeket a nagyvárosi hálózatoknak[23] nevezik, kábeltévé hálózatok esetében pedig a vonalhálózat fogalommal találkozhatunk.

---

[17] Backbone network, network backbone.
[18] Wide Area Network (WAN).
[19] Core network.
[20] A hozzáférési, vagy felhordó hálózatokat és a gerinchálózatot (törzshálózatot) különböző szolgáltatók is üzemeltethetik.
[21] Access network.
[22] Aggregation / backhaul / metro[politan] network.
[23] Metropolitan Area Network (MAN).

Hierarchikusan összekapcsolt hálózatok esetében a felső hálózatot ráépített, az alsót alaphálózatnak is nevezik.[24] [10, 73. o.] A *ráépített* (átfedő) *hálózat* valós csomópontok és logikai kapcsolatok olyan logikai (virtuális) hálózata, amely egy másik hálózatra, annak szolgáltatásaira épül. A ráépített hálózat csomópontjait tehát logikai (virtuális) kapcsolatok kötik össze, amelyeket az alaphálózat egy, vagy több fizikai kapcsolatából álló útvonalai valósítanak meg. A ráépített hálózat olyan szolgáltatásokat nyújt, amelyek az alaphálózatban nem, vagy nem a szükséges módon állnak rendelkezésre. A ráépített hálózat lehet végszolgáltatásokat, vagy hordozó szolgáltatásokat nyújtó hálózat, az alaphálózat viszont csak hordozó hálózat lehet.

Ráépített és alaphálózatokra példák: faxhálózat távbeszélő hálózat felett, számítógép-hálózat távbeszélő hálózat felett, PDH hálózat SDH hálózat felett, vagy IPv6 hálózat IPv4 hálózat felett. Eredetileg az Internet is a távbeszélőhálózatra épülő ráépített hálózat volt, ma már viszont a hálózatok többsége az Internetre épülő ráépített hálózat.

A ráépített hálózatok speciális fajtája a *virtuális magánhálózat*[25], amely az alaphálózat – jellemzően nyilvános távközlési infrastruktúra – szolgáltatásaira építve, alagútprotokollok és informatikai védelmi eljárások segítségével biztosítja az információáramlás bizalmasságát. [13] Más megfogalmazásban a virtuális magánhálózat nyilvános, vagy magánhálózatok felhasználása más hálózati felhasználóktól elkülönített felhasználói csoportok létrehozására, amelyek egymás között úgy cserélnek információt, mintha magánhálózaton lennének. [14, 6. o.]

A virtuális magánhálózatok egyrészt magánhálózatokat kapcsolnak össze biztonságosan, másrészt egyes eszközök hálózathoz kapcsolódását biztosítják biztonságos módon. A virtuális magánhálózatokban a csomópontok közötti információcsere virtuális kapcsolatokon át, a közvetítő (közbenső) hálózat(ok)on beágyazottan, a hálózatok más eszközei számára láthatatlan módon kerül megvalósításra. A virtuális magánhálózat alhálózatai egy-egy átjárón keresztül kapcsolódnak az alaphálózatra (Internetre), majd miután hitelesítették egymást, kiépítenek egy-egy titkosított alagutat az alhálózatok közti forgalom ezeken az alagutakon keresztül folyik. A virtuális magánhálózathoz egy távoli, vagy mobil állomás is csatlakozhat, ebben az esetben az állomás egyben átjáró is.

Az egyes konkrét hálózatok leírására különböző absztrakciós szintek választhatóak, amelyekhez hálózatfogalmak is kapcsolódnak. A két végletet a részletektől leginkább elvonatkoztató logikai és a legrészletesebb leírást tartalmazó fizikai megközelítés képezi. A két véglet között – elsősorban számítógép-hálózatok esetében, az OSI rétegmodellhez kapcsolódóan – két további szinttel is találkozhatunk. Így a négy hálózati absztrakciós szint a fizikai hálózat, az adatkapcsolati hálózat, a forgalmi hálózat és a logikai hálózat.[26]

A *fizikai hálózat* részét képezi valamennyi csomópont és az ezeket összekötő valamennyi átviteli út (vezetékes és vezetéknélküli útszakasz, irányított, vagy osztott átviteli közeg). Csomópont minden olyan technikai elem, amely átviteli úthoz kapcsolódik (vezetékekhez csatlakozik, vagy adó/vevő interfésszel rendelkezik). [10, 63. o.]

Az *adatkapcsolati (transzport*[27]*, vagy szállító) hálózat* az első absztrakciós szint, amelynek csomópontjai a végpontok mellett a hálózat 2. OSI – adatkapcsolati – rétegbeli feldolgozást (is) végző elemei. Ennek a hálózatnak már nem képezik részét (pontosabban nem kerülnek

[24] Overlay network, base network.
[25] Virtual Private Network (VPN).
[26] Physical network, data link/transport network, traffic network, logical network.
[27] Ebben az összefüggésben nem összekeverendő a transzport hálózat gerinchálózat tartalmú értelmezésétől.

megjelenítésre) a jelismétlők, jel-elosztók, de szerepelnek benne a kapcsolók és az útválasztók[28]. A hálózat elemei közötti kapcsolatok itt már bizonyos értelemben logikai jellegűek.

A *forgalmi hálózat* a második absztrakciós szint, melynek csomópontjai között a végpontok mellett már csak azon kapcsolóeszközök (elsősorban útválasztók) szerepelnek, amelyek 3. OSI – hálózati – rétegbeli feldolgozást végeznek. Ebben a modellben különválasztásra kerülnek a végberendezések, valamint a gerinchálózat (törzshálózat). Ez utóbbinak részét képezik a gerinchálózati határcsomópontok és belső csomópontok, illetve a más hálózatokhoz történő csatlakozást biztosító kapcsolóeszközök. [10, 63-64. o.]

A legmagasabb szintű absztrakciót a tisztán *logikai hálózat* képezi, amely a végpontok (végberendezések) mellett más csomópontokat, kapcsolóelemeket nem is tartalmaz. Ennek ábrázolása általában a megszokott felhő szimbólummal történik, amely egymagában képviseli a végpontok közötti kapcsolatokat, jelezve hogy minden csomópont bármely másikkal információ- (adat-) kapcsolatban áll.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A szakirodalom tanulmányozása azt bizonyítja, hogy nem találkozunk a rohamos ütemben integrálódó információs (számítástechnikai), kommunikációs (távközlési), média- és más tágabb értelemben vett információs (navigációs, információgyűjtő, vezérlési/szabályozási, stb.) technológiák hálózatfogalmai alapjául szolgáló átfogó hálózatfogalommal, meghatározással. A különböző szakterületek önálló fejlődésük során kialakult saját fogalmakat használnak, összefoglaló fogalmakként csak olyan kifejezések jelentek meg, amelyek tartalma nem öleli fel az információs szolgáltatásokat nyújtó hálózatok teljes körét.

Megítélésünk szerint az integrálódó szakterületek közös kiinduló pontot képező alapfogalmát a következő tartalom képezheti: olyan hálózat, amelynek rendeltetése információs tevékenységek támogatása, megvalósítása, elemei technikai eszközök (rendszerek) és az elemek között információcserét biztosító valós fizikai, vagy absztrakt – más hálózatok szolgáltatásaira épülő – logikai kapcsolatok állnak fent. Ez fogalom a technikai hálózatok alárendelt fogalma, amelynek megkülönböztető jegye a rendeltetése. A fogalom megnevezésére a magyar (szak)nyelvben számos jelzős kifejezés – pld. információs, informatikai, infokommunikációs, információtechnológiai, stb. – lehetséges lenne, amelyek közül majd a használat választja ki (esetleg) az egységesen elfogadottat. Jelen publikáció az információs szolgáltatásokat nyújtó hálózatok megnevezésére az informatikai hálózat kifejezést használja.

Az információs szolgáltatásokat nyújtó hálózatok elsőként az információtovábbítás támogatására jelentek meg. Ezek közé a hagyományos távközlési (távíró, távbeszélő, telex, fax, és műsorközlő) hálózatok tartoztak. A következő csoportot az információk, információs képességek megosztását támogató számítógép-hálózatok képezték. Végül megjelentek a hálózatba kapcsolódó összetevők képességeinek egyszerű összegzését meghaladó, magasabb szintű, vagy akár új képességek kialakítását támogató hálózatok. A konvergencia és integráció következtében napjaink hálózatai már egyre kevésbé sorolhatóak be a szakterületi kategóriákba, emiatt is szükséges egy minden korábbi és újonnan megjelenő, szakterületi hálózat-fogalmat keretbe foglaló átfogó fogalom bevezetése. Ezzel párhuzamosan egyre kevésbé használhatóak az olyan fogalmak, mint számítógép-hálózat, adatátviteli hálózat, távadatátviteli hálózat.

Mivel az informatikai hálózatok minden tekintetben megfelelnek a rendszerfogalom kritériumainak (működő technikai rendszerek), így elvileg informatikai rendszernek is tekinthetőek. Ugyanakkor a két fogalom értelmezései számos esetben utalnak 'rész / egész', vagy 'szol-

[28] Router.

gáltatást igénybe vevő / szolgáltatást nyújtó' viszonyra. A hálózatok és rendszerek viszonyának tisztázásához meg kell tudni határozni a hálózatok határait, el kell dönteni mit tekintünk egy hálózat részének és mit azon kívül álló összetevőnek.

Egy hálózat határai, összetevőinek köre megítélésünk szerint a hálózat által nyújtott szolgáltatásokhoz kapcsolódóan határozható meg, vagyis azon összetevők tartoznak egy hálózathoz, amelyek hozzájárulnak a hálózati szolgáltatások megvalósításához és nem tartoznak oda azok, amelyek léte nincs hatással a nyújtott szolgáltatásokra. Ebből következően a hálózat információáramlást támogató belső csomópontjai és a csomópontokat összekapcsoló logikai, vagy fizikai összeköttetések a hálózat lényegi részét képezik.

Így mérlegelési lehetőség csak a hálózati szolgáltatások igénybevételét biztosító, illetve a szolgáltatásokat nyújtó csomópontok esetében van, ami alapvetően két megközelítést nyújt. Az első a végszolgáltatásokat nyújtó hálózat, amelynek részét képezik részét a szolgáltatások igénybevételét biztosító végberendezések, valamint a szolgáltatások nyújtásában részt vevő (kiszolgáló) eszközök, berendezések. A második az átviteli, hordozó szolgáltatásokat nyújtó hálózat, amely csak az információtovábbítást biztosító csatolóelemeket (interfészeket), a hálózati kapcsolóelemeket és az átviteli vonalakat foglalja magában.

Az információs szolgáltatásokat nyújtó (informatikai) rendszerek szempontjából a hálózatok két nagy csoportba sorolhatóak. Az első csoportot az egyes (szervezeti, vagy funkcionális) informatikai rendszerek saját, 'dedikált' hálózatai alkotják, a másodikba a több informatikai rendszer számára szolgáltatásokat nyújtó, más néven szolgáltatói hálózatok tartoznak. A dedikált hálózatok lehetnek autonóm, vagy más hálózatok szolgáltatásaira (is) épülő hálózatok.

Az informatikai hálózatok (mint rendszerek) esetében is értelmezhető az alhálózat (alrendszer) fogalma, illetve hálózatok, mint összetevők összekapcsolódhatnak egy nagyobb hálózatban (amelynek így alhálózatait képezik). Az informatikai alhálózat egy nagyobb informatikai hálózat olyan része (összetevője), amely önmagában is informatikai hálózatnak tekinthető. Összetett informatikai hálózat alatt pedig olyan hálózatot értünk, amelyen belül önálló alhálózatok különíthetőek el.

Egy informatikai hálózati eszköz-együttes különböző kritériumok alapján tekinthető önálló hálózatnak (alhálózatnak). Ezek közé tartoznak mindenekelőtt: a rendeltetés, a technológia, az irányítás/felügyelet, a biztonsági követelmények/megoldások, valamint a földrajzi elhelyezkedés. Elemi hálózatnak így egy meghatározott rendeltetésű, valós fizikai kapcsolatokra épülő, egységes irányítás alatt álló, esetleg azonos technológiát alkalmazó hálózatot (erőforrásrendszert) célszerű tekinteni.

Összetett hálózatok (al)hálózatok összekapcsolódása, együttműködése révén jönnek létre, amelyek ezzel a felhasználók számára, szolgáltatási szempontból egyetlen hálózatnak 'látszanak'. A hálózatok összekapcsolásának alapvető célja az általuk nyújtott szolgáltatások körének, elérhetőségének kibővítése. Az összekapcsolás lehet egyenrangú, vagy hierarchikus. Az előbbi két hálózat közötti olyan közvetlen kapcsolat, információcsere megoldás, az utóbbi hálózatok közötti olyan közvetett kapcsolat, megoldás, amelyben az információcsere lehetőségét egy másik hálózat biztosítja.

A hierarchikus felépítésű összetett hálózatok alhálózatai egy gerinchálózat segítségével kapcsolódnak össze. A gerinchálózat által összekapcsolt alhálózatok maguk is lehetnek hierarchikus felépítésűek, rendelkezhetnek alacsonyabb szintű gerinchálózattal. A gerinchálózat kifejezés mellett – elsősorban szolgáltatói hálózatok esetében – találkozhatunk a törzshálózat kifejezéssel is. Szolgáltatói hálózatok esetében a végberendezések csatlakoztatásában, a hálózati szolgáltatások elérésében játszott szerepük alapján további alhálózatok – hozzáférési és

körzeti (felhordó) hálózatok – különíthetőek el. Ezek a hálózatok az egyes hálózattípusok esetében más megnevezést is viselhetnek.

Hierarchikusan összekapcsolt hálózatok esetében használatos a ráépített és az alaphálózat fogalma. A ráépített (átfedő) hálózat valós csomópontok és logikai kapcsolatok hálózata, csomópontjait az alaphálózat egy, vagy több fizikai kapcsolatából álló útvonalaira épülő logikai kapcsolatok kötnek össze. A ráépített hálózatok speciális fajtája a virtuális magánhálózat, amely az alaphálózat szolgáltatásaira és speciális megoldásokra építve valósít meg védett információcserét, magánhálózatot.

A hálózatok leírása különböző absztrakciós szinteken lehetséges. Ennek megfelelően beszélhetünk fizikai hálózatokról, amelyeknek részét képezi valamennyi csomópont és valamennyi átviteli út. Az adatkapcsolati (transzport, szállító) hálózatnak a végpontok mellett már csak a legalább 2. rétegbeli feldolgozást (is) végző elemek részei. A hálózat elemei közötti kapcsolatok itt már bizonyos értelemben logikai jellegűek. A forgalmi hálózat csomópontjai között a végpontok mellett már csak azon kapcsolóeszközök (elsősorban útválasztók) szerepelnek, amelyek 3. rétegbeli feldolgozást végeznek. Végül a legmagasabb szintű absztrakciót a tisztán logikai hálózat képezi, amely a végpontok (végberendezések) mellett más csomópontokat, kapcsolóelemeket nem is tartalmaz.

FELHASZNÁLT IRODALOM

[1] Manuel CASTELLS: *Az információ kora: Gazdaság, társadalom és kultúra. I. kötet A hálózati társadalom kialakulása.* – Gondolat-Infonia, Budapest, 2005.

[2] *Digitális Megújulás Cselekvési Terv 2010-2014. Az infokommunikációs ágazat cselekvési terve a társadalom és a gazdaság megújulásáért.* – Nemzeti Fejlesztési Minisztérium, Budapest, 2010 december.

[3] MUNK Sándor: A kommunikáció fogalomrendszerének keretei az integrálódó információs technológiák korában. – In. *Kommunikáció 2009 konferencia kiadványa*, 2009.10.14., Budapest, ZMNE (51-64.o.)

[4] MUNK Sándor: Hálózatok fogalma, alapjai. - *Hadmérnök*, 2010. (V.)/3. (176-186.o.)

[5] Andrew S. TANENBAUM: *Számítógép-hálózatok.* Második, bővített, átdolgozott kiadás. – Panem Könyvkiadó, Budapest, 2003.

[6] *IEC Electropedia: The World's Online Electrotechnical Vocabulary.* - International Electrotechnical Commission, Genf, 2010.
[www.electropedia.org, 2011.04.15.]

[7] *ISO/IEC 2382-1:1993 Information Technology – Vocabulary – Part 1: Fundamental Terms. Third Edition.* – International Organization for Standardization/International Electrotechnical Commission, Genf, 1993.

[8] MUNK Sándor: *Katonai informatika II. Katonai informatikai rendszerek, alkalmazások.* Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006.

[9] *ITU-T Recommendation I.210, Integrated Services Digital Network (ISDN) service capabilities. Principles of telecommunication services supported by an ISDN and the means to describe them.* – International Telecommunication Union, 1993

[10] HENK Tamás-NÉMETH Krisztián: *Távközlő hálózatok. Jegyzet.* – BME Távközlési és Médiainformatikai Tanszék, 2005.

[11] Andrew S. TANENBAUM-Maarten VAN STEEN: *Distributed Systems: Principles and Paradigms.* Prentice Hall, 2002.

[12] Alan BURNS-Andy WELLINGS: *Real-time systems and programming languages (3rd edition).* – Addison Wesley, 2001.

[13] *VPN Technologies: Definitions and Requirements.* – VPN Consortium, Santa Cruz, 2008 július.
[www.vpnc.org/vpn-technologies.html, 2011.04.15.]
[14] ANDERSSON L., MADSEN, T.: *RFC 4026, Provider Provisioned Virtual Private Network (VPN) Terminology.* – Internet Engineering Task Force, 2005 március.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Répás József
jozsef_repas@hellokitty.com

GPS ALKALMAZÁSA A LÁTÓK ÉS LÁTÁSSÉRÜLTEK ÖSSZEHASONLÍTÓ VIZSGÁLATÁRA

Absztrakt

A cikk célja, hogy érintőlegesen bevezetve a látássérült alapismeretekbe, bemutasson néhány mérési eljárást látók és látássérültek képességeinek összehasonlítására, tudományos igényességgel és közölje az eddigi eredményeket. Látó emberek térhallását sokszor, sokan vizsgálták eltérő paraméterek és peremfeltételek mellett, amely során megállapítható, hogy a lokalizációs képességek mitől, mennyire függenek. Ilyenek pld. a lokalizációs bizonytalanság, fejhallgatós hibák a virtuális térben, test- és fejmozgás szerepe, a látás szerepe stb. Ugyanakkor vakokkal és gyengén látókkal korrekt, alapos összehasonlító vizsgálat még nem készült, amelynek során választ adhatunk arra, mikor, hol, hogyan hallanak jobban vagy rosszabbul a vakok?

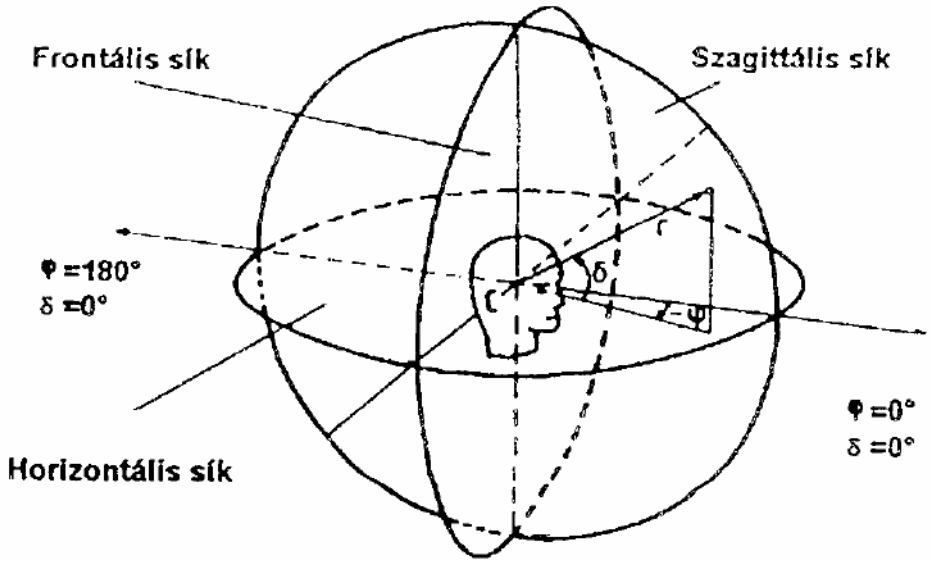
This article aims at introducing tangentially to the visually impaired literacy, produce some measurement procedure sighted and visually impaired ability to compare, and communicate scientific fastidiousness of the previous results. Spatial hearing of often sighted people, many different parameters and boundary conditions studied, which reveals that the localization capabilities for what, how much depends. Such specimens. the localization uncertainty, headphone errors in the virtual space, body and role of print head, etc. The role of vision. However, the blind and sighted fair, thorough comparative study has not yet been made, to which the answer can be given, when, where and how the blind hear better or worse?

Kulcsszavak: *GPS, látók, látássérültek, térhallás, látás ~ GPS, sighted people, visually impaired, spatial hearing, sight*

TÉRBELI HALLÁS

Az akusztika egyik legfontosabb területe az emberi hallásvizsgálatok, azon belül is a térhallás vizsgálatok. Ilyenkor gyakran pusztán irányhallásra szorítkozunk és a távolságérzékelés másodlagos.

Az ember, mint látó lény, „legfontosabb" érzékszerve, a szem alapján szerez információt a környezetéről. A hallás szerepe másodlagos, ezért kevésbé fejlett, sőt a hallást a látvány befolyásolni is képes. A *hang* valamilyen rugalmas közeg mechanikai rezgése és hullámzása az emberi hallás frekvenciáján (20 Hz-20 kHz). Azon forrást, amely a hangot kelti (rezeg, és a közeget rezgésbe hozza) *hangforrás*nak nevezzük. Jellemző rá a *helye*, amit az iránnyal, a távolsággal, és a szöggel adunk meg. A háromdimenziós vonatkoztatási rendszer az ún. fejhez rögzített (head-related) koordináta-rendszer. Síkjai: a fej szimmetriasíkja (mediális vagy szagittális sík), a hallójárat középvonala és a szemgödör alsó csontján átfektetett (horizontális), valamint az ezekre merőleges és a hallójáratok elülső peremére fekvő (frontális) sík. Ezek metszéspontja az origó, valahol a fej belsejében található (1.ábra). A vízszintes síkban az oldalirányú kitéréseket, a mediális síkban az előre-hátra iránymeghatározást vizsgálhatjuk (ebben a koordináta-rendszerben). Jelöljük φ-vel az oldalszöget, azaz a „pontosan szemben" iránytól (φ=0º) való eltérést a vízszintes síkban. A „pontosan hátul" irány felel meg φ=180º-nak. Delta szög az emelkedési (elevációs) szög. A mediális síkban δ=0º a fülek síkja, 90º a fej feletti, 180ºa fej mögötti. A távolságot r-rel jelöljük.



1. ábra. Fejhez rögzített koordináta-rendszer [1]

Hallásérzetnek nevezzük azt a jelenséget, amely a hallórendszerben valamilyen hangforrás hatására létrejön. Az érzet kialakulásának helye szintén leírható a távolsággal, szöggel, és az iránnyal. Fontos előrebocsátani, hogy a hangforrás helye egyáltalán nem biztos, hogy megegyezik a hallásérzet helyével. A helymeghatározhatóság, azaz a lokalizálhatóság a hangforrás, ill. a helyére vonatkozó kialakult érzetre jellemző. Megmondja, hogy az adott körülmények között mekkora a már érzékelt minimális helyváltoztatás, és az hogyan változik térben és időben. Egy forrás esetén is ez általában időben változó, tehát idővariáns.

Az irányhallás, mint képesség, az emberi fejlődés során alakul ki, és lesz egyre jobb tapasztalati úton. Az irányhallás olyan ösztönös folyamat, mely során a különböző forrásokat egymástól el tudjuk különíteni, és nem lép fel ún. diffúz hallástér. Diffúz hallástér esetén a hallás az irány pontos meghatározására már nem képes, minden irányból azonos hangterjedést észlelünk.

A lokalizáció az a helymeghatározási folyamat, melynek során a hallás kiértékeli a füljeleket, és információt szerez a hangforrás helyéről. A lokalizációs bizonytalanság az a küszöb, mely alatt a hallórendszer a térbeli jellemzőket nem képes megkülönböztetni. Ezen határ alatt a hangforrás (pontosabban a kialakult érzet) helyének megváltozását nem vagyunk képesek érzékelni, azaz nem észleljük, hogy helyváltoztatás történt volna. A lokalizáció során a hallás a hallásérzet helye és a hullámjelenség meghatározott ismertetőjelei között létesít kapcsolatot. Ezen jellemző(k) kis megváltozása helyváltoztatás-érzetet kelthet. A lokalizációs bizonytalanság az a minimális helyváltoztatás, amit a hallórendszer már érzékelni tud, azáltal, hogy a füljelben történt változást már ki tudja értékelni. A minimális lokalizációs bizonytalanság, azaz a hallás térbeli felbontóképessége a kísérletek szerint 1º körüli (abszolút minimum), és ez kb. két nagyságrenddel rosszabb, mint a látórendszer érzékenysége, ami 1'-nél kisebb változásokat is érzékelni képes.[2]

LÁTÁSSÉRÜLT ALAPISMERETEK

Látássérültnek nemcsak a vakokat és gyengén látókat nevezzük, hanem azokat az embereket is, akik összekeverik, illetve nem látják a színeket, és akik csak bizonyos napszakban látnak jól. A színtévesztők összekevernek bizonyos színeket, például a pirosat zöldnek látják és fordítva. A színvakság esetében pedig egyáltalán nem látják a színeket, nekik minden fekete és fehér. A szürke hályog is látásproblémát okoz, az illető homályosan lát, mintha egy hártya lenne a szeme előtt. Ezt csak orvosi műtéttel tudják kezelni. A farkasvakságban szenvedők nem látnak kevés fénynél, illetve alkonyatkor és hajnalban, tehát szürkületkor, sötétben és világosban viszont jó a látásuk.

A gyengénlátók általában csak elmosódott képeket, alakokat látnak. Esetükben a szemüveg se segít. A fény változásait érzékelik, meg tudják állapítani, hogy merről jön a fény, ez valamelyest segít a tájékozódásban, de nem sokat. A vakok pedig teljes látáskárosodottságban szenvednek, ők egyáltalán nem látnak semmit, így csak tapogatással és hallással tudnak tájékozódni. A szemüveg a kisebb szembetegségeken segít, illetve idősebb korban, amikor a szem romlásnak indul. Minél rosszabb valakinek a szeme, annál több dioptriás szemüveget kell hordania.[3]

A látás elveszítése vagy súlyos romlása mindenki számára nagyon nehéz helyzetet teremt. Az élet azonban nem áll meg, csak nagyon más lesz. A történteket nagyon nehéz feldolgozni nemcsak annak, aki megsérül, de a családjának is. Sokan elveszítik a munkájukat, a megélhetésüket, de még a mindennapok önállóságát is. Megváltoznak az emberi kapcsolatok is: sokan sajnálkoznak, legtöbben szívesen segítenek is, csak esetleg ügyetlenül fognak hozzá, de szinte senki nem viselkedik úgy, mint azelőtt. Aki szeretné visszaszerezni az élete irányítását, annak nagyon nagy erőfeszítéseket kell tenni: újra kell tanulni a legegyszerűbb dolgok elvégzését is, azután az önálló közlekedést, az információszerzés új módjait és gyakran új szakmát is.[4] Ebben a folyamatban a rehabilitáció központok nyújtanak segítséget.

Elsőként meg kell határozni azokat a kritériumokat, amelyek alapján meghúzható a határ az ép látásúak és a látássérültek között. A jó látás és a látássérülés között nyilvánvalóan folyamatos az átmenet. Az ép láthoz képest lehet rosszabb a látása valakinek anélkül, hogy ez a mindennapokban súlyos problémákat okozna szamara. A hagyományos definíció a látásélesség, latinul a visus, értekében határozza meg azt az értéket, a 0,3-at, ami alatt már gyengénlátásról, aliglátásról vagy vakságról beszélünk.[5]

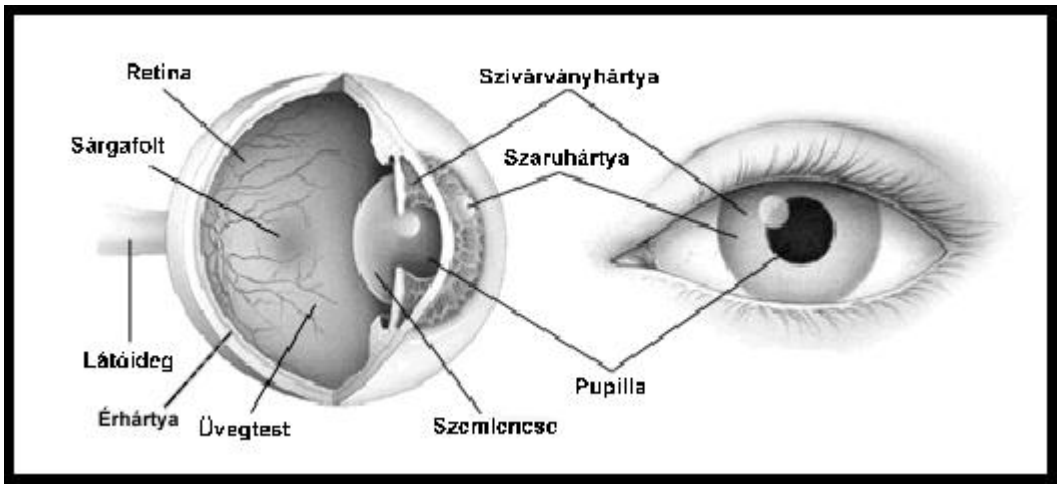
2. ábra. Vak logo[6]

A szervezetünket elsősorban külvilágból, környezetünkből fenyegeti veszély. Ezeket a behatásokat érzékszerveink hozzák tudomásunkra.[7] Figyeljük meg az utcán a vak embert (4. ábra). Fehér botjával maga előtt kopogtatja a járdát és szinte olyan sebességgel és könnyedséggel halad, mint a többi járókelő. A járda szélén le- és fellép, sőt az úttesten is átkel. Ha falkiszögellés kerül útjába, úgy kerüli ki, mintha látná. A szobában - kezeivel tapogatva maga körül – könnyedén, szinte észrevétlenül körüljár, pillanatok alatt tájékozódik szűkebb környezetéről és ezentúl mozgásán nem venni észre, hogy „sötét szobában" van. Egyik legfontosabb tájékozódó érzékszerve hiányzik és ezt meglepően nagymértékben pótolja más érzékszerveivel. Ha bekötött szemmel, kezünkben tartva vizsgálunk egy tárgyat, akkor arról többféle információt szerezhetünk, így felismerjük egyik vagy másik tulajdonsága - alakja, mérete, súlya, textúrája, összenyomhatósága - alapján. A felismerés tehát összetett folyamat, amelyben a legmagasabb agykérgi tevékenység is lényeges szerepet játszik.[8] A környezetből szerzett információ megszerzéséhez és feldolgozásához általában közvetlen érintkezés kell, de nem minden esetben. A vakok esetében például egy bottal történik a jellemzők megállapítása.

LÁTÁS

Az ember a környezetével az érzékszervei segítségével tartja a kapcsolatot. A látás, hallás, szaglás, tapintás, ízlelés közül a legnagyobb jelentőségű a látás. A szemünk a legfontosabb és legtöbbet használt érzékszervünk, az információ jó részét a látásunk útján szerezzük. Nem csak felépítését, de működését tekintve is valóságos mestermunka. A látás alapja az emberben és a gerinces állatokban a fényinger által kiváltott érzet, amelynek kiindulópontja a szem.[9]

A szemgolyó szabályos golyó formája nagyon fontos a tökéletes látáshoz. Szemben a pupilla szabályozza a fény bejutását, ezért van, hogy hol összeszűkül, hol kitágul. Akkor szűkül össze, ha nagy a fény napközben, és este a sötétben kitágul, így valamennyire éjszaka is látunk. Ha a szem formájában bármilyen változás lép fel, akkor a szaruhártyán érkező, a lencsében megtörő fénysugár keresztülhaladva az üvegtesten, nem a megfelelő részére érkezik az ideghártyának.



3. ábra. A szem felépítése [10]

A szembe érkező képet a retina jelekké alakítja át, a látóidegek pedig elküldik az agy látóközpontjába. A szem nagyon érzékeny, ha pld. porszem kerül a szemünkbe, azonnal reagál az idegen anyagra könnyezéssel, pislogással. Szemben nagyon sok apró ideg van, amelyek közül, ha csak egy is károsodik, a látás romlik.

A születésüktől fogva vak emberek vizuális ingerek feldolgozásáért felelős agyterületei részt vesznek a hang- és tapintásérzékelés feldolgozásában is. A Georgetown University Medical Center (GUMC) kutatóinak eredményei magyarázatot nyújtanak a vakok ezen ingerek érzékelése terén nyújtott kiemelkedő – a látó emberekét jócskán meghaladó – eredményeire.[11] A kutatók a vizsgálat során az FMRI (funkcionális mágneses rezonanciás képalkotó technika) eljárást alkalmazták, amely kimutatta, hogy a vakok bizonyos objektumok térbeli elhelyezkedésének megállapítására a látókéreg (vizuális kortex) specializált „moduljait" használják. A különböző funkciók, amelyeket a látáshoz társítunk – mint például a térérzékelés, minták és mozgás érzékelése – a vakok látókérgében továbbra is megtalálhatók. A vakok azonban ahelyett, hogy a látókéregben a szemből érkező információkat dolgoznák fel, a hallási és tapintási ingerek finomításába vonják be ezen agyterületeket.[12]

A lokalizációt vak emberek esetén a virtuális tér helyett gyakrabban vizsgálják a való életben, amelybe részben beletartozik a süketszobai környezet is. Utóbbi inkább alapkutatás jelleggel és általános információk szerzését szolgálja a hallásról és az agyi feldolgozásról, míg előbbi a gyakorlati felhasználást célozza meg. A tájékozódás során a vak ember számára elsődleges az egyes akadályok felismerése, megtalálása és kikerülése. Ezt a képességet akadályérzékelésnek nevezzük és esetünkben pusztán az akusztikai hatások alapján történő érzékelésre koncentrálunk [13].

A vakok képesek lehetnek jobban behatárolni a hangforrás irányát és az azt körülvevő akadályokat, mint a látók [14,15]. Ez azonban, ahogy láttuk, nem a perifériális érzékelés különbségéből adódik, hanem a hangszínváltozás tanult agyi feldolgozása során javul fel. A látók ill. a vakok szubjektív benyomása, értékítélete a hangszín változásairól eltérő. Amikor akadályt kell érzékelni két önkényes határvonalat húzhatunk: az első a távolabbi pont, amikor az alany először észleli az akadályt az útjában, míg a második a végső pont, amikor megáll, mert szerinte már ütközés következne be. Korábbi megfigyelések szerint az első ún. „első érzékelés" pont kb. 3 méter, míg az „ütközéselkerülő pont" 0,3 m. [16, 17, 18, 19, 20] Utóbbi estben maximális az akadályérzékelés érzékenysége (ehhez kb. 2 ms időeltérés tartozik). Ekkor a veszélyérzet is maximális, ami a vakok számára fontosabb.

ÖSSZEHASONLÍTÓ VIZSGÁLATOK

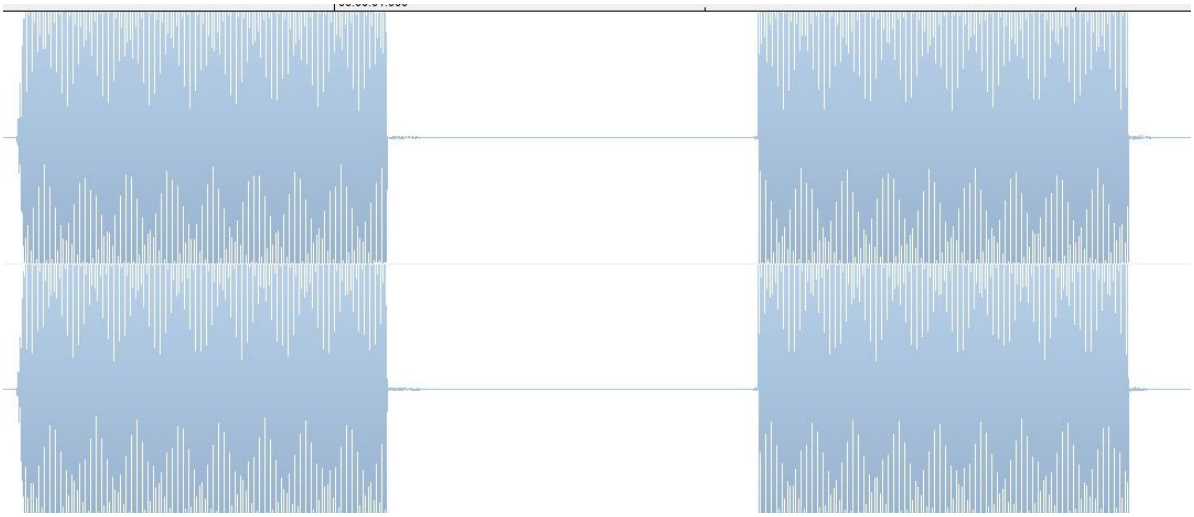
A kidolgozott kísérletekben, laborkörnyezetben azt is vizsgáltam, hogy látók képesek-e az objektumok térbeli elhelyezkedésének érzékelése. Első kísérletként a vizuális inger nélkül hanghatások alapján (visszaverődések, árnyékolás) kell egy akadályt megtalálni és „nem nekimenni". Előzetes próbáink alapján, amikor az akadály a hangszóró és az alany között volt elmondható, hogy nem süketszobai környezetben ez szinte lehetetlen. Első körben még zenével próbáltam, ám később 5 látóval, fehérzajjal megismételve bebizonyítottam, hogy valóban nem vagyunk képesek érzékelni az akadályt.

A szabadtéri kísérletekben minden feladathoz ugyanazokat az eszközöket használtam: kétféle 5 perces gerjesztőjelet, hogy kellően hosszú legyen több vizsgálathoz is. Ezek a gerjesztőjelek CD-minőségű (mono) wave vagy 192kbps mp3 formátumban állnak rendelkezésre és egy Microsoft Windows Mobile 5.0 for Pocket PC Premium Edition operációs rendszerrel működő Fujitsu-Siemens Pocket LOOX N560 PDA-ról kerülnek lejátszásra. A fejhallgató-kimenetet összeköttem egy SONY TA-D505 erősítővel és egy egyutas hangsugárzóval. Magassága 110 cm. A kibocsátott hangnyomásszintet BK 2260-as

kézi zajanalizátorral ellenőriztem a hangszóró főtengelyében 1 méter távolságban, értéke 80,4 dB.

Második kísérletet az egyetem melletti 20*40 méteres kézilabda pályán végeztem. Az egyik kapuközepén elhelyeztük a hangforrást, majd a hallgatóknak egyik kapuból a másikba kellett sétálniuk bekötött szemmel. Első körben vakon, a hangforrás segítsége nélkül. Második esetben 1 kHz-es pityegést (click-train gerjesztést) kellett követniük, míg a harmadik esetben fehér zaj történt kisugárzásra.

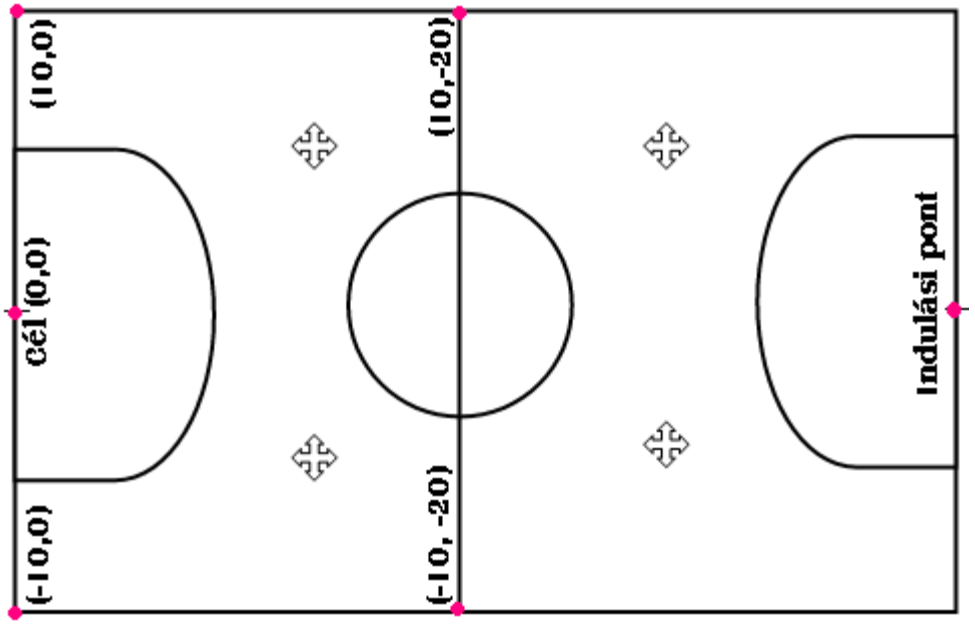
A mérőjel ún. 1-kHz click-train gerjesztés, amely során 200 ms hosszúságú 1 kHz-es szinuszcsomagot követ egy 200 ms-os csend stb. Egy wave editorban ez az alábbi módon néz ki (4. ábra). A másik mérőjelünk klasszikus fehérzaj (5. ábra), amelyet a későbbiekben használunk.



4. ábra. Click-train gerjesztés Készítette: Tasi István 2011

5. ábra. Fehérzaj gerjesztés Készítette: Tasi István 2011

A feladat közben rögzítésre került az útvonal, az idő és a célhoz viszonyított eltérés. Az útvonal GPS segítségével és papír alapon került rögzítésre. Az eltérést egy koordináta rendszerben rögzítettem, ahol a kapu közepe cél, a (0,0) pont. Az alapvonal az X tengely, a pálya középvonala pedig az Y tengely. A középvonaltól való eltérések pozitív, illetve negatív értékeket kaptak. Abban az esetben, ha az alany az alapvonalat elérve jobbra tért el a céltól, akkor pozitív az eltérés előjele, míg a bal irányú eltérés negatív előjellel rendelkezik. Amennyiben az alany nem az alapvonalat éri el, hanem az oldalvonalat, abban az esetben nem csak az X koordináta változik, hanem az Y koordináta is, negatív irányban. Ekkor a kísérletnek vége.



6. ábra. Kézilabdapálya és nevezetes koordinátái Készítette: Répás József

A nyomvonalkövetéshez a High Tech Computer (HTC) Diamond 2-es készüléket választottam. A Microsoft Windows Mobile 6.1 Professional operációs rendszerrel működő mobiltelefon IGO 8-as navigációs szoftverrel és 20 csatornás GPS vevővel rendelkezik. Kis méretéből adódóan nem befolyásolja az alanyokat a kísérlet során, kézbe véve kényelmesen használható.

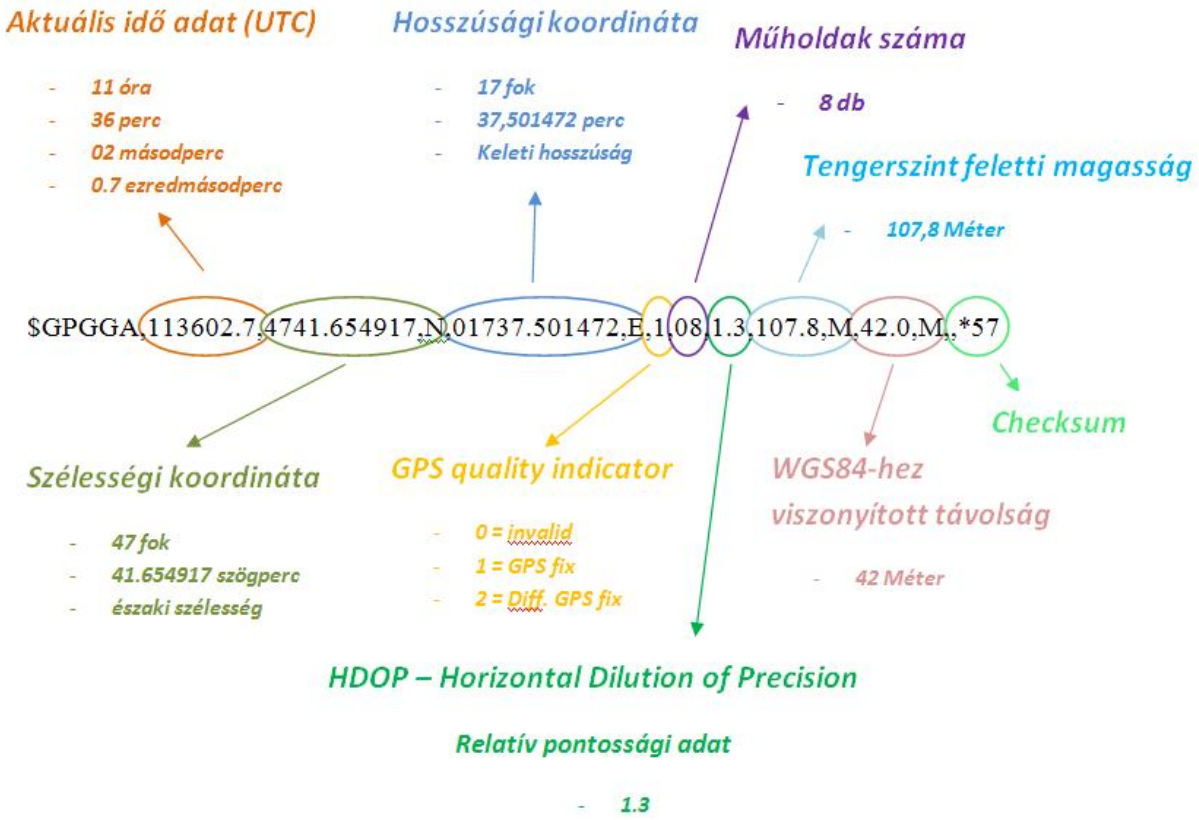
A nyomvonal felvétele lehet egyszerű, vagy intelligens. Az egyszerű programnál beállítható, hogy a készülék milyen időközönként-, vagy milyen távolságonként rögzítse az GPS paramétereket.

A navigációs szoftver lehetővé teszi az útvonaladatok rögzítését, későbbi feldolgozását. A készülék a GPS adatokat, például a pozíció meghatározó adatokat ún. GPS Fix Adatokat (Global Positioning System Fix Data - GPGGA), a sebességet meghatározó Track Made Good and Ground Speed (GPVTG) adatokat a *.bin* kiterjesztésű log fájlokban tárolja el.

A GPS log fájl számunkra legérdekesebb része a GGA mondat (7. ábra), illetve a sebességet rögzítő mondat, ami alapján konvertálás után elkészül a *.gpx* kiterjesztésű fájl, amely a teljes útvonalat tartalmazza.

A Föld nem szabályos gömb alakú, a geoid formát csak közelíteni lehet. Ehhez a közelítéshez több ellipszoid modellt dolgoztak ki (GRS80, NAD83, WGS84). A GGA mondatban a WGS84-hez viszonyított távolság szerepel. Az akár másodpercenként rögzített adatokat kinyerve a log fájlokból, a szoftver elkészíti a *.gpx* kiterjesztésű fájlokat, amelyek felhasználhatóak az útvonal kirajzolásához. A .gpx fájlok a GPS adatok szabványos tárolási formája.

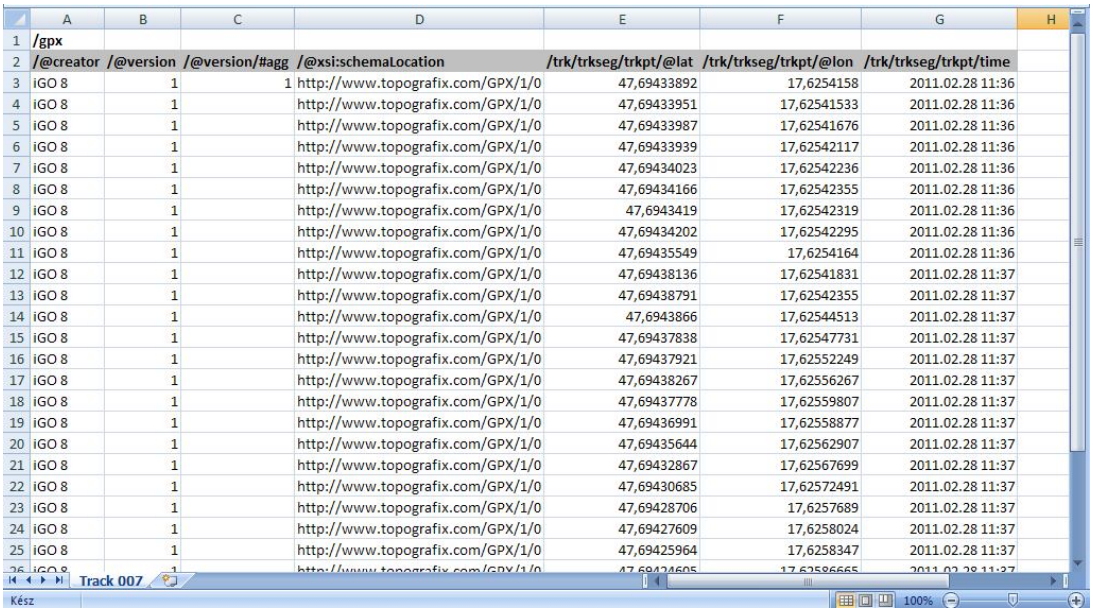
GGA MONDAT (GLOBAL POSITIONING SYSTEM FIX DATA)



7. ábra. GPS GGA mondat szerkezete Készítette: Répás József 2011-03-04

.GPX FÁJLOK FELDOLGOZÁSA

A .gpx típusú fájlok megnyitására alkalmas a Microsoft Excel nevű táblázatkezelő program, amelyben láthatjuk, hogy melyik időpontban milyen koordinátájú helyen voltunk.



	A	B	C	D	E	F	G
1	/gpx						
2	/@creator	/@version	/@version/#agg	/@xsi:schemaLocation	/trk/trkseg/trkpt/@lat	/trk/trkseg/trkpt/@lon	/trk/trkseg/trkpt/time
3	iGO 8	1	1	http://www.topografix.com/GPX/1/0	47,69433892	17,6254158	2011.02.28 11:36
4	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69433951	17,62541533	2011.02.28 11:36
5	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69433987	17,62541676	2011.02.28 11:36
6	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69433939	17,62542117	2011.02.28 11:36
7	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69434023	17,62542236	2011.02.28 11:36
8	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69434166	17,62542355	2011.02.28 11:36
9	iGO 8	1		http://www.topografix.com/GPX/1/0	47,6943419	17,62542319	2011.02.28 11:36
10	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69434202	17,62542295	2011.02.28 11:36
11	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69435549	17,6254164	2011.02.28 11:36
12	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69438136	17,62541831	2011.02.28 11:37
13	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69438791	17,62542355	2011.02.28 11:37
14	iGO 8	1		http://www.topografix.com/GPX/1/0	47,6943866	17,62544513	2011.02.28 11:37
15	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69437838	17,62547731	2011.02.28 11:37
16	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69437921	17,62552249	2011.02.28 11:37
17	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69438267	17,62556267	2011.02.28 11:37
18	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69437778	17,62559807	2011.02.28 11:37
19	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69436991	17,62558877	2011.02.28 11:37
20	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69435644	17,62562907	2011.02.28 11:37
21	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69432867	17,62567699	2011.02.28 11:37
22	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69430685	17,62572491	2011.02.28 11:37
23	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69428706	17,6257689	2011.02.28 11:37
24	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69427609	17,6258024	2011.02.28 11:37
25	iGO 8	1		http://www.topografix.com/GPX/1/0	47,69425964	17,6258347	2011.02.28 11:37

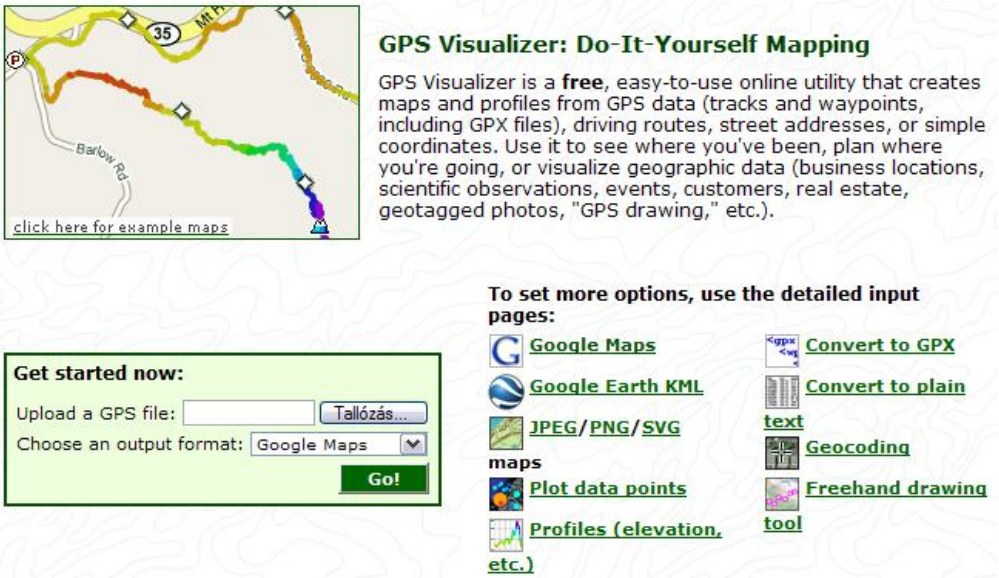
Track 007

Kész

100%

8. ábra. 007-es útvonalfájl megnyitása Microsoft Excel táblázatkezelővel
Készítette: Répás József 2011-03-05

Léteznek olyan alkalmazások, amelyek a *.gpx* kiterjesztésű fájlokat átkonvertálják egyéb formátumokra, hogy más programok számára is értelmezhetőek legyenek. Ilyen formátum például a Google Earth *.kmz* kiterjesztésű fájlja. Egyik szabadon használható alkalmazás a www.gpsvisualizer.com oldalon található, ami Google térképre is felrajzolja az útvonalat.



9. ábra. www.gpsvisualizer.com oldal főoldala Letöltve: 2011-03-05 0:42

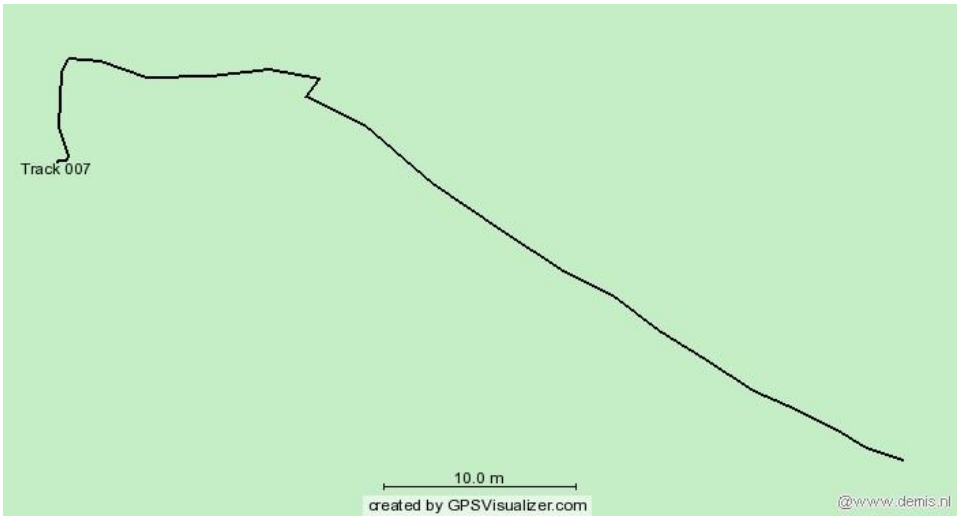
Legegyszerűbb és leggyorsabb módja az útvonal felrajzolásának, ha a Tallózás gombra kattintva kikeressük a *.gpx* kiterjesztésű fájlunkat, beállítjuk a kimeneti formátumot, majd a GO! gombbal elindítjuk a rajzolást. A kimeneti formátum lehet Google Maps, PNG képfájl, JPEG képfájl, vagy szöveges dokumentum is.

.GPX ÚTVONALFÁJL MEGJELENÍTÉSE

type	time	latitude	longitude	name	desc
T	2011-02-28 11:36:42	47.6943389	17.6254158		Track 007
T	2011-02-28 11:36:44	47.6943395	17.6254153		
T	2011-02-28 11:36:46	47.6943399	17.6254168		
T	2011-02-28 11:36:48	47.6943394	17.6254212		
T	2011-02-28 11:36:50	47.6943402	17.6254224		
T	2011-02-28 11:36:52	47.6943417	17.6254236		
T	2011-02-28 11:36:54	47.6943419	17.6254232		
T	2011-02-28 11:36:56	47.6943420	17.6254230		
T	2011-02-28 11:36:58	47.6943555	17.6254164		
T	2011-02-28 11:37:00	47.6943814	17.6254183		
T	2011-02-28 11:37:02	47.6943879	17.6254236		

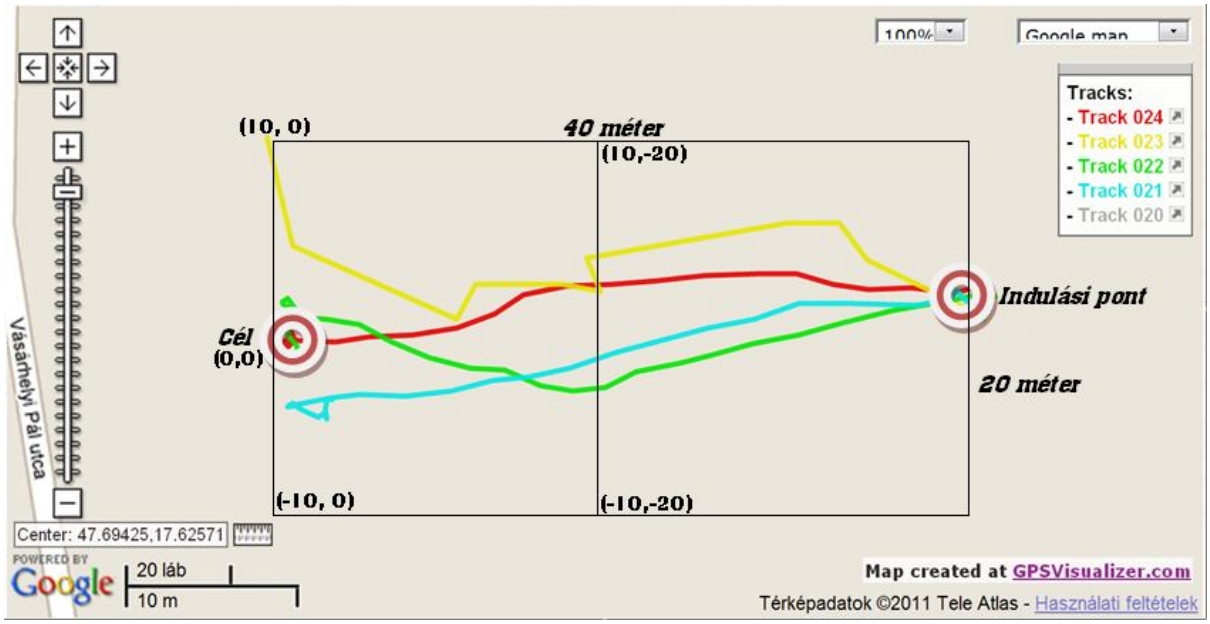
10. ábra. Track 007-es útvonalfájl Készítette: Répás József 2011-02-28

A 10. ábrán jól látható, hogy az egyes időpontokhoz milyen koordináták tartoznak. Ennél a fájlnál a rögzítés 2 másodpercenként történt. A 11. ábra az útvonalat mutatja. A méretskála alapján látható, hogy egy adott szakasz hány méternek felel meg a valóságban.



11. ábra. Track 007-es útvonalfájl Készítette: Répás József 2011-02-28

A 12. ábrán jól látható, hogy az útvonal a Győri Széchenyi István Egyetem területén, a Vásárhelyi Pál utca felöli oldalon lett rögzítve. Ez a terület az egyetem udvari kézilabdapályája.



12. ábra. Track 020-024-es útvonalfájl megjelenítése Google Map-en Készítette: Répás József 2011-04-05

Az 12. ábrán látható, hogy a Track024-es útvonalon sétáló alany, szinte teljesen egyenesen ment az indulási ponttól a célig és mindössze 34 másodperc alatt, csupán 0,5 méteres eltérést produkálva, míg a Track022-es egy hosszabb, nem egyenes útvonalon ért el 37 másodperc alatt pontosan a célba. A másik két alany jelentős (8,5 és -3,4 méteres) eltérést produkált. Az eredményeket egy táblázat tartalmazza, kiegészítve a vizsgált alanyok egyéni jellemzőivel, mint a kor, nem, hogy jobb- vagy balkezesek-e illetve, hogy látókkal vagy látássérültekkel végeztük-e a feladatot. Az első néhány eredményt az alábbi táblázat tartalmazza: 1. táblázat.

Monogram	Nem (F-1;N-0)	Kor	Kéz (J-1; B-0)	Látó-1/Vak-0	Csipogás		Zaj		Vak		
					Idő	Eltérés	Idő	Eltérés	Idő	Eltérés (X)	Eltérés(Y)
K. P.	1	21	1	1	46	0	41	0	33	10	-1,4
									31	-3,4	0
V. Á.	1	21	1	1	68	0	54	0	35	-10	-5,3
									37	0	0
M. L.	1	22	1	1	61	0	56	0	43	-10	-3,9
									47	8,5	0
L. Z.	1	21	1	1	50	0	45	0	36	-2,6	0
									34	-0,5	0

1. táblázat. Az eredmények rögzítésére szolgáló táblázat Készítette: Répás József 2011

A táblázat első oszlopában láthatóak az alanyok monogramjai, mellette a nemük, koruk, jobb vagy balkezességük, látásuk. Ezt követi az elvégzett feladatok típusa, ideje és az eltérések. A csipogással és zajjal történt vizsgálatok esetén, ha az alany célba ért, akkor az eltérése „nulla” vagyis az alany célba ért, karnyújtásnyira megközelítette a hangszórót. A kísérlet során először hang nélkül, aztán csipogással (click-train gerjesztés), majd fehérzajjal, végül ismét hang nélkül mértem. A hangforrás nélküli vizsgálat esetén több próbát is végeztem, ezt az egymást követő sorokban tároltam.

Eddig 41 látóval végeztem kísérletet, az ő eredményeik láthatóak a második táblázaton, amely részletezi a vizsgált alanyok számát a nemük szerinti, látásképességük szerinti és jobb-, bal kezességük szerinti felosztást. Az időeredményekből és eltérésekből maximumot, minimumot, átlagot és szórást számoltam. A kísérletben 15 nő és 26 férfi vett részt, 20 és 83 év közötti korosztályból vegyesen.

A vakon, hangforrás segítsége nélküli eredmények a 2. táblázat tartalmazza. A 3. és 4. oszlopból leolvasható, hogy a legnagyobb eltérés az alapvonalon jobb és bal irányba is 10 méter volt, az oldalvonalon való áthaladás már 21,7 méternél volt. Ebben az esetben az alany a félpálya vonalán sem haladt át, máris elhagyta a pályát oldal irányban. A táblázatból leolvashatóak még az átlagos út, idő és sebességértékek, valamint a szórások is.

	Idő	Eltérés (X)	Eltérés(Y)	Út	Sebesség
Maximum	63	10	0	90	2
Minimum	18	-10	-21,7	24	0,709090909
Átlag	37,1025641	-0,13717949	-4,25897436	46,027027	1,269797086
Szórás	9,12480527	7,68863403	6,235267017	10,9806467	0,228520089

2. táblázat. Hangforrás segítsége nélküli eredmények Készítette: Répás József 2011

Összevetve az eredményeket már kevés eredmény alapján is látszik, hogy az egyenestartás tanulható folyamat. A vakon, hangforrás segítsége nélküli feladatokban a második próbálkozásra mindenki jobb eredményt ért el. Azon alanyok 90 %-a, akik első körben nem érték el az alapvonalat, második próbálkozásra mind elérték az alapvonalat és átlagosan 5 méteres eltérésen belül teljesítettek. Zajjellel való mérés esetén az eredményeket a 3. táblázatban látható.

	Idő	Eltérés	Út
Maximum	73	0,5	72
Minimum	26	0	30
Átlag	43,35	0,017857	50,5405405
Szórás	10,0218991	0,094491	8,52641189

3. táblázat. Zajjellel való mérés Készítette: Répás József 2011

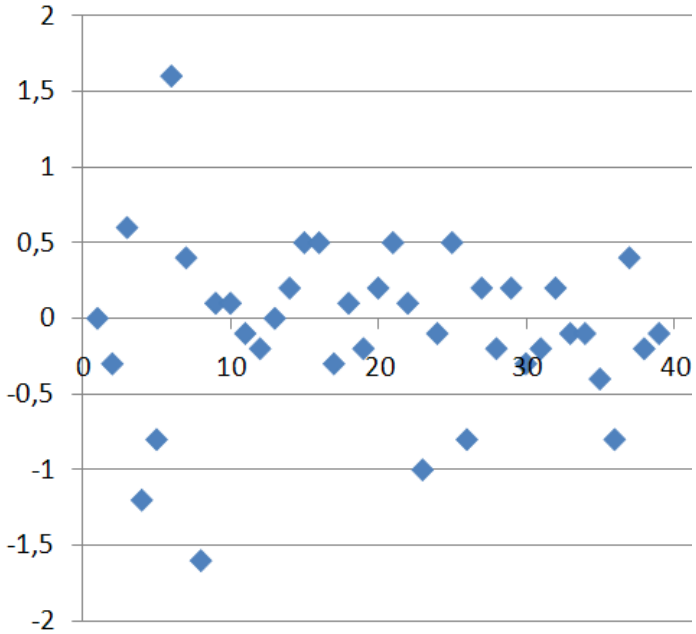
A 4. táblázatban a Click train gerjesztéses kísérlet eredményei találhatóak. Ennél a kísérletnél egy alany volt aki nem ért célba, 2,5 méteres eltérést produkált.

	Idő	Eltérés	Út
Maximum	72	2,5	65
Minimum	31	0	33
Átlag	47,15	0,073529	49,1891892
0	9,06825966	0,428746	7,17185021

4. táblázat. Click-train gerjesztéses kísérlet eredményei Készítette: Répás József 2011

A csipogás és fehér zaj közt eredményekben nincs számottevő különbség az időkben, eltérés pedig nincsen, egy kivételével mindenki célba ért. A kivételes esetben valószínűsíthető a hallás erős romlása. Az alanyok a hangforrástól 5-6 méterre kezdtek el bizonytalanná válni, nem érezték, hogy meddig mehetnek, nem tudták milyen messze lehet. A pityegést körülbelül a félpályától tudták beazonosítani az alanyok, ellentétben a fehér zajjal, amit az induláskor hallottak jobban, majd közeledve egyre jobban szétterült, illetve a szél is jobban befolyásolta a hallhatóságot.

A harmadik feladatban az alanyoknak az egyetem melletti parkolóház oldalfala mellett kellett bekötött szemmel, a vakok által is használt fehér bot segítségével érzékelni az épület sarkát. Ebben a feladatban 20 alany vett részt, gyakorlás után két próbát tettek. Különböző távolságokból indulva az alanyok kopogtatással, a falról visszaverődő hangokból próbáltak különbséget tenni aközött a két hangtípus között, amit a fal mellett és a falat elhagyva hallottak. A produkált eltérésekből maximumot, minimumot és szórást számoltam.



13. ábra. Sarokérzékelésnél elért pontosság Készítette: Répás József 2011

Az eredményekből következtetést egyelőre nem lehet levonni, mert kevés volt a vizsgált alanyok száma, illetve nagyon eltérő eredményeket produkáltak. A 10. ábrán látható, hogy volt, aki pontosan eltalálta a sarok hollétét (minimum érték), de nem volt ritka az egy méternél nagyobb eltérés sem. Az eltérések szórása 0,56 méter volt, a legnagyobb eltérés +/- 1,6 méter volt, ebben az esetben az alany elmondása alapján nem tudott különbséget tenni, inkább csak kitalálni próbálta, hogy hol lehet az épület sarka.

ÖSSZEFOGLALÁS

A megtervezett és végrehajtott kísérletek eddigi eredményei alapján elmondható, hogy ezekkel a módszerekkel alapos összehasonlítások tehetőek a látók és látássérültek között. Az elkövetkezendő időszakban már látássérültek is részt vesznek a kísérleteken, így nem csak a látók képességeinek vizsgálatra lesz lehetőségem.

Felhasznált irodalom

[1][2] Wersényi György: Térbeli hallás BME-TTT oktatási segédanyag 1-4. oldal 1998. http://vip.tilb.sze.hu/~wersenyi/Terbeli.pdf Letöltve: 2011-03-30 14:56

[3] Tömösközi Katalin – A látássérült emberek világa http://www.ringmagazin.hu/index.php?option=com_content&view=article&id=2958:a-latasseruelt-emberek-vilaga&catid=172:esely&Itemid=476 Letöltve: 2011-02-03 16:11

[4] Észak-Magyarországi Látássérült-rehabilitációs Központ internetes bemutatkozó oldala http://www.latasrehab.hu/ Letöltve: 2011-03-11 17:11

[5] Dávid Andrea, Dr. Gadó Márta, Csákvári Judit „*Látássérült emberek elemi és foglalkoztatási rehabilitációja"19. old. 2008* ISBN 978-963-87899-6-9

[6] Vak logo Forrás: http://topnews.in/health/files/blind.jpg Letöltve:2011-03-05 16:02

[7][8][9] Emberi test. 1. vol. Szerk.: OBÁL Ferenc, Bp.: Gondolat Kiadó, 1982. pp. 352. 439. 472. oldal ISBN 963-281-068-6

[10] A szem felépítése Forrás: http://www.lelekgyogyaszat.hu/szem.JPG Letöltve: 2011-03-05 14:57

[11] Laurent A. Renier, Irina Anurova, Anne G. De Volder, Synnöve Carlson, John VanMeter, Josef P. Rauschecker,"*Preserved Functional Specialization for Spatial Processing in the Middle Occipital Gyrus of the Early Blind*", Neuron, Vol. 68, No. 1, pp. 138-148, 2010 October

[12] Borsics József,*" Agyi plaszticitás - a vakok látókérge részt vesz a hallásban és a tapintásban „,* http://www.mrns.hu/index.php?page=content/hirek.php&nid=279 2011-02-03 15:07

[13] T. Miura, T. Muraoka and T. Ifukube, "Comparison of obstacle sense ability between the blind and the sighted: A basic psychophysical study for designs of acoustic assistive devices," *J. of the Acoust. Science and Technology Japan (AS&T)*, vol. 31, no. 2, pp. 137-147, 2010.

[14] C. Muchnik, M. Efrati, E. Nemeth, M. Malin, and M. Hildesheimer, "Central auditory skills in blind and sighted subjects," *Scandinavian Audiology*, vol. 20, no. 1, pp. 19–23, 1991.

[15] H-H. Lai, and Y-C. Chen, "A study on the blind's sensory ability," *International Journal of Industrial Ergonomics*, vol. 36, no. 6, pp. 565–570, 2006.

[16] M. Supa, M. Cotzin and K. M. Dallenbach, " „Facial vision": The perception of obstacles by the blind," *American Journal of Psychology*, vol. 57, pp. 133–183, 1944.

[17] M. Cotzin, and K. M. Dallenbach, ”„Facial vision”: The role of pitch and loudness in the perception of obstacles by the blind,” *American Journal of Psychology*, vol. 63, pp. 485–515 1950.

[18] F. A. Bilsen, and R. J. Ritsma, ”Some parameters influencing the perceptibility of pitch,” *J. Acoustical Soc. Am.*, vol. 47, no. 2, pp. 469–475, February 1970.

[19] Y. Ando, and H. Alrutz, ”Perception of coloration in sound fields in relation to the autocorrelation function,” *J. Acoustical Soc. Am.*, vol. 71, no. 3, pp. 616–618, March 1982.

[20] J. M. Kates, ”A central spectrum model for the perception of coloration in filtered gaussian noise,” *J. Acoustical Soc. Am.*, vol. 77, no. 4, pp. 1529–1534, April 1985.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Seres György - T. Fórika Krisztina - Miskolczi Ildikó - Sz. Lengyel Piroska - Gerő Péter - Pálinkás Yvette

drseres@drseres.com – krisztina@forika.hu – miskolczi.ildiko@gmail.com – l.piroska@t-online.hu – gp.project@gmail.com – palinkas.yvette@gek.szie.hu

A CLUB FOR E-LEARNING RESEARCHER - EDUCATORS IN THE CLOUDSSOME ASPECTS OF E-LEARNING

Absztrakt

Működik Magyarországon egy online e-Learning club oktatók számára. A klubtagok különböző felsőoktatási intézményekben oktatnak. Tapasztalataikat, eredményeiket több mint 3 éve osztják meg egymással. Az első írásban az egész életen át tartó és az egész életre kiterjedő tanulás formális és nem formális módjairól írnak a szerzők. A második cikk az élethelyzethez igazított tanuláselveiről és módszereiről szól. Harmadikként bemutatatásra kerül, hogy hogyan vált az elektronika az oktatás tárgyából és eszközéből annak színterévé. A negyedik írásban az élménypedagógia kerül elemzésre. Az ötödik írásban a szoftverrobotok oktatásban történő alkalmazhatóságáról olvashatunk.

There is an online Club for e-Learning researcher-educators in Hungary. Members of the Club are lecturers in different Universities and Colleges. They research some aspects of e-Learning together since more than three years. First aspect is coherency of lifelong and life-wide learning – formal and/or informal sides of e-Learning. Second one is life-tailored learning – principles of the new methodology–, competence-oriented methods and culture using of technology and virtual classrooms. Third aspect is progress of technological environment of e-Learning – how did electronics turn from subject and tool of education to scene of education? Fourth topic is method of the experience pedagogy in e-Learning – motivation for learning, commitments, attitudes, personalities, interactive teaching materials and learning by enjoying. Last research line of members is application of software robots in e-Learning – searching robots, translating robots, text recognition robots, speech recognition robots, plagiarism-recognition robots, simulators, tutor robots.

Kulcsszavak: *felhőtanulás, egész életre kiterjedő tanulás, élethelyzethez igazított tanulás, élmánypedagógia, szoftver robotok ~ cloud learning, lifelong learning, life-wide learning, life-tailored learning, experience pedagogy, software robots*

INTRODUCTION BY GYÖRGY SERES

There is an online SysAdminLess Club for e-Learning researcher-educators in Hungary. Permanent members of the Club are lecturers in different Hungarian Universities or Colleges. They are authors of this study.

We research some aspects of e-Learning since more than three years:

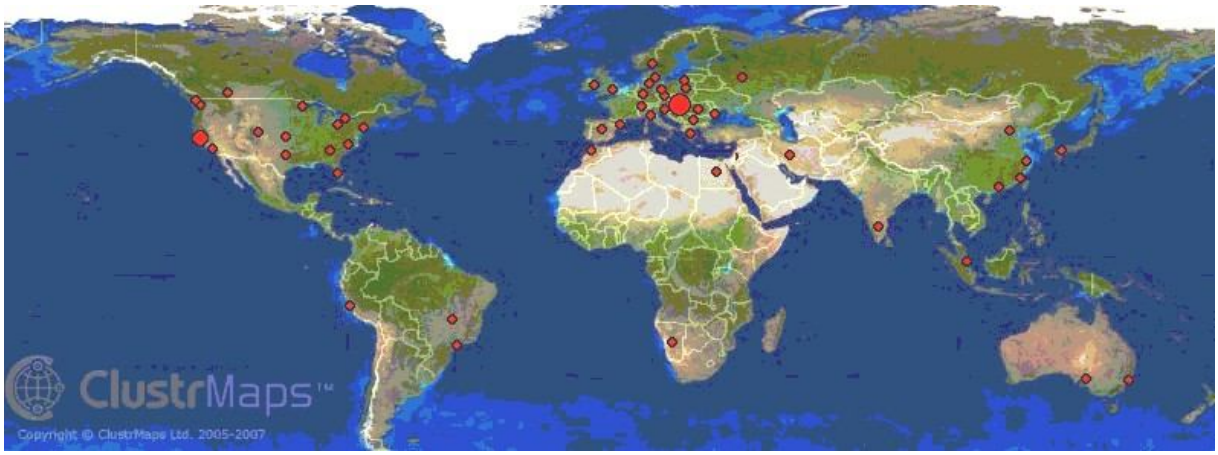
- progress of technological environment of e-Learning;
- method of the experience pedagogy in e-Learning;
- coherency of lifelong and life-wide learning;
- opportunity of application of software robots in e-Learning;
- life-tailored learning.

Short story of the Club

A doctoral topic – „*Use of e-Learning and distance learning in military higher education*" – and a curriculum – „*IT bases of interactive e-Learning and d-learning*" – has been called at PhD School on Military Technology of Zrinyi Miklos National Defence University (ZMNDU) in 2007 year.

Because the 10 years old personal homepage[1] was unable for interactive distance learning, that's why a new Drupal engine based Web 2.0 portal has been created – named E-TEACHER[2].

The new portal has been discovered by great searching providers without any advertisement, and many – more than 5000 – quests were directed by them to the portal from the entire world



1. figure. Visitors' map of our portal[1]

A distance e-Learning course has been called on the new portal by called curriculum "*IT bases of interactive e-Learning and d-Learning*". Many people begun the course – and some of them have successfully performed it. Four persons from them report for doctoral student at PhD School on Military Technology of ZMNDU successfully.

A six person's researcher team came into being as an outcome of the course. All of us are lecturers in different Hungarian Universities or Colleges. All of us have individual personal

[1] http://drseres.com
[2] http://drseres.com/elearning

homepage and professional educational portal without system administrators. That's why we established SysAdminLess Club and the portal was altered to blog form[3].

Permanent members of the club meet weekly on Skype, on WiZiQ or other virtual classroom among the Clouds. A lot of individual and common publications, lectures at scientific conferences, applications and awards and four individual Moodle portals[4] were born as a result of our meetings.

And we learn so much from one another.

Research topics

Members of the Club research some aspects of e-Learning since more than three years.

First aspect is coherency of *lifelong and life-wide learning* – formal and/or informal sides of e-Learning.

Second one is *life-tailored learning* – principles of the new competence-oriented methodology, methods and culture using of technology and virtual classrooms.

Third aspect is progress of *technological environment of e-Learning* – how did electronics turn from subject and tool of education to scene of education?

Fourth topic is methods of the *experience pedagogy in e-Learning* – motivation for learning, commitments, attitudes, personalities, interactive teaching by four levels of e-Learning curriculum and learning by enjoying.

Last research line of our members is *opportunity of application software robots in e-Learning* – searching robots, translating robots, text recognition robots, speech recognition robots, plagiarism-recognition robots, simulators, tutor robots.

What are our results in researched by us topics?

LIFE-WIDE LEARNING LIFELONG – BY ILDIKÓ MISKOLCZI

In the 21st century there is more and more knowledge. This is increasingly more difficult to make the process of reception and processing of the user. However, the knowledge becomes the very quickly obsolete, so the renewal time of the knowledge is less and less. We want to know more and more in less time. In a specific field of knowledge "up-to-date", complex way, however, many-to-know knowledge applied, which means the significantly increased the length of time in learning.

Change of factors of learning

Technical development

However strange it may seem, but if we research on the development and the appearance of distance learning, we have to search for its roots in the correspondence course. According to some researchers, the founder of the correspondent education was St. Paul, [1] who has made his clerks write his doctrines and made his messengers spread his teachings. The papyrus was massive product were so it could take the long-distance transport well. St. Paul "has also used a certain degree of interactive items" in his written messages to ensure that his words get into the thought of the followers. He put rhetorical questions in his texts (and even

[3] http://drseres.com/elearning

[4] http://miskolczi.net/moodle , http://forika.hu/moodle , http://www.lengyelpiroska.hu/moodle , http://www.geropeter.hu/moodle

he replied to them). So he has broken the monotonous tune of the written text. These questions-answers had claimed to continue the thinking of the raised thoughts.

Opinion and research result of authors about technical development of learning in 20th century see in chapter 3.

Changes in the needs of society

"In the second half of the 20th century, however, not only science, technology, but society, and the economy have also begun a fast development, and because of this, the knowledge that we obtain in the schools become obsolete in our active life many times, so that we have to start to learn again and again if we want to save our competitiveness on the labor market. At the end of the 20th century, it has been born the concept of 'lifelong learning'[5] [2].

Development of info-communication technology (ICT) and significantly changing social needs have effected on the attitude of the people to the knowledge and learning in the third part of the last century.

Today, there is no doubt that the lifelong learning, more specifically, the extending of it to each part of our life is the necessary coefficient of our life. We have renewed our knowledge always to adapt to the evolving changing economic conditions and social expectations – it is essential in the sense in the globalised world. Beyond the individual, personal demands the constraint is often the reason for a continuous learning process as it is in the 21st century's accumulated knowledge that are produced by hyper-society – information has increased almost exponentially from hour to hour. However, a factual knowledge can very quickly become obsolete on any territory/special field of life.

Changes in the methodology of education

The eLearning

In the second half of the 21st century, at the end of the 1960s, the beginnings of eLearning were appeared. In the 1970th were already operating networks specifically for higher education (PLATO, TICCIT). The modern ICT supported education has been developed from the end of the 1980th – that formed eLearning, what can change the learning process and the methodology of teaching fundamentally.

"The nice new world of e-Learning is virtuality *just so it's only an opportunity, potential a reality ... It is the virtual reality of pedagogy*."[6] [3]. Today, probably he thinks himself otherwise these lines, a part of them. Today e-Learning is not only a possibility, not only virtuality. Here is an integral part of our everyday life. *"Virtual reality of the pedagogy"*-type Komenczi. So I would say: the virtual world of pedagogy is the reality.

The opportunities, giving by eLearning, make today's pedagogical practices wider and more colorful. More and more elements of it are displayed and continuously incorporated into the training attendance (joint learning, blended learning), as well as in a large part of the distance learning. In the regular training and in non-formal education systems both, the application of it spread quickly. Today's N-generation, or digital generation, who has already increased by up to life was not in a section, when you do not have a computer, internet, take for granted and require the application of modern techniques, technologies in the field of education too.

The dominance and spread of electronic devices in the education means that we won't talk about *"learning"* and *"eLearning"*. The "*e"* prefix will disappear quickly from this form of

[5] Translated by author.
[6] Translated by author.

education, because the electronic education, e-Learning, as a form of learning will become usual, natural.

The networked learning

The networked learning as a technique is significant, because with the help of technically a specially developed electronic learning curriculum, the eLearning (necessarily), students don't go ahead in the curricula in a linear way, but also the construction of the digital curriculum allows that students explore the existing context independently.

However, the networked learning not only means the structure of the curriculum, but the possibility (and need) to advance knowledge can be reached, not only from the syllabus but with the using of additional resources (which are attached to it), and which are found somewhere in the virtual space. A virtual learning environment, closed, or the World Wide Web can be the stage or incarnate of this network.

The cloud-learning

The formation of a cloud-learning practice is over the past two years a revolutionary new opportunity for education-methodological issues. From education-technical point of view, I see the importance of it that can allow eliminating the space and time limits and the lack of the presence of personal trainers in the educational system. Virtual consultations, virtual conferences, can be created by the Internet service providers. Thus, the learning support will be not only modern, but also interactive. The services of the cloud support not only the learning of individual student, but it also give thumbs up the teacher and student exchanges. In addition to the individual learning, group learning can also be taking shape.

The networked Learning in a connectivity way

The fundamental principle of connectives means that we view the knowledge, as a network, the minimum elements of which are the nodes in our network. These could be the conceptual definitions, phrases, definitions, any elementary knowledge. The extremes among them are those relationships, with which we connect the nodes. In this sense, learning may mean two things:

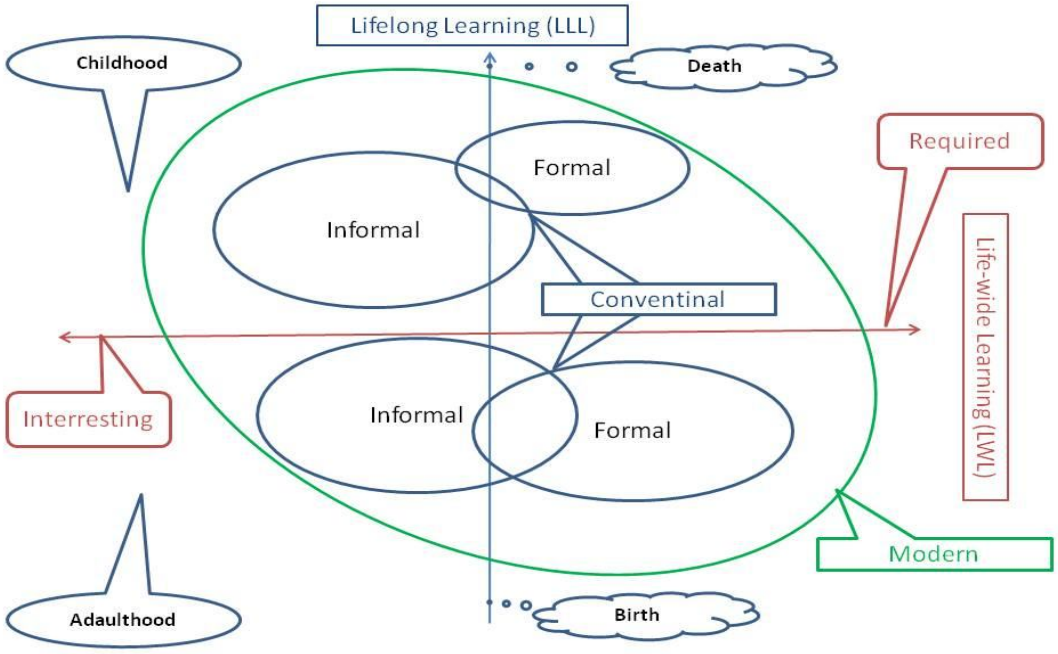
- - new nodes to be connected to the fabric
- - reordering the net connections.

The high-profile (connecting with many edges to other nodes) nodes determine our thinking. The connectivity view determines the learning process and its relevance in the opportunity of the construction of the knowledge network and its restructure on demand. Thus, our knowledge increases changes constantly through the established network connections. The network research deals with the examination of this new paradigm which is also a method and an approach. The network research, on a micro level, examines the relationships between things, and on a macro level, samples, that drawn by the connections [4].

Life-wide learning

Needs of the lifelong learning (LLL) is basic from view of point of economy and society in the 21st century. To become a good technician and potential worker is not enough to learn a job when we are young. All life we have to learn that can be professionally recognized. The economic and financial crisis in the world, the changes in societies are demand not to know only one thing, but we are able to stand other areas of life is our place. This is the concept of the whole of life learning, covering the all territory of life (life-wide learning, LWL). The

interpretation of KOMENCZI [5]: the LLL is at the same time, and the contents of the LWL are determined by the content of the thinking (life-wide learning) in the 21st century. We can see the contents of throughout the life-wide learning (LLL and LWL) context on the Figure 2.



2. figure. The whole life-wide learning model (by Ildikó Miskolczi)

In the 21st century there is more and more knowledge. This is increasingly more difficult to make the process of reception and processing of the user. However, the knowledge becomes the very quickly obsolete, so the renewal time of the knowledge is less and less. We want to know more and more in less time. In a specific field of knowledge "up-to-date", complex way, however, many-to-know knowledge applied, which means the significantly increased the length of time in learning.

LIFE-TAILORED LEARNING – BY PÉTER GERŐ

Life-Tailored Learning [6] is one of the educational methodologies available for adults to support their learning. It is a sequence of methods and instructions (a practical guideline) to help with planning, organizing, carrying out, evaluating as well as governing knowledge acquisition and its transfer. It is a learning-teaching technology, which describes the learning process step by step, starting by assessing the learning needs, identifying whether entrance requirements / criteria are met through developing the professional content, structuring the learning content into modules as well as defining the roles of the student, teacher, consultant, tutor, mentor, all leading up to the closing evaluation (exam).

Adult learners usually learn with a more specific goal in mind. Further characteristic is that there are big differences between certain learners' recognitions and circumstances. Besides the adult students' learning patterns are also different: they differ from one another's and from the patterns which can be observed in case of children. In other words: people with different existing knowledge and motivation, living in different circumstances have to achieve particular learning aims.

Life-Tailored Learning is a learning technology developed for cases, where the exclusive aim of learning is to reach the adult learners own, measurable goals.

The fundamental idea of the methodology is that by knowing the goal of learning it is possible to reveal the necessary studies for the given student (to expand his/her preliminary knowledge, studies, and existing competences). With the help of this information we can choose (considering the given student's situation, possibilities, schedule etc.), from the huge number of known means, methods and sources, the ones that are the most effective in case of a given learner. The student, guided by the adequate teacher, goes through the planned learning process.

The "learning with a more specific goal and expectation" is considered to be a learning in order to get new and expand existing competencies. From the various interpretations of competency we use the one that also includes the motive system that serves the given function beyond the ability to apply. Regarding to the final tests and assessments the question naturally arises whether legitimacy and entitlement should be included, but they are not strongly connected to pedagogy so in terms of the methodology we do not consider them as part of the concept definition.

The principles of the methodology and the course by the methodology of Life-Tailored Learning

The methodology of Life-Tailored Learning is a practical guideline proceeded from the above mentioned. Its structure is defined in the following way.

- The process should be divided into different steps that are connected to the individually defined parts of the learning aim.
- Entry and completion requirements should be defined to each step.
- The specialized material (the content of learning: the gap between the entrance and completion conditions of the given step) and the learning material (the specification of the learning devices and methods) should be separated.
- The development process should be divided into steps so that we do not advance to the next without having cleared the preconditions, and if we make a mistake we should only take one step backward. That is to say every step includes the supervision of the previous step (we should only be able to complete each step successfully, if we proved that we successfully finished the previous step).

Within this: the methodology chooses from the methods and devices from the point of view of practicality, leaving place to possible additions in the future.

Forms of Life-Tailored Learning

- university coursebook, and training for learning content development and learning assistance activities;
- learning content and learning assistance system to help attain the desired, envisaged competence;
- in mobile version: a workstation (in accordance with log-in there can be a student, teacher, author... and so forth workstations) [7];
- virtual classrooms in the clouds of internet .

There are various technological and methodological tools for a properly designed distance learning process or computer assisted learning in different life situation.

CLOUD LEARNING – BY KRISZTINA FÓRIKA

Tool of education last century – how did electronics turn from subject and tool of education to scene of education?

Start of Public Radio and TV broadcast made the electronics new important *subject* of education in 20th and 30th of the last century.

Spreading of schools' broadcast and the school televisions' made the electronics *tool of public education* in 40th, 50th and 60th.

Electronics became *tool of education in schools* when audio and video recorders' and PCs' price turned into one which can be reached in 70th and 80th.

But the wide-ranging application of the internet and the fast internet availability leads to a big breakthrough in the 90th and in the 1st decade of the new millennium. Any kind of curriculum became accessible for *anybody, anywhere and anytime under real time* with help of digital audio or video recording and broadband data transfer on the internet. [8]

So, the building of eLearning, the Internet has been built. There is the situation, when electronics turned from subject and tool of education to *scene of education*. The computers – the most modern desks – are ready to welcome students. All the imaginable and unthinkable forms of demonstration multimedia devices – as blackboards – and presentation software – as boxes of chalk – are available for teachers.

Clusters for e-Learning

Running of increasingly more complicated application programs, transfer and storage of increasingly more data files and more speed of data transfer or processing make ore hardware and software demand on users and providers. It is the recognition, which born service of Computing techniques like Cluster-, Grid-, and Cloud computing. These distributed environments should promote high cooperation and effective e-Learning. We can be aware that grid computing, cluster computing and cloud computing are all terms closely interrelated with each other. In order to give the most appropriate definition of cloud computing we have to start with looking at cluster computing. During the last three decades of the last century in the field of low-cost high-performance microprocessors, high-speed networks and distributed computing has inspired many researchers to diverge from expensive and specialized parallel supercomputers towards cheaper and general purpose clusters [9].

The cluster concept is, that the implementation of the programs picked in a parts which can perform at the same time with each other in a separate processor. Thus, the processing of programs on 'n' processors can also be up to 'n' times faster. In the cluster more, then one processor use the same memory and bus system within a single computer. The cluster interconnection network speed is dedicated, high-end with low latency and high bandwidth. The applications are associated with science, business, enterprise computing, based on data centres. In addition to the scientific cluster applications in 90's emerged clusters to support e-Learning. The e-Learning cluster in general has the goal of researching and advancing the state of the art in learning techniques on the application, and use, of semantic technologies with particular emphasis. Sometimes schools are establishing a collaborative and innovative learning community that engages learners in inquiry and cutting edge pedagogy through meaningful participation and contribution in their global community, like Eastern Block e-Learning cluster [10].

Grid computing in education

From the early 2000's the grid computing became a popular term, and the application has started in the e-Learning. This technology has been applied to computationally intensive scientific, mathematical, and academic problems through solving large-scale and data intensive computing applications. Grid computing is used in commercial enterprises for such diverse applications as molecular modelling for drug design, economic forecasting, seismic analysis, brain activity analysis, and high energy physics, and e-Learning. Learning grids provides the flexibility and opportunities to reach out to a much larger audience. Schools and institutions have been using it to complement their existing classroom lectures. e-Learning grid allows information and learning contents to be shared or retained as proprietary materials for the individual school. It allows all users to interact and grow with the learning community, sharing ideas and ways to manage learning and project work [11].

Special educational Cloud Computing – the Cloud Learning

In 2007 after floating "Blue Cloud computing" planes IBM expand its leading a joint research initiative of 13 European partners to develop technologies that help automate the fluctuating demand for IT resources in a cloud computing environment. In 2008 cloud computing started gaining popularity and became emerging approach to shared infrastructure in which large pools of systems are linked together to provide IT services. We must to get acquainted with a new concept at begin of the 10th of the new millennium – it is the Cloud Computing [12].

Modern interactive education in our time can be up-to-date and cost effective if it takes up special educational Cloud Computing services and Community portals.

Cloud computing services tested by SysAdminless Club

Cloud Learning is a side of Cloud Computing technology which includes services of learning software, platform or infrastructure free or pay for use between the didactic organizations and the attendees. Our SysAdminless Club is a Hungarian community, which goal is to use Cloud Learning technology to providing free services to students, which include email, contact lists, calendars, document storage, creation and sharing documents, presentations, virtual classrooms etc. and support the effective lifelong learning. There are various services like this, which are tested by our team.

- Storage and share of the most often-used curriculums – documents – can be realized by a lot of service provider on the internet.
    - Most widespread are Google Docs and the Windows Office Live of Microsoft. Both of them are able for individual and shared editing various documents online with chat among editors.
- Storage and share of audio-visual curriculums – pictures and videos – is the oldest service of Cloud Computing after search providers.
    - Most popular is Picasa and Youtube, but Vimeo and Flickr portals are used by a lot of users too.
- Presentations are the most used tools in all forms and level of education, knowledge management and business. That's why a lot of service providers are specialized to storage and share of presentations.

- By our experiences the authorSTREAM portal warrants the most authenticable show of presentations like PowerPoint, but Slideshare and Scribd portals are popular in this service of Cloud Computing too.
- Novel, interesting and scenic presentations can be created, stored and showing online by a new portal Prezi – which is bring into being by Hungarian developer. Providers of storage presentations Google Docs and authorSTREAM permit of public or private show with parallel chat among presenter and audience.
- Conference call by Skype or Windows Messenger can be used for talking in the time of presentation too.

- Special services of WiZiQ and DimDim portals provide more lifelike feasibility for lectures which meets condition of virtual classroom.
  - They confirm smart board service with voice and video contact beside show of pictures, videos and presentations.
  - These portals provide to meet each other teachers and students in a topic of education as an addition special online TV portal Ustream permit of broadcasting a lecture from our webcam.
- Blogging – the trendiest service of Cloud Computing – can be used in education process too. Teachers and students can to keep a text or multimedia diary – blog – about their ideas, observation from curriculums, lectures, fellow students and teachers.
  - Posts on the most popular blog providers Blogger and Wordpress are text with pictures and links mostly. The tumblr portal usable embedding miscellaneous blog posts – text, picture and video.
  - Service of the Wallwisher portal can be used as a bulletin board of a class, because its editing is very simple.
  - More of Learning Management Systems – like Moodle or Ilias – provides blogging for its users.
  - Social contacts confirmed by community portals in Cloud Computing can be very useful for network based education.
- Learning Management Systems provide complex tools of e-Learning in the world of Cloud Learning.
  - There is some free software beside buyable and rentable systems of great firm – like Microsoft, Oracle, Adobe etc.
  - The most popular free LMS Moodle and Ilias are used by many Hungarian educational, business or government organization and individual teachers.
- More of provider of Cloud Learning offers tools for creating tests and self test.
  - Online questionnaires can be created with Google Docs, which are appreciable in common table after submitting.
  - More of virtual classroom services and LMS contain a lot of testing tools too.
  - Effective, interesting and scenic tests can be created with special software – like free Hot Potatoes and Quandary.

3. figure. Cloud Learning (by György Seres)

We have tested these Cloud Learning services by creating individual sub-domains at above providers.

EXPERIENCE LEARNING – BY PIROSKA SZ. LENGYEL

Educating in the virtual environment may only be fruitful, if we create high quality learning curriculum, following the differences in the individual cognitive styles and learning habits of the students, when relying on such learning methods, which will keep the students' interest alive, will motivate them for learning.

Moreover, the teaching/learning process, itself, has to follow the pedagogic principle of forming personalities in an appropriate way and developing abilities in an adequate way. Thus, the process is to aim at providing a convertible knowledge, a problem solving way of thinking in addition to the quantity of knowledge to be gained [13].

A set of e-books (Accounting of Subsidies, Introduction to the Accountancy, General Accounting, Taxation) having been compiled on the basis of the above principle is available (in Hungarian language) on the Moodle-portal of the author's home page[7].

4. figure. E-books compiled by the author[8]

[7] http://www.lengyelpiroska.hu/elkonyv.html

The methodology of the e-books are being relied, on the one hand, on the appropriate aspects of the knowledge management, the learning management, and on the aim at assisting students in finding and developing their own learning style, in order to obtain real knowledge, through a self-relied learning activity.

The e-books, on the other hand, are to present how to increase the students' motivation for learning, to develop their commitments, their positive attitudes, and their personalities by using state-of-the-art interactive teaching curriculum, by acknowledging their results performed and by rewarding them.

Furthermore, the e-books are inducing the students to accomplish a self-organised learning, supported by the Internet; however they are obliged to follow a disciplined and linear progress in the learning material. Due to the specificities of the learning material, the students, for the sake of the successful accomplishment, have to respect the offered order of a four-level progress:

- Level one (TO READ TO PREPARE YOURSELF): learning on their own, using "The learning material" module, which is easily readable and rich in multimedia devices.
- Level two (TO DISCOVER THE ESSENCE OF THE ISSUES): deepening the acquired knowledge by using the "Lectures" module.
- Level three (TO DEBATE TO CHECK YOUR KNOWLEDGE) checking the knowledge by using the "Practices" module which offers practice-oriented examples with an opportunity to work in teams and to debate the different problem-solving approaches.
- Level four (TO PERFORME TO FEEL THE SUCCESS) the "Stage" module, as the "level of play/action", serves for trying the practical application of the knowledge.

The e-curriculum, also, contain a set of practical works of different difficulty level. The opportunity of a random choice among them increases the probability of the successful problem solving, as well, which influences the competence sensation advantageously, while the successful solution of the works strengthens the self-confidence of the student/user, which is extremely important for both the intellectual health and the learning success, as well. A built-in program of the module evaluates the student/user's results promptly, thus the immediate feedback can contribute to confirm himself in his personality and to respect himself for his result achieved. From learning efficiency's point of view, it is exceptionally important for the student/user to release his own negative attitudes against himself, to have a healthy self-confidence and to realize, he is a valuable man.

Four levels of progress

Level one, i. e. the level of acquiring information, serves for a self-relied acquisition of the knowledge for the student, thus learning on his own. The module uses passive and active elements, supported by multimedia devices, for presenting the topics, illustrated by pictures, figures. The content, being split into information units, will form an organic entity, thus supporting the structuring of the acquired knowledge. The built-in guiding elements and feedbacks are encouraging the students/users for active learning and are, at the same time, directing, optimizing the learning process, adapting to the learning styles and mental standards of the students.

[8] http://www.lengyelpiroska.hu/elkonyv.html

Level two of deepening the knowledge is for learning with interaction and learning with teacher's cooperation. The lectures presented are fundamentally being relied on an illustrative-explanatory method. The essence of this method lies in visually presenting, modeling the topic, even playing it, to the extent possible, and commenting and explaining it in a short text. The advantage of the method, that it presents the topic in one shot and in its context, at the same time, while directing the students/users' attention to the message. Notwithstanding, the very key element of all learning action is the perception, the cognition. The progress made on his own, the self-relied development, is able to multiply the efficiency of the learning process. The activity and progress his own is a real, natural learning action. It is being fed by the student's curiosity and manifested in increasing desire for learning (observing, appraising etc.). One's knowledge, acquired in this way, can be recalled even in many years later.

Level three, the "Practice" module, serves to measure the level of acquisition of the knowledge. Both the teacher and the student/user receive a feedback on how and to what extent the latter has managed to acquire the learning material. The module serves for strengthening self-confidence of the students/users. Every student/user may choose out of the works with different difficulty level of the Practices, in accordance with his own assessment regarding the level of knowledge acquired by him/her.

Level four, could also be called the Stage (the acting level) emphasizes the importance of "the acting school" [14] the view that the "acting" is inevitable both for developing the thinking and for maintaining the interest. It gives an opportunity to the students to try how they can apply their knowledge in practice. The students/users choose a case study out of the "Practices", they prepare its script, then they present it, they "play the story" and show its possible solution.

The assessment of the student/user teams' presentations will be carried out, under teacher's guidance, in the framework of "a stage debate", prepared in advance according to appropriate appraising points.

The Stage gives the experience of joyful learning, it raises the lower status students/users' interest, too and increases their autonomy sensation. Its atmosphere, being characterized by cooperation, enhances the inner motivation, the long lasting maintenance of which may only be fruitful in such a learning environment, where the single elements, the "players" are strengthening and presupposing each other.

Successes of author's home page

The individual home page of author (http://www.lengyelpiroska.hu/elkonyv.html) has been developed and used for the purposes of college and university education for the last three semesters. Despite the relatively short time elapsed, the number of visits exceeded 19 000. The overwhelming part of users is students of Zsigmond Király Főiskola (King Zsigmond College) in Budapest. The acknowledgments received from students/users have been proving the successes of the above presented four level interactive learning curriculum and distance learning method, which combines the state-of-the-art online teaching with the most valuable characters of the traditional education.

SOFTBOTS IN E-LEARNING – BY YVETTE PÁLINKÁS

The software robots can be any kind of programs which replace human activities. Repetitive tasks can be solved by such speed which can't be done by humans. The word robot or bot has a bit wider meaning on the internet. It means mostly a program which is looking for any information on the Web.

I would like to highlight a few examples for software robots which can be used in higher education.

- Searching robots – such as Google, Bing and Yahoo – can traverse the Web automatically to build a big searchable database. Already they are indispensable for network-generation in learning.
- Translator robots – such as Google Translate, Morphologic or Babylon – can translate web pages, mails or any texts. They are able to learn, if once they get an advice so that they can make better translation next time.
- Speech to text and text to speech robots for deaf or lightless students.
- Simulators for training in dangerous or expensive situations.
- Plagiary-checking robots can compare texts and find the similarities between homework and coursebook.
- Chatting or talking robots with artificial intelligence for tutoring students 7 day a week and 24 hours a day.

e-Learning is the most democratic learning method of the world but there is a problem between the tutor and the students. e-Students need permanently consultations but tutor has limited working time for it. This is much bigger problem if they live in different time-zones. It can happen often in any e-Learning practice.

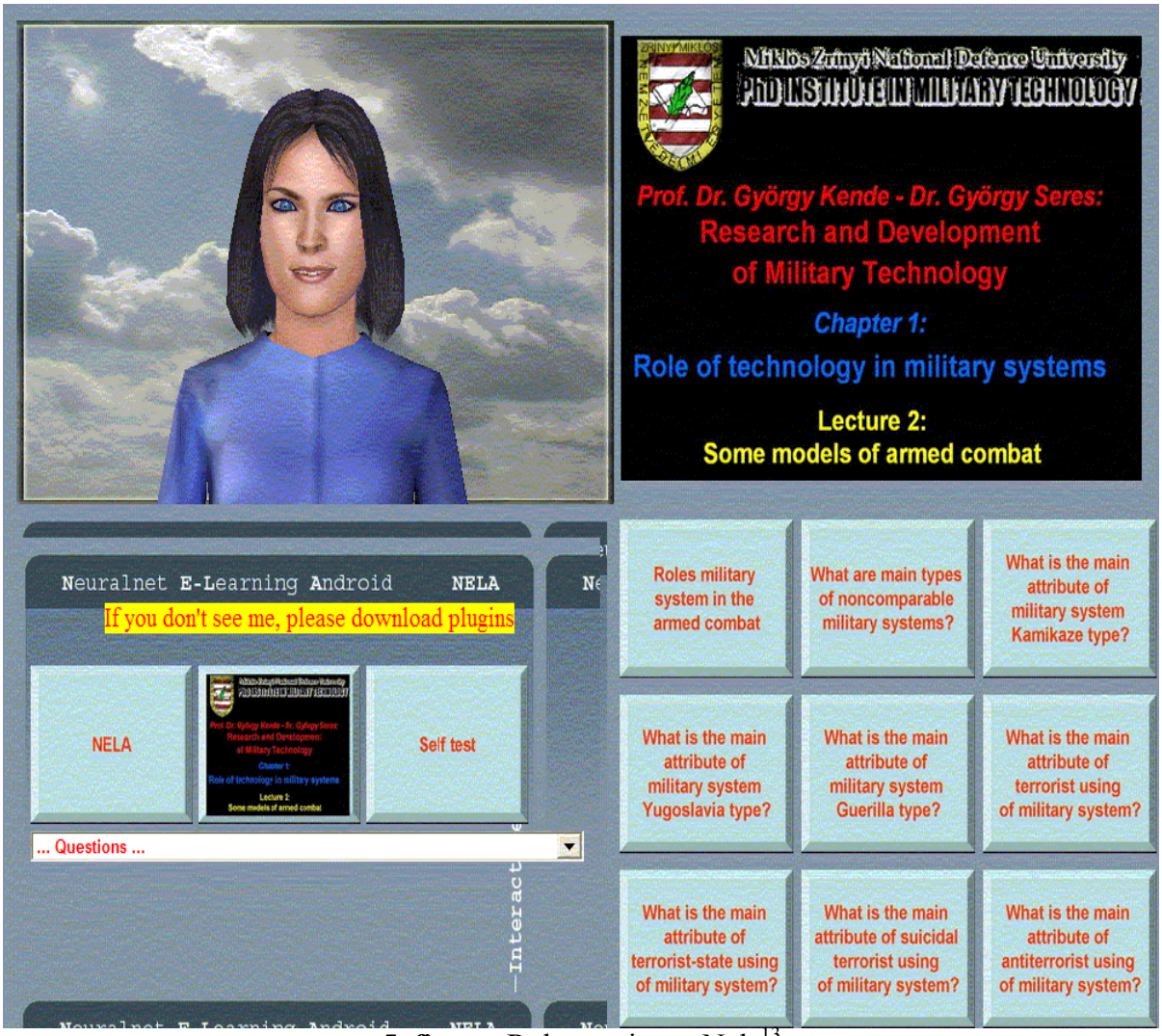
The robots used by e-Learning systems contain unique object program and this is the most modern type of education. The use of multimedia school-work, even teaching and the virtual lessons are managed by an interactive talking software robot aided by artificial intelligence. The knowledge base of the robot of course can be expanded by any topic. In multilevel test systems the bot can provide time limited assessment, control and communication.

- There is a virtual university in Hagen, Germany [15]. The system contains all functions of the university, including the curriculum and the administration, moreover a user-friendly and effective communication environment such as peer learning or group work, video conference, billboard and usage of the library.
- The Carnegie Learning program[9] which was realized in the Carnegie Mellon University was made to help students in learning mathematics. The system is aided by artificial intelligence and help pupils to solve their personal problems and give instructions to solve their tasks. The system is able to notice if there is any difficulty and help if it is needed. This system is used in more than 1700 high school in mathematics education at the USA.
- Claude Frasson[10] and his firm called uMind[11] integrated artificial intelligence in computer aided education system. uMind has already designed courses for such

[9] http://online.carnegielearning.com/
[10] http://www.umindsoft.com/En/About/Frasson.html
[11] http://www.umindsoft.com/

organizations as the Department of National Defence and the Montreal Transit Corporation.

- An experimental robot assistant Nela[12] helps students of subject "R&D in Military Technology" in ZMNDU [16].



5. figure. Robot assistant Nela[13]

Of course there are lots of other systems aided by artificial intelligence to help education so that we can write about this topic only without the claim to entirety. The virtual tutors have very important role in the future of education because they are independent from human activity, residence and time. They are very effective in education, learning, controlling and rating, too.

The intelligent tutoring systems are any kind of computer systems that can provide directly customized instructions or feedback to students, without any intervention of human beings, If the system can be available across internet in that case the system will be reachable apart from residence and time.ű

[12] http://www.drseres.com/shahin/
[13] http://www.drseres.com/shahin/index0.htm

CONCLUSION

If you read all of chapter, you can ask: what is the research topic of authors? There are five different research profiles.

No, there is one topic only – it is the e-Learning.

We can flash this statement with a story:

'Four lightless people met with an elephant in Zoo Park. They research it with their ear and hand, then they ask caretaker: "A what kind of animal is it?"

Caretaker said: "It is an elephant."

*In the evening they tell their friends:"*We were in the Zoo where we met an elephant."

Friends ask: "And what kind of animal is elephant?"

First answer: "Elephant is like that than a ship's horn" – *he heard only the elephant.*

Second answer: "Elephant is like that than a garden hose" – *he felt elephant's trunk all over.*

Third answer: "Elephant is like that than a hawser" – *he got his share of the tail of the elephant.*

Fourth answer: "Elephant is like that than a column of the church" – *said who felt elephant's foot.'*

Story of our researches is like this. We all met e-Learning in the world of education.

One of us sees it so, that e-Learning is the best method of the life-wide learning lifelong.

Other one thinks so, that e-Learning can be more effective, if it is life-tailored.

A member of our Club observes accelerated progress of technological environment of the e-Learning in the last century.

Experience is the key of success of e-Learning process, by one of our researchers.

Software robots can provide an efficient support for learners and teachers in monotonous, expensive and dangerous e-Learning tasks – in opinion of our other colleague.

As a summary we can see that all of members of the SysAdminLess Club research different sides of the same topic – different aspects of the e-Learning.

REFERENCES

[1] TIFFIN, John & RAJASINGHAM, Lalita: Education in an Information Society. 1995. London, New York, p. 88:

[2] SERES, György & KENDE, György & MISKOLCZI, Ildikó: Let' s learn easily and quickly - lifelong, anytime, anywhere. 2008. Jampaper. 2008/3 http://www.jampaper.eu/Jampaper_E-ARC/No.3_III._2008_files/JAM080302e.pdf. ISSN 1789-6967

[3] KOMENCZI, Bertalan: Didaktica elektromagna? Az e-Learning virtuális valóságai. 2004. Új Pedagógia Szemle, 2004/11., pp. 31-49.

[4] BEDŐ, Viktor: Magyar Virtuális Enciklopédia. MTA Budapest, 2009. http://www.enc.hu/1enciklopedia/fogalmi/inf/halozatkutatas.htm

[5] KOMENCZI, Bertalan: Az e-Learning lehetséges szerepe a magyarországi felnőttképzésben (kutatási zárótanulmány). 2006. pp. 15-16.. https://www.nive.hu/konyvtar/content/edoc/files/03_komenczi.pdf .

[6] GERŐ, Péter: Az élethelyzethez igazított tanulás, (Life-Tailored Learning, university course-book), ZMNE, Budapest, 2008. ISBN 978-963-7060-54-0

[7] GERŐ, Péter & SERES, György: e-Learning from the point of view of methodology, AARMS, ISSN 1588-8789, Vol. 9, No. 2 (2010) pp. 377-394.

[8] SERES, György, & al.: Cloud Learning, EDEN Research Workshop, 24-27. October 2010, Book of Abstracts, ISBN 978-963-87914-4-3, p. 188

[9] FOSTER, I.: What is the Grid? A Three Point Checklist, 2002. Argonne National Laboratory & University of Chicago

[10] BAKER, M., & BUYYA, R., & LAFORENZA, D.. Grids and Grid Technologies for Wide-Area Distributed Computing, 2002. Practice and Experience (SPE) Journal, Wiley Press

[11] NAGHSHINEH, M. at al.. IBM research division cloud computing initiative, **2009.** IBM Journal of Research and Development, Vol. 53 , Issue 4, pp.499-508, ISSN:0018-8646

[12] JOINT, A., & BAKER, E., & ECCLES,: EHey, you, get off of that cloud?, 2009. Computer Law & Security Review, (Vol. 25, Issue 3, pp. 270-274).

[13] SZ. LENGYEL, Piroska: Hatékony virtuális oktatás a pedagógia és a didaktika szemszögéből, 2010. Hadmérnök 2010/2., pp. 380-390, ISSN 1788-1919 http://www.hadmernok.hu/2010_2_szegedine2.pdf

[14] AEBLI, H.: Lélektani didaktika, 1984. Országos Pedagógiai Intézet, Budapest.

[15] SCHLAGETER, G. & BUHRMANN, P. & MITTRACH, S.: Virtual University - University of Hagen Online, 1996. Issue 11 "Learning in a Global Information Society" 28 October 1996
http://www.pjb.co.uk/11/vu.htm

[16] KENDE, György & SERES, György: Robotok az oktatásban, 2008. ZMNDU „ROBOT WARFARE-8" (international Scientific Conference)
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/05_Seres%20Gyorgy.pdf

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Erdei Gábor

A FÖLDRAJZI MODELLEZÉSBEN ALKALMAZOTT MATEMATIKAI ÖSSZEFÜGGÉSEK

Absztrakt

A cikk szerzője modellezés során alkalmazott matematikai összefüggésekkel foglalkozik. Ismerteti azokat a számítási eljárásokat, melyek a profilalkotáskor felhasználhatók. Az alkalmazott matematikai összefüggések alapparadigmákra épülnek, melyek segítenek a tettes tartózkodási helyének meghatározásában. Az eredményeket nagymértékben befolyásolja az a körülmény, hogy az elkövető utazó jelleggel, avagy a lakhelye közelében követi el a bűncselekményeket, ezért szükséges a problémakör több irányú megközelítése, illetve a legmegfelelőbb módszer kiválasztása. A modellezés akkor eredményes, ha a földrajzi jellemzés módszerei figyelembe veszik nemcsak a szabályszerűségeket, hanem a korlátokat is. A profilalkotó módszer az időben elnyúló sorozatbűncselekmények elkövetőjének felderítésére a bűncselekmény típusától függetlenül is jól alkalmazható.

The author used in modeling the geographic deals with mathematical equations. Describes the calculation procedures which can be used for profiling. The applied mathematical relationships based on basic paradigms which help in determining the location of the offense. The results are greatly influenced by the fact basis that the offender is traveling, or living in the vicinity of the crimes committed by therefore necessary for multi-directional approach to the problem, selecting the most appropriate method. The modeling is effective the method takes into account not only the geographical characterization of the regularities but the constraints. The profiling method stretching out the time series to detect the perpetrator of crimes regardless of the type of crime can be applied.

Kulcsszavak: *földrajzi profil, rögzítési pont, Fokker-Planck egyenlet, határfeltételek, sorozatbűncselekmény, puffer zóna, utazó bűnözés, MLE egyenlet, CGT algoritmus, számítási módszerek, modellezés fejlesztése, térbeli pont ~ geographical profile, fixation point, Fokker-Planck equation, boundary conditions, crime series, buffer zone, traveler crime, MLE equation, CGT algorithm, calculation methods, modeling development, point in space.*

A BŰNÖZÉSFÖLDRAJZ ÉS A FÖLDRAJZI PROFIL KAPCSOLATA

A bűnözésföldrajz alakulásának egyik meghatározója az elkövető földrajzi profiljának megalkotása. A földrajzi profil a bűncselekmény gyanúsítottjának a legvalószínűbb tartózkodási helyére mutat rá. A profilalkotás számítógépes modellezés, ami a tettesekre és az elkövetések helyszíneire szolgáltat adatokat, melyek egzakt számításokon alapul. A modellezés tehát területbehatárolást jelent (Brantingham & Brantingham (1993), Canter and Larkin (1993), and Rossmo (2000). Canter, D. and Larkin, P. (1993).

Az elkövető tartózkodási helye abban a területben helyezkedik el, ahol a mindennapos tevékenységét végzi és ahol a bűncselekményeket elkövette (Groff, E. 2008). A két terület aránya eredményezi az elkövető legközelebbi és a legtávolabbi tartózkodási helye közötti távolságot.

A keresési terület komplex valószínűségi számításokkal állít elő egy centrális pontot (Clarke, R. V. and Felson, M., eds. 1993).

A földrajzi profilok szerepe nem csak abban rejlik, hogy eredményesen kutatja fel az elkövetőket, hanem az adott bűncselekményekre standard modelleket lehet építeni és ezek a modellek más nyomozásokban is alkalmazhatók (Levine, N. (2007)..

A profilalkotás tendenciózus folyamatokra is rávilágít a területi elemzésekben nagy mértékben nyújt segítséget, amely lehetősséget ad a bűncselekmények bekövetkezése elleni hatékony fellépésre (Rossmo 2000, Canter, D., Co_ey, T. Huntley, M., and Missen, C. (2000).

A KINETIKAI MODELL FELÁLLÍTÁSA

A földrajzi profilalkotás kinetikusan modellezhető, mely során a tettes tartózkodási helye lineáris úton határozható meg. A számításkor egy alappont kijelölése szükséges abban a keresési területben, melyben nemcsak a lakóhely, munkahely, stb. tartózhat bele, hanem a bűncselekmények helyszínein kívül az is, ahol az elkövetőt a szemtanúk látták, vagy megfigyelték. A kinetikai modell a Fokker-Planck egyenlet és a Bayes-tétel felhasználásával, valamint az alappontok (rögzítési) pontok segítségével állítható fel (Keats, A., Yee, E., and Lien F-S. (2007).

A földrajzi értelemben vett változók, mint pl. a népsűrűség, a földrajzi akadályok, a folyók, a tavak, a parkok stb. befolyásoló tényezőként jelennek meg a helymeghatározás elliptikus parciális differenciál egyenletében (PDE). A modellezés számításaiban a Multigrid módszer (a numerikus analízis egyik csoportja) alkalmazható, mely a PDE egyenletek segítségével az algoritmusok megoldására szolgál. (O'Leary, M. 2009).

Klasszikus problémaként vetődik fel minden bűnügy nyomozásakor egy olyan rögzítési pont meghatározása, mely az elkövető tartózkodási helyét valószínűsíti. A rögzítési vagy alappontot $z \in R2$ halmazon értelmezzük (O'Leary, M. 2009).

Sorozat bűncselekmény esetén az összefüggés kiegészül a helyszínekkel és azokkal a helyekkel, ahol az elkövetőt látták. $x1, \ldots, xN \in R2$

A rögzítési pont lehet a cselekményekkel összefüggésbe nem hozható hellyel, mint a barátnál, vagy a családtagnál való tartózkodási hely, a munkahely, stb., de lehet pl. autóbusz megállóhely is, mely elkövetési helyszínként jelenik meg (O'Leary, M. 2009).

A rögzítési pont egyenlete

A gyakorlatban rögzítési pontként az alábbi összefüggés használható.

$$S(\mathbf{z}) = \sum_{i=1}^{N} f(d(\mathbf{x}_i, \mathbf{z}))$$

.

A d metrikus távolságfüggvény, f egy olyan mag, mely jellemzően a távolság növelésével az eredmény pontosságát befolyásolja (O'Leary, M. 2009).

A számítási eredmények megbízhatósága

A módszer megbízhatóságát O' Leary (2009) vonta kétségbe, aki azt állította, hogy a modellezés csak a helyszíneket és az elkövető megjelenési pontjait mérlegeli. Az f általában izotróp (a térbeli iránytól független), és nem vesz figyelembe olyan földrajzi jellegzetességeket, mint az épületek és a lakosság sűrűségét.

P(z|x1, …, xN).

A betörések esetében a tettesek rögzítési pontjai meghatározhatók z1, z2, és a z3 alapján úgy, hogy a helyszínt centrális pontként jelöljük. A mintában a z rögzítési pontok egymáshoz képest növekvő sort alkotnak. A többi pont egyenlő távolságra van az 1. helyszíntől, mivel az elkövető egy kör kerületén mozgott. Hasonlóképpen a z2 kisebb mint a z3, mert olyan helyzet merülhet fel, ahol a központi z3 helyszín elérését az előtte elkövetett bűncselekmények megakadályozzák. Egy másik modellezés szerint a betörések földrajzi változatossága miatt a központi z helyszín körül rajzolt körben minden pont közelebb van a centrumhoz, mint z1, z2, vagy z3, alternatív megközelítésben a tettes tartózkodási helye a Bayes-tétel felhasználásával állapítható meg (Keats, A., Yee, E., and Lien F-S. (2007).

A Bayes-tétel

P (z | x sűrűsége a kikötési pont, P(z|x1, …, xN).

A tétel alkalmazásához szükséges az elkövetési helyekből következtetett, valamint a korábbi eloszlásokból adódott rögzítési pontok. A sorozat bűncselekmények kinetikai modellezése megmutatja a tettes térbeli mozgását és az általa kiválasztott helyszíneket. A modell figyelembe veszi a földrajzi profilalkotás grafikai jellemzőit, melyekkel más modellezés nem számol. A számítások valójában egy becsült értéket adnak, mely az elkövető valószínűsíthető tartózkodási helyére mutat rá (Keats, A., Yee, E., and Lien F-S. (2007).

A kinetikai modellek megalkotására a Bayes-tételen kívül a Fokker-Planck egyenlet is segítséget nyújt. A parciális differenciál egyenletek (PDE) által a földrajzi profilalkotás hatékonyabbá válik. A Monte Carlo módszer esetében a közvetlen számítások a kinetikus modell pontatlanságához vezetnek. A kinetikai modell a gyanúsított táplálkozási szokásaiból is megalkotható, ami meghatározó tényező a bűncselekmény típusának (Keats, A., Yee, E., and Lien F-S. (2007).

A térbeli elmozdulás definíciója

A térbeli elmozdulás $A(y) \geq 0$ azt jelenti, hogy a helyszínek mekkora területen oszlanak el. A betörés esetében feltételezhető, hogy minden lakás, családi ház egyformán lehetséges célpontjai a tettesnek, így lakóépületek eloszlása H(y). A lehetséges helyszínek által határolt mező az elkövetés gyorsaságát is jelzik a tettes y(t) helyzetében és t időpontban. A modell a gyanúsított valószínűsíthető mozgását a sztochasztikus differenciálegyenlettel írja le (Holcman, D., Marchewka, A., and Schuss, Z. (2005).

$$\frac{d\boldsymbol{y}}{dt} = \vec{\mu}(\boldsymbol{y}) + \sqrt{2D}\mathbf{R}_t ,$$

ahol Rt fehér zaj, vagyis $\langle \mathbf{R}_t \rangle = \mathbf{0}$ és $\langle R_t^i R_{t'}^j \rangle = \delta_{ij}\delta(t-t')$ és a D diffúziós paraméter (Holcman, D., Marchewka, A., and Schuss, Z. (2005).

A drift ($\vec{\mu}$) együttható alkalmazásának feltétele

Bonyolultabb büntetőügyekben a viselkedés tárgyilagosabb leírása céljából a drift (csúsztatási együttható: $\vec{\mu}$) elhanyagolható Példaként említhető, amikor a vizsgált régióban a lehetséges helyszínek a tettesek mozgási irányát módosíthatják. A tettes viselkedésére épített gradiens (függvény deriváltja) egy olyan helyet határozhat meg $\vec{\mu} = \chi \nabla A$ esetén, amely a lehetséges elkövetések övezetén kívül helyezkedik el. Rögzítési pontként lehet tekinteni azt, ahonnan az elkövető keresése megkezdődik és célként az eredeti feltételt, az y(0)=z összefüggés vehető figyelembe (Mohler, G., Short, M., Brantingham, P., Schoenberg, F., and Tita, G.(2008).

Az y(t) bűncselekményt y(t) egységnyi idő alatt követték el úgy, hogy az adott pályához a tér-idő y(t) pont megszűnik, mely pontban számítható a földrajzi profil. A Monte Carlo számítógépes modellezés feltételez egy olyan valószínűsíthető keresési területet, melyben a rögzítési pont P(z). A közvetett alapú modellezés igen elterjedt a nyomozásokban, mivel az elemzéskor nem szükséges felhasználni a matematikai analízist (Mohler, G., Short, M., Brantingham, P., Schoenberg, F., and Tita, G.(2008).

A Fokker-Planck egyenlet

A pontosabb helymeghatározás elérése érdekében a matematika nem hagyható figyelmen kívül. A büntetőeljárás megindításakor a feltételezések határozzák meg ρ(x,t|z) valószínűségi környezetben az elkövető z rögzítési pontját, mely az alábbi Fokker-Planck egyenlettel írható le.

$$\frac{d\rho}{dt} = \nabla \cdot (D\nabla\rho) - \nabla \cdot (\vec{\mu}(\mathbf{x})\rho) - A(\mathbf{x})\rho \quad , \qquad \rho 0 = \delta\,(\text{x-z}),$$

ahol ∇ változó a valószínűséget jelenti az integrált x időben Mohler, G., Short, M., Brantingham, P., Schoenberg, F., and Tita, G.(2008).

A bűncselekmény valószínűsége $P(x|z)=A(x)\rho(x|z)$, ha $\rho(\mathbf{x} \mid \mathbf{z}) = \int_0^\infty \rho(\mathbf{x}, t \mid \mathbf{z})\, dt$ oldja meg az alábbi elliptikus parciális differenciál egyenletet,

$$-\nabla \cdot (D\nabla\rho) + \nabla \cdot (\vec{\mu}(\mathbf{x})\rho + A(\mathbf{x})\rho = \delta(\mathbf{x}-\mathbf{z}) .$$

A $\int_0^\infty \rho(\mathbf{x}, t \mid \mathbf{z})dt$ nem ad pontos meghatározást drift $\vec{\mu}$ együtthatóra és az elkövetési területre.

Akkor egyértelmű a meghatározás, ha a $\vec{\mu}$=0 és A(x)=A0>0 (a mag $A_0 e^{-A_0 t}$ szorzóval (Mohler, G., Short, M., Brantingham, P., Schoenberg, F., and Tita, G.(2008).

Dirichlet és Neumann-féle határfeltételek

Az egyenletnek figyelembe kell venni egy véges tartomány numerikus közelítését. Reális peremfeltétel és a megfelelő nagyságú vizsgált terület (domain) esetén a véletlenszerű elkövetések nélkül a határ elérésekor a bűncselekmény alacsony valószínűségű.. A figyelembe vett 70km*70km-es (domain) terület arányos az A(x) lakóépületek sűrűséggel. Dirichlet és Neumann a határfeltételekre a $\rho(\mathbf{x},t\,|\,\mathbf{z})$ jól körülhatárolásával adott választ. R (Estep, D. 2004).

A földrajzi-grafikai profilokat az adjungált (komplex algebra) egyenlet a Bayes-tétel segítségével határozható meg, ahol a P(x) rögzítési pontot jelöl:

$$P(\mathbf{z}\,|\,\mathbf{x}) = \frac{P(\mathbf{x}\,|\,\mathbf{z})P(\mathbf{z})}{\int_{R^2} P(\mathbf{x}\,|\,\mathbf{z})P(\mathbf{z})dz} = \frac{A(\mathbf{x})\rho(\mathbf{x}\,|\,\mathbf{z})P(\mathbf{z})}{\int_{R^2} A(\mathbf{x}\,|\,\mathbf{z})\rho(\mathbf{z})dz} = \frac{\rho(\mathbf{x}\,|\,\mathbf{z})P(\mathbf{z})}{\int_{R^2} \rho(\mathbf{x}\,|\,\mathbf{z})P(\mathbf{z})dz}.$$

A $\rho(\mathbf{x}\,|\,\mathbf{z})$ Green függvény lineáris együtthatói közül a bal oldali fix x és a változó z függvényt az $f(\mathbf{z}) = \rho(\mathbf{x},t\,|\,\mathbf{z})$ oldja meg az adjungált (komplex) egyenletet

$-\nabla\cdot(D\nabla f) - \vec{\mu}(\mathbf{z})\cdot\nabla f + A(\mathbf{z})f = \delta(\mathbf{z}-\mathbf{x})$, ahol ∇ a változó.

A földrajzi profil valószínűségének megoldásában az egyenlet bal oldalán az alappontot a jobb oldali helyszínek feltételezett eloszlás rögzítési pontjaival megszorozzuk, mely által az egyenlet normalizálódik. Az elsőrendű származtatott változások jele lesz az új egyenletnek, mely a maradék egyenletben hoz változást. A gyakorlati szempontból, ha a bűnözők az elkövetési terület felé orientálódnak, a nyomozások kezdetben a helyszínektől távolodnak (Estep, D. 2004).

A földrajzi profil egyenlete sorozatbűncselekmény esetén

A feltételezés szerint, ha a sorozat bűncselekményt ugyanaz a személy követte el, akkor a földrajzi profil több esemény alapján megalkotható,

$$\mathrm{P}(\mathbf{z}\,|\,\mathbf{x_1},\ldots,\mathbf{x_N}) = \frac{P(\mathbf{x_1}\,|\,\mathbf{z})\ldots P(\mathbf{x_N}\,|\,\mathbf{z})P(\mathbf{z})}{\int_{R^2} P(\mathbf{x_1}\,|\,\mathbf{z})\ldots P(\mathbf{x_N}\,|\,\mathbf{z})P(\mathbf{z})dz} = \frac{\prod_{i=1}^{N} f_i(\mathbf{z})P(\mathbf{z})}{\int_{R^2}\prod_{i=1}^{N} f_i(\mathbf{z})P(\mathbf{z})dz},$$

ahol fi(z) megoldása,

$-\nabla\cdot(D\nabla f_i) - \vec{\mu}(\mathbf{z})\cdot\nabla f_i + A(\mathbf{z})f_i = \delta(\mathbf{z}-\mathbf{x}_i)$ (Estep, D. 2004).

A puffer zóna egyenlete

A puffer zóna az alábbi egyenlettel oldható meg:

$P(\mathbf{x} \mid \mathbf{z}) = 1_{\{|\mathbf{x}-\mathbf{z}|>r\}} A(\mathbf{x}) \rho(\mathbf{x} \mid \mathbf{z})$ ahol a $\rho(\mathbf{x} \mid \mathbf{z})$ a módosított következő egyenlet oldja meg

$$-\nabla \cdot (D \nabla \rho) + \nabla \cdot (\vec{\mu}(\mathbf{x}) \rho) + 1_{\{|\mathbf{x}-\mathbf{z}|>r\}} A(\mathbf{x}) \rho = \delta(\mathbf{z}-\mathbf{x})$$

.

Az ötlet szerint a tettesek nem hagyják el a kör alakú pufferzónát, azonban a körben és a rögzített pont környékén bűncselekményt nem követnek el. A maradék egyenlet megoldása szerint

$$-\nabla \cdot (D \nabla f) - \vec{\mu}(\mathbf{z}) \cdot \nabla f + 1_{\{|\mathbf{x}-\mathbf{z}|>r\}} A(\mathbf{z}) f = \delta(\mathbf{z}-\mathbf{x})$$

.

A földrajzi profilalkotás valószínűsége,

$$P(\mathbf{z} \mid \mathbf{x}) = \frac{1_{\{|\mathbf{x}-\mathbf{z}|>r\}} f(\mathbf{z}) P(\mathbf{z})}{\int_{|\mathbf{x}-\mathbf{z}|>r} f(\mathbf{z}) P(\mathbf{z}) d\mathbf{z}}$$ (Estep, D. 2004).

A LEHETSÉGES ELKÖVETÉSEK ÉS A TERÜLET VISZONYA

A 2003-2007 között a los angelesi betörések közül 244 sorozatot derítettek fel a nyomozó hatóságok. A sorozatok 3 és 32 közötti elkövetésekből álltak, melyek átlaga 3,7-et mutatott. A feltételezés szerint a tettesek közötti eloszlás egyenletes, minden városon belüli lakóház egyformán „vonzó” a bűnözők számára (Schuss, Z. (1980)..

Az elkövetési területen az elkövetési lehetőség A(x)=A0·H(x) és az előzetes cselekmények P(z)=P0·H(z) arányos a lakások H sűrűségével. A gyakorlatban a P(z) kiegészítő információként jelenhet meg a rendőrségi adatbázisból a lakásokra, a korábbi elkövetőkre, a feltételes szabad lábon lévőkre, a potenciális gyanúsítottakra és más bűncselekményekre vonatkozóan (Silverman, B. W. (1986).

Feltételezhető továbbá, hogy a tettesek mozgását a város sztochasztikusan szabályozza, ezért $\text{drift}(\vec{\mu}) = 0$. A tényleges paraméter $\Theta^k = \frac{D}{A_0}$ lehet becsülni egy x megoldott bűncselekmény sorozatban a k helyszínen $\{X_i^k\}_{i=1}^{N_k}$ és a rögzítési pont zk maximalizálja a log függvény valószínűségét,

$$\hat{\Theta}^k = \arg\max_{\Theta} \sum_{i=1}^{N_k} \log(P(\mathbf{x}_i^k \mid \mathbf{x}^k, \Theta)$$

.

ahol az események egymástól függetlenek. A tényleges paraméter értékét π(Θ) kell beépíteni a valószínűsítésen alapuló egyenletbe,

$P(\mathbf{z} \mid \mathbf{x_1},...,\mathbf{x_N}) \alpha \int \mathrm{P}(\mathbf{x_1} \mid \mathbf{z}, \Theta)...\mathrm{P}(\mathbf{x_N} \mid \mathbf{z}, \Theta) P(\mathbf{z}) \pi(\Theta) d\Theta$ (Fouque, J-P., Papanicolaou, G., and Sircar, K. R. 2000).

A földrajzi környezet és az utazó bűnözés közötti összefüggés

Gyakran előfordul, hogy a tettesek egy része nem a lakókörnyezetében követi el a bűncselekményeket, hanem azoktól távol, ahová közlekedési eszközökkel jutnak el. Az ingázások nemcsak nagy területekre, hanem a régióra, vagy városra is vonatkozik. A los angelesi sorozat betörések vizsgálatakor matematikai úton kimutatható, hogy az összes bűncselekmény helyszínei által megrajzolt legkisebb körben található az elkövető tartózkodási helye, azonban a teljes elemzés kiterjed a város agglomerációs övezetére is. A földrajzi környezet változatossága, illetve az elkövető ingázása azt eredményezheti, hogy a valószínűsíthető keresési terület nem esik egybe a ténylegessel. Az eltérés a tettes egy adott irányba történő mozgásából adódhat (Brantingham, P. J. and Tita, G. 2008).

Két los angelesi bűncselekmény sorozat a lakóházak sűrűségéből adódóan 70km*70km övezetben megrajzolható. A rajzolt négyzetben a tettes tartózkodási helye, attól távolabbi, illetve közelebbi helyszínek körökkel jelölhetők. A megközelítés módszerével felállított egyenletbe beépíthető az utazásokkal elkövetett cselekmények.

$\min_i d(\mathbf{z}, \mathbf{x}_i) > \gamma \max_{i,j} d(\mathbf{x}_i, \mathbf{x}_j)$ (Johnson, S. D., Summers, L., Pease, K. (2009).

Ha a bűncselekményhez megtett távolság nagyobb, mint a helyszínek közötti távolságok, akkor megállapítható, hogy utazó bűnözőről van szó.

Az alábbi egyenletben a földrajzi profil felhasználásával a P(M) a helyi elkövetőket a P(C) az utazó bűnözőket jelöli.

$P(\mathbf{z} \mid \mathbf{x_1},...,\mathbf{x_N}) \alpha \int \mathrm{P}(\mathbf{x_1} \mid \mathbf{z}, \Theta)...\mathrm{P}(\mathbf{x_N} \mid \mathbf{z}, \Theta) \pi_M(\Theta) d\Theta \cdot P(M) P(\mathbf{z}) + \int P(\overline{\mathbf{x}} \mid \mathbf{z}, \Theta) \pi_C(\Theta) d\Theta \cdot P(C) P(\mathbf{z})$
(Johnson, S. D., Summers, L., Pease, K. (2009)

Az MLE egyenlet

A $\pi_M(\Theta)$ az empirikus úton történt maximális valószínűsítés becslése az MLE (maximum likelihood estimation) kernel paraméter segítségével számolható

$$\pi_M(\Theta) = \sum_{k \in M} K(\Theta - \hat{\Theta}^k),$$

ahol az M index a betörés sorozat és a $\hat{\Theta}^k$ az MLE paraméter a k sorozatban. A $\pi_C(\Theta)$ becsült értéke hasonlóan alakul

$$\hat{\Theta}^k = \arg\max_{\Theta} \sum^{N_k} \log(P(\bar{\mathbf{x}}^k \mid \mathbf{z}^k))$$

,

ahol $\bar{\mathrm{x}}^k = \frac{1}{N_k} \sum_{i=1}^{N_k} \mathrm{x}_\mathrm{i}^k$.

Az elkövető rendszeres mozgása azt sugallja, hogy a helyszínekre utazik. Az xi helyszínek egy rögzített (s) pont mentén kör alakban helyezkednek el. A munkavégzés helye, a barát lakása, stb. nem ismertek, ezért az $\bar{x}$ rögzítési pont meghatározása problémát okoz., mivel nem fogja megtalálni azt az alappontot, mely az elkövető valószínűsíthető z tartózkodási helyét határozza meg. Az elővárosi rögzítési pont kiválasztásának ugyanaz a célja, mint az elkövetőjének, azonban a feltételezések megfelelő irányát a jövő kutatásai határozzák meg. A földrajzi profilalkotás a CGT (Criminal Geographic Targeting) algoritmusban a PDE-alapú egyenletekkel alkalmazhatók (Johnson, S. D., Summers, L., Pease, K. (2009).

A CGT algoritmus

$$\mathrm{f(d)}= \begin{cases} \frac{k}{d^h}, d > B \\ \\ \frac{kB^{g-h}}{(2B-d)^g}, d \le B \end{cases}$$

ahol a távolság függvény metrikus. Az f = g = 1,2 és a két legközelebbi helyszín között az átlagos távolság B 1/2. A PDE-alapú modellben az adathalmazt 128x128 felbontású 70 km x70 km domain területen Dirichlet függvényanalízis feltételrendszere alapján vizsgálják. Az elemzés a trapéz alakú 20 pontos diszkretizációs közelítéssel végezhető el. A P(M) és a P(C) paramétereket leave-one-out (rangsorolásos) módszer segítségével empirikus úton lehet kiszámítani, ha γ=1. A modell egy adott sorozatban a paraméterek kalkulációjával értékelhető. A PDE-alapú modellek összehasonlításakor az összes elkövető paramétere (P(M)=1) annak érdekében, hogy a kinetikai hatásokat az utazó bűnözők adatinak felhasználásával a Bayes-tétel alapján értékeljük (Keats, A., Yee, E., and Lien F-S. (2007).

Számítási módszerek profilalkotás modellezésére

A három földrajzi profilalkotó modell (CGT) algoritmusaiban a PDE-M (P(M)=1), a PDE-MC (P(M)≠1). A PDE-MC a helyszínek, a közeli és távolabbi elkövetések segítségével rajzolható meg. A PDE-alapú modell figyelembe veszi a földrajzi változatosságot a valószínűsíthető helyszíneket a lakóövezetekben. A földrajzi profilok megalkotásakor a CGT algoritmus a két PDE-M sorozat segítségével értékeli a magánterületektől kezdve a kereskedelmi központokon át, a hegyeket, és az óceánokat is. A módszer azt tételezi fel, hogy a bűncselekmények egymástól függetlenül következtek be (Briggs, W. L., Emden Henson, V., McCormick, S. F. 2000).

A három modell log valószínűségét a CGT pontszám funkció értékeli. A módszer megfelelő rögzítési pontok felállítása alapján valószínűségi mennyiséget mér. A PDE-M modell CGT algoritmussal az elkövetők részhalmazára pontosabb számítást eredményez, mint a statisztikai módszer (log-likelihood). A valószínűsíthető bűncselekmények körül helyezkedik el a tényleges sorozatelkövetés, mely alapján az agglomerációs övezetben

elkövetett cselekmények negatív hozzájárulása biztosítja a teljes valószínűség PDE-M értékét. A PDE-MC modell CGT algoritmusa a Bayes-tétel felhasználásával ad megközelítést, mely átlagosan 66,7% (Mohler, G., Bertozzi, A., Goldstein, T., and Osher, S. (2009).

A CGT algoritmus alsó statisztikai (log-likelihood) értéke elővárosi bűncselekményekből. következik. Az egyenlet valószínűsége a CGT és hasonló algoritmusokkal számolható a mag paraméterek segítségével feltételezve, ha a cselekmények egymástól függetlenül következtek be. A módszerrel pontosabb eredmény érhető el, ha az elkövetőnek van állandó tartózkodási helye, ugyanis utazó tettes esetén, a számítások már pontatlanok (Mohler, G., Bertozzi, A., Goldstein, T., and Osher, S. (2009).

A CGT és a PDE közötti eltérések

Az alábbi táblázat a CGT és a PDE módszerek közötti eltéréseket mutatja.

CGT	PDE-M	PDE-MC
-2446,9	-2595,2	-2348,1

A CGT és a két PDE alapú modellek metrikus összehasonlítása során az egyik példában a várost kisebb területekre 0,3 km2-es övezetekre) osztjuk fel. Minden sorozat betörés adatsora, valószínűsége az előbb meghatározott méretű területekben, ún. cellákban jelölhető. A 244 sorozat a lakóépületek %-os arányában ábrázolható, melyben található a top-x%-ú cella. A nyomozás szempontjából a top-x cellát lehet tekinteni a helyes helymeghatározásnak. A modellek közül PDE-M algoritmussal az eredmények pontosabbak annak ellenére, hogy a statisztikai (log-likelihood) adatok szerint a másik két módszerhez képest alacsonyabb besorolásba került. (Short, M. B., D'Orsogna, M. R., Pasour, V. B., Tita, G. E., Brantingham, P. J., Bertozzi, A. L. and Chayes, L. (2008).

A PDE-M kevesebb helyre vonatkoztatja a valószínűséget, azonban a keresett területen végzett szűkítése kedvező. A PDE-MC modellt a fejlesztések valamelyest javították, azonban komolyabb előrelépést a számítások terén még nem jelentett. A földrajzi profilalkotásban új keretet kínál a Bayes-tétel, amely a tettesek mozgását kinetikai alapokra helyezi (Mohler, G., Bertozzi, A., Goldstein, T., and Osher, S. (2009).

A modellezés fejlesztésére irányuló elképzelés

A jövőt illetően fontolóra kell venni, hogy az általános modellek az alábbi egyenletből induljanak ki.

$$-L\rho + \nabla \cdot (\vec{\mu}(\mathbf{x})\rho) + A(\mathbf{x})\rho = \delta(\mathbf{x} - \mathbf{z})$$

Az egyenletben az L a relatív diffúziós együttható, melynek sorozatbűncselekmények földrajzi profilalkotásakor van nagy szerepe Lehetőség nyílik arra is, hogy a diffúziós paraméter valószínűségszámításra épülő (sztochasztikus) folyamat mentén épüljön be az egyenletbe. A sztochasztikus, nagy amplitudóban változó (volatilitás) modelleket a gazdasági folyamatok elemzésére használják, mely modellezés előnyös lehet az inhomogén

büntetőügyekben is, vagyis $L = \nabla \cdot (d(\mathbf{x})\nabla)$ jelenti a földrajzi profil valószínűségét (Barton G. 1989).

A nagy városok forgalma is fontos szerepet játszik a rögzítési pontok meghatározásában. A rögzítési pontok egyenlő távolságra vannak (térben) a helyszínektől, de időben eltérnek egymástól és a bekövetkezések valószínűsége sem jelenik meg azonos súllyal. A földrajzi akadályok, mint a parkok, a folyók, a tavakat stb. is a valószínűségi számítások részei, mivel a tettesek eme szétszórt (diffúz) objektumok körül vagy mentén mozognak (Tadjeran, C., Meerschaert, M. M., Scheffler, H-P. 2006).

Az olyan típusú bűncselekményekben, ahol a lakások sűrűsége nem játszik szerepet, a figyelem arra a területre irányul, ahol pl. személy elleni bűncselekményeket, gépjárműlopást, stb. követtek el, melyek kedvező feltételeket jelentettek a tettesnek a cselekmények elkövetésére (Tadjeran, C., Meerschaert, M. M., Scheffler, H-P. 2006).

A térbeli pont meghatározása

Az alábbi modellben a P marginális érték a Pc(x) a bűncselekmények valószínűsíthető sűrűsége,

$$P_c(\mathbf{x}) = \int_{R^2} A(\mathbf{x})\rho(\mathbf{x} \mid \mathbf{z})P(\mathbf{z})d\mathbf{z}$$

,

melyből lehet következtetni az összes helyszín térbeli adataiból egy adott valószínűsíthető térbeli pontra, mely $\hat{P}_c(\mathbf{x})$ keresési terület minimálisra csökkentésével számítható a közelítő érték.

$\int_{R^2} (\hat{P}_c(\mathbf{x}) - \int_{R^2} A(\mathbf{x})\rho(\mathbf{x} \mid \mathbf{z})P(\mathbf{z})d\mathbf{z})^2 d\mathbf{x}$ (Tadjeran, C., Meerschaert, M. M., Scheffler, H-P. 2006).

ÖSSZEGZÉS

A modellezés akkor eredményes, ha földrajzi jellemzés módszerei figyelembe veszik nemcsak a szabályszerűségeket, hanem a korlátokat is. A profilalkotó módszer az időben elnyúló sorozat bűncselekmények elkövetőjének felderítésére a bűncselekmény típusától függetlenül is jól alkalmazható. A marginális sűrűség $\hat{P}_c(\mathbf{x})$ segítségével rekonstruálni lehet térben és időben a sorozatbűncselekmény elkövetésének teljes folyamatát.

Felhasznált irodalom

[1] Barton G. (1989): Elements of Green's Functions, Waves, and Propagation: Potentials, Diffusion, and Waves. Clarendon Press: Oxford. pp.246-262.

[2] Brantingham, P. J. and Tita, G. (2008): Offender mobility and crime pattern formation from first principles. Artificial Crime Analysis Systems, Edited by Lin Liu and John Eck. IGI Global: Hershey, PA. pp.6-18

[3] Briggs, W. L., Emden Henson, V., McCormick, S. F. (2000): A multigrid tutorial. SIAM. pp.333-390.

[4] Canter, D., Co_ey, T. Huntley, M., and Missen, C. (2000): Predicting serial killers' home base using a decision support system. Journal of Quantitative Criminology, 16 (4), 457-478

[5] Canter, D. and Larkin, P. (1993): The environmental range of serial rapists. The Journal of Environmental Psychology, 13, pp.63-69.

[6] Clarke, R. V. and Felson, M., eds. (1993): Routine Activity and Rational Choice: Advances in Criminological Theory. Vol. 5. Transaction Books: New Brunswick, NJ. Pp. 79-107.

[7] Estep, D. (2004): A short course on duality, adjoint operators, Greens functions, and a posteriori error analysis. pp.421-434 www:math:colostate:edu/~estep/research/preprints/adjointcourse_final.pdf

[8] Fouque, J-P., Papanicolaou, G., and Sircar, K. R. (2000): Derivatives in Financial Markets with Stochastic Volatility. Cambridge University Press. pp.451-477.

[9] Groff, E. (2008): Characterizing the Spatio-Temporal Aspects of Routine Activities and the Geographic Distribution of Street Robbery. Artificial Crime Analysis Systems. Liu and Eck (Eds.) IGI Global: Hershey, PA. pp. 75-103.

[10] Holcman, D., Marchewka, A., and Schuss, Z. (2005): Survival probability of diffusion with trapping in cellular neurobiology. Physical Review E, 72 (3), 031910. pp.13-19

[11] Johnson, S. D., Summers, L., Pease, K. (2009): Offender as Forager? A Direct Test of the Boost Account of Victimization. Journal of Quantitative Criminology, in press. pp.11-20.

[12] Keats, A., Yee, E., and Lien F-S. (2007): Bayesian inference for source determination with applications to a complex urban environment. Atmospheric Environment, 41, 465-479.

[13] Levine, N. (2007): CrimeStat: A spatial statistics program for the analysis of crime incident locations (v 3.1). Ned Levine and Associates, Houston, TX and the National Institute of Justice, Washington, D.C. pp. 13-22.

[14] Mohler, G., Short, M., Brantingham, P., Schoenberg, F., and Tita, G.(2008): Self-exciting point processes explain spatial-temporal patterns in crime, in review. Pp. 201-219.

[15] Mohler, G., Bertozzi, A., Goldstein, T., and Osher, S. (2009): Fast TV regularization for 2D maximum penalized likelihood estimation, in review. pp. 16-34

[16] O'Leary, M. (2009): The mathematics of geographic pro_ling. preprint. pp. 397-416

[17] Rossmo, K. (2000): Geographic Profiling. CRC Press. pp.159-175.

[18] Schuss, Z. (1980): Theory and Applications of Stochastic Di_erential Equations. Wiley Series in Probability and Statistics: New York. Pp.112-118.

[19] Short, M. B., D'Orsogna, M. R., Pasour, V. B., Tita, G. E., Brantingham, P. J., Bertozzi, A. L. and Chayes, L. (2008): A Statistical Model of Criminal Behavior. M3AS, 18, pp. 1249-1267

[20] Short, M. B., D'Orsogna, M. R., Brantingham, P. J., and Tita, G. E. (2009): Measuring repeat and near-repeat burglary e_ects. Journal of Quantitative Criminology, to appear. pp.325-340.

[21] Silverman, B. W. (1986): Density Estimation for Statistics and Data Analysis, London: Chapman and Hall. Pp. 683-690.

[22] Tadjeran, C., Meerschaert, M. M., Scheffler, H-P. (2006): A second-order accurate numerical approximation for the fractional diffusion equation. Journal of Computational Physics, 213, 211-249.

[23] Wang, X., Liu, L. and Eck, J. (2008): Crime Simulation Using GIS and Artifical Intelligence. Artificial Crime Analysis Systems, Edited by Lin Liu and John Eck. IGI Global: Hershey, PA. pp. 205-213

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Zsigovits László
zsigovits.laszlo@zmne.hu

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM K+F+I ÉS PÁLYÁZATI TEVÉKENYSÉGÉNEK LEHETSÉGES IRÁNYAI

„A tudás az, amely a használat során soha nem kopik”

Absztrakt

E tanulmány röviden összefoglalja az új Nemzeti Közszolgálati Egyetem K+F+I lehetőségeit. Az új egyetem oktatási portfoliója átfogja a honvédelemmel, rendvédelemmel és a közigazgatással kapcsolatos tudományterületeket. Ez lehetővé teszi a komplex biztonság egységes rendszerben történő tudományos vizsgálatát. A széleskörű, nemzetközi együttműködésben végzendő tudományos kutatómunka feltételei az új egyetem számára adottak lesznek. A cikk bemutatja ennek szervezeti, technikai lehetőségeit (kutatói hálózat, HBONE+, szuperszámítógépek, gridek, cloud).

This study summarizes the research, development and innovation opportunities of the newly established University of Public Services. The new university's educational portfolio includes areas of sciences related to the national defence, order protection and the public administration. This makes possible to analyze the complex security in a unified system. The conditions of the wide-ranging, international scientific research work will be provided at the new university. The article presents the organizational, technical opportunities of this (researcher network, HBONE+, supercomputers, grids, cloud).

Kulcsszavak: *Nemzeti Közszolgálati Egyetem, Biztonság fogalma, Információgyűjtés fajtái (módjai), Információszerzés fajtái (módjai), Globális, elektronikai információgyűjtés, Kritikus infrastruktúra, Cloud – felhő, Szuperszámítógép, Grid, Kutatói hálózat, Videotorium*

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM ÉS A BIZTONSÁG KAPCSOLATA

Az új Nemzeti Közszolgálati Egyetem megalakulásával létrejön egy olyan kedvező állapot, amelyben a széles értelemben vett biztonság megteremtésének tudományos platformja egy intézményhez kötődik. Ez az új egyetem a honvédségi, rendvédelmi és közigazgatási vezetők képzését végzi és ez a három széles oktatási terület szinte teljes egészében felöleli a biztonság megteremtésének elméletével kapcsolatos témaköröket. Ha, ezen széles értelemben vett biztonság megteremtésének konkrét gyakorlati teendőivel minden tekintetben nem is az említett három nagy társadalmi kategória foglalkozik, de a biztonság elméleti, kutatási, tudományos aspektusai minden vonatkozásban a kompetenciájukat képezik.

Először is körvonalazzuk, hogy mit értünk a széles értelemben vett biztonság fogalmán.

A biztonság fogalma [1]

A biztonság olyan állapot, amelyben a fenyegetések, veszélyhelyzetek feltárásra kerültek és ki lettek dolgozva azok a megelőző, védelmi, elhárító, felszámoló intézkedések, amelyek kizárják, akadályozzák, enyhítik, helyreállítják a bekövetkezett káros hatások következményeit, valamint ezek végrehajtásához rendelkezésre állnak a megfelelő tervek, modellek, felkészült erők, eszközök.

Kiindulásként azt kell megállapítani, hogy a biztonság az egy állapot, egy természetesen kialakuló állapot, amely a veszélytényezők feltárásával befolyásolásra kerül.

Miért van egy természetes állapota a biztonságnak?

A biztonság alanyai lehetnek személyek, természeti képződmények, objektumok, létrehozott alkotások, politikai koncepciók, adatok. Ezek közül legfontosabb a személy biztonsága. A természeti képződmények alatt mindazon környezeti- és természetes értékeinket értjük, amelyek földrajzilag kialakultak, mint például erdők, tavak, folyók, növények, állatvilág. Az objektumok közé tartoznak mindazon létesítmények, amelyeket az ember hozott létre az életkörülményeinek fenntartására. Ezek lehetnek az épületek, gyárak, hidak, utak és még számtalan más műtárgy. A létrehozott alkotások az ember szellemi termékei, illetve szellemi termékének tárgyiasult megjelenési formái, médiumok, kutatási eredmények, gépek, műszerek, könyvek, szoftverek, egyéb tárgyak és művészeti alkotások. Az adatok a fentiekre vonatkozó jellemzők dokumentációit tartalmazzák.

A biztonság eme alanyai valamilyen környezetben élnek, funkcionálnak, léteznek, tárolódnak és ez az a környezet, amely a természetes állapotot kialakítja. Valamelyik alany a tengerparton, másik folyók mellett, harmadik hegyes területen vagy nagyvárosban él, települt, található. Ez a helyhez való kötődés határozza meg alapvetően a biztonsági állapotot, mivel minden helynek mások az objektíve kialakult veszélytényezői.

A tengerparton veszélyforrás lehet a cápatámadás vagy a szökőár. A hegyes területen a lavina vagy szakadékba zuhanás. A nagyvárosban a bűnözők. Számítóközpontban a hackerek. Folyóparton az árvíz. Törésvonalak mentén a földrengés. Gazdaságilag stabil térségekben az illegális migráció és a drogeladás. Politikailag feszült térségekben a háború, terrorizmus.

Ezért egy természetes állapot a biztonság, hiszen a veszélyforrások a biztonság alanyaitól függetlenek, objektíve léteznek.

De ez az állapot befolyásolható a veszélytényezők feltárásával. Ha a veszélytényezők feltárásra kerülnek, akkor az állapot minősége javítható, azaz a biztonság növekedni fog. A jól beazonosított veszélytényezők alapján lehet a fogalomban lefektetett alapvetések (megelőző, védelmi, elhárító, felszámoló intézkedések / tervek, modellek, felkészült erők, eszközök) megvalósítása. Ezen alapvetések arra hivatottak, hogy egyrészt kizárják a veszélytényezők hatásait, de legalábbis mérsékeljék azokat, másrészt pedig a bekövetkezett káros hatások felszámolása szervezetten, hatékonyan kerüljön levezetésre.

Csak két egyszerű példa a biztonság állapotának növelésére. Ha egy útvonal jelentősen kanyarog, ez természetes állapot a terep adta lehetőségek miatt. A biztonság ezen útvonalon, a veszélytényezők helyes feltárásával, sebesség korlátozással és előzési tilalommal fokozható. Másik példa, ha a turista útvonal szakadék mellett halad el, akkor korlátot kell építeni az útvonal mentén a biztonság fokozására.

Tudományos kutatók a biztonságot sok szempont alapján másként és másként értelmezik. [2] Én azokkal értek egyet, akik komplex értelemben közelítik meg a biztonságot, azaz a széles értelemben vett biztonságtartalmat vizsgálják.

Általában a biztonság szűkebb értelmezése során a kritikus infrastruktúrák védelmét tekintik sok esetben a vizsgálat tárgyának.

Ha biztonságot a komplex értelmében vizsgáljuk, megállapítható, hogy az nagyon széles területet ölel fel.

Ezek közül, a teljeség igénye nélkül, néhány fontosabb elem felsorolása is jól mutatja a bonyolultságát, összetettségét: pénzügyi- gazdasági biztonság, katonai biztonság, államhatárok biztonsága, rendvédelem biztonsága, katasztrófák elleni biztonság, tűzvész elleni biztonság, élelmiszer biztonság, ökológiai biztonság, egészség biztonság, egyéni biztonság, információbiztonság, jogbiztonság és még hosszan sorolható lenne a biztonság elemrendszere.

A komplex biztonság ezen elemei szorosan összefüggnek egymással, hatnak egymásra, feltételezik egymás érvényesülését. Például, pénzügyi- gazdasági biztonság nincsen katonai biztonság, államhatárok biztonsága, rendvédelem biztonsága, információbiztonság, jogbiztonság nélkül. De az államhatárok biztonsága sem tartható fenn a pénzügyi- gazdasági biztonság, katonai biztonság, rendvédelem biztonsága, információbiztonság, élelmiszer biztonság, jogbiztonság nélkül. Az összefüggések szinte megszámlálhatatlan kombinációban érvényesülnek.

A biztonság megteremtéséhez információkra van szükség, amely információk első sorban az állapot szintjéről, minőségéről adnak tájékoztatást, illetve a fenyegetettségeket tárják fel. [3]

Az állapot szint és a minőséget leíró információ egyrészt a biztonság alanyainak körülményeiről ad tájékoztatást, másrészt a védekező, elhárító, megelőző, következmény felszámolási erők és eszközök képességeit, lehetőségeit veszi számba.

A fenyegetettségek feltárására számtalan módszer és modell (PTA - Practical Threat Analysis – Gyakorlati Fenyegetés Elemzés, SWOT, PEST, Hibafa, Fenyegetés mátrix, Sérülékenység és kockázatértékelés, Realistic Threat Scenario – Várható Fenyegetés Forgatókönyv, Real-Time Vulnerability Analysis – Valós-idejű Sebezhetőség Elemzés, RISK – Monte Carlo szimuláció stb.) áll rendelkezésre, amelyeknek az alapja szintén az információ. Az információgyűjtés (információszerzés) fajtái (módjai)[1] a hagyományos értelemben két fő csoportra oszthatók, a titkos információgyűjtésre és a nyílt információgyűjtésre.

Napjaink technológiai fejlődése, az internet térhódítása, a világ digitalizálódása, a robottechnológia fejlődése kitermelte a harmadik információgyűjtési módot, a globális elektronikai információgyűjtést.

Ez az információgyűjtési mód (fajta) nem sorolható sem a titkos, sem a nyílt információszerzési módhoz (fajtához), mivel mindkét hagyományos információgyűjtési mód (fajta) jellemzőt magán hordozza, illetve nincsen tér- és időbeli korlátja.

A titkos információgyűjtés általában jogellenes cselekmények felderítésére valamint államérdek szavatolására irányul titkosszolgálati eszközökkel, azaz rejtve folyik úgy a célszemélyek, mint az egész társadalom tekintetében. [4]

[1] A szakirodalom módot és fajtát is említ.

A nyílt információgyűjtés a publikus adatok összegyűjtését jelenti nyilvános módon. Nem sérti a személyiségjogokat. Köztudott úgy a célszemélyek, mint a társadalom előtt.

A globális elektronikai információgyűjtés nyílt abban a vonatkozásban, hogy mindenki előtt ismert az a tény, hogy vannak műholdak, amelyek kamerái olyan felbontással rendelkeznek, hogy a gépkocsi rendszáma is látható a műholdképen, mindenütt biztonsági- és térfigyelő kamerák pásztázzák a terepet, objektumok környékét és rögzítik a történéseket.

Titkos olyan formában, hogy nem tudjuk, ki, mikor, milyen célból készít rólunk videofelvételt és azt mire használja fel. Mindenki életében lehetnek kényes pillanatok, amelyeknek a közzététele sértheti a személyiségjogokat, erkölcsi kárt okozhat a számára. Az a rövid ruhában, fehérnemű nélkül előrehajoló hölgy, - akiről egy élelmiszerüzlet biztonsági kamerája készített hátulról felvételt és az kikerült az internetre, mint jó sztori, - nem biztos, hogy hozzájárult volna a nyilvánossá tételhez. A kétezres évek elején, amikor a Határőrség technikai korszerűsítése kapcsán a határőr járőrrádiókba GPS nyomkövető került beépítésre, azt az adatvédelmi biztos aggályosnak találta, mivel a járőr tartózkodási helye így állandóan követhetővé vált és ez véleménye szerint sértette a személyiség jogokat.

Globális, mert térben, időben határtalan, a korszerű automatizált eszközök az egész földet átfogva, a nap minden másodpercében képesek az események rögzítésére.

A műholdak az egész földfelszínt látják, az internet behálózza az egész világot, ha egyszer valaki fellép a világhálóra, akkor annak az összes virtuális kalandozása nyomon követhető, a hackerek mindent megtudhatnak róla, bankszámlája virtuális rablás áldozatává válhat. A mobiltelefonok figyelésével a használó személy mozgása, fizikai tartózkodási helye rögzíthető, a bankkártya használata megint csak helyszíni nyomot hagy maga után. A video- és infrakamerák bárhol elhelyezhetők, éjjel nappal képesek figyelni, elektronikusan rögzíteni a történteket. Más számtalan mozgásérzékelő és felfedő szenzor is használható az emberek tevékenységének figyelemmel kísérésére. A 2010-es influenzajárvány kapcsán napvilágot láttak olyan híresztelések, hogy a védőoltással mikrocsipet ültetnek az emberekbe. Ez technikailag lehetséges, hiszen a kutyák, macskák nyilvántartására már alkalmazzák az ehhez hasonló módszert.

Ezek a berendezések, eszközök mind elektronizáltak, intelligensek, emberi felügyelet nélkül képesek folyamatosan működni és elektronikusan, többnyire digitalizáltan rögzítik, tárolják az általuk begyűjtött információkat. Ez a digitalizált információ az adatátviteli hálózatokon gyorsan, torzításmentesen továbbítható a világ bármely pontjára.

Amíg a két hagyományos információgyűjtési fajta nagyrészt analóg módszerekre épül (dokumentum elolvasása, élő beszéd, fénykép, hangfelvétel, telefon lehallgatás stb.), a megszerzett információ is analóg információhordozóra kerül, addig a globális elektronikai információ már eredendően digitalizált formában keletkezik. A hagyományos módon megszerzett információt a gyors továbbításhoz, a számítógépi tároláshoz a hatékony feldolgozás érdekében először digitalizálni kell, amely időbe kerül, korszerű és drága eszközöket igényel.

A globális elektronikai információgyűjtés adathordozója már digitális eszközökön és módszereken alapul, így azonnal feldolgozható és továbbítható elektronikus hálózatokon. Egy videokamera által rögzített személy arcképe azonnal lefuttatható egy arcfelismerő programon és találat jelezhető ki, ha ezen személy valamilyen célból szerepel az ellenőrzést végző szervezet arckép archívumában.

A fentieket alapul véve, célszerű az információgyűjtés módjait (fajtáit) az alábbiak szerin meghatározni.

Információgyűjtés módjai (fajtái):

- nyílt;
- titkos;
- globális elektronikai.

A biztonság szintje emelésének egyik fontos eszköze lehet a globális elektronikai információgyűjtés. Természetes, e mellett a nyílt és titkos információgyűjtés jelentősége sem csökken. A globális elektronikai információgyűjtés egyrészt irányulhat a védendő objektum állapotának figyelésére, másrészt a veszélyteményezők feltárására. A globális jellegnél fogva időben szakadatlanul lehet a védendő objektumról a szükséges adatokat gyűjteni és elektronikusan feldolgozni. Ha a vörös iszap tározó folyamatosan ellenőrizve lett volna valamilyen videokamera rendszerrel, akkor a gáton fellépő repedés időben észlelhető lett volna. Vannak olyan intelligens kamerák, amelyek változás észlelésekor automatikusan riasztó jelzést adnak. A kialakuló veszélyhelyzetek szintén időben felfedhetők a globális elektronikai információgyűjtő eszközökkel. Ilyenek is már számtalan helyen üzemelnek, mint például a szökőár előrejelző rendszer, a különböző meteorológiai mérőállomások, vulkántevékenység felmérő berendezések, hő-kamerák a határőrizetben stb.

AZ ÚJ NEMZETI KÖZSZOLGÁLATI EGYETEM K+F+I LEHETŐSÉGEI

A biztonság és az információgyűjtés alapvetésekből kiindulva, az új Nemzeti Közszolgálati Egyetem K+F+I tevékenysége elméleti szinten a biztonság széles értelemben vett területeire irányulhat, amíg gyakorlati téren csak a kritikus infrastruktúra védelmének kutatását célszerű művelnie.

Mi indokolja a biztonság széles értelemben vett körére irányuló elméleti kutatómunka felvállalását?

Első sorban a hadtudomány tágabb értelemben való felfogása, vizsgálata, másod sorban az új Nemzeti Közszolgálati Egyetem tudomány művelő területeinek összetétele. [5]

A három ősi mesterség egyike a harc, a másik az ezzel szorosan összefüggő kémkedés, a harmadik a „rosszlánykodás”. A harc az ember kifejlődésével együtt jelent meg, hiszen az ember harcot folytatott a természettel, harc volt a vadászat, harc volt a saját védelme más támadókkal szemben. A fejlődés során a harc tudománya a hadtudomány lett. A harcot nem biztos, hogy le kell szűkíteni a fegyveres küzdelemre, sok fegyverek nélküli küzdelem is folyik az emberi tevékenységek során. Példaként nézzük a biztonságot.

Bármely elemét vizsgálva is a biztonság megteremtésének, azt kell megállapítani, hogy az egy küzdelem, harc folyamán valósul meg. Ezen harc, küzdelem alatt nemcsak a fegyveres harcot és küzdelmet kell érteni, hanem a szellemi, jogszabályi, politikai, gazdasági, rendfenntartási, emberi viszonyalakítási, feltétel megteremtési, objektum-, eszköz- és létesítményalkotási szinten folytatott harcot, küzdelmet is. Ha tovább folytatjuk a nem fegyveres harc és küzdelem megvívásának elemzését, akkor azt kell megállapítanunk, hogy mindegyikben fellelhető a klasszikus fegyveres harc megszervezésére és megvívására irányuló úgynevezett „parancsnoki munka” folyamata és elemrendszere, csak az más szavakkal történik kifejezésre.

Azt senki nem tagadhatja, hogy bármely, nem fegyveres jellegű tevékenység során is meg kell érteni, hogy mit akarunk végrehajtani, szükség van időütemezésre, a körülmények, lehetőségek feltárására, a feltételek megteremtésére, tervezésre, szervezésre, a folyamatok irányítására, a szükséges beavatkozásokra anomáliák esetén. Különböző módszertanok láttak napvilágot a nem fegyveres folyamatok megszervezésére, irányítására. A teljesség igénye nélkül, csak párat említve, léteznek különböző projekttervezési és -levezetési módszertanok (PRINCE, SSADM, PCM, LFA, TOGAF), időütemezési eszközök (Gantt diagram), SWOT,

FMEA, HAZOP, HRA, QRQ, ETA, PEST elemzés, hibafák (FTA), kockázati tényező mátrix, folyamat gráfok, különböző számítógépi elemző, modellező programok.

Az is nyilvánvaló, hogy a hadtudomány az a tudomány, amely a legrégebb idők óta tárja fel a harc megvívásának általános és specifikus törvényszerűségeit, dolgozza ki a harc előkészítésének, megvívásának elveit, gyakorlatát, emberi és technikai feltételeit.

Ezek alapján célszerű a hadtudományt a legszélesebb értelemben felfogni, és ebből leszármaztatni a nem fegyveres küzdelem megvívásának tudományos megalapozását, így a rendvédelem, rendészet, államigazgatás területeken is. A hadtudomány foglalkozhat a fegyveres és a nem fegyveres harc általános törvényszerűségeivel, elméletével, a fegyveres harc specifikus törvényszerűségeivel, elméletével, az egyes kialakuló tudományok, mint például a rendvédelem tudomány az adott terület specifikus törvényszerűségeit kutathatja és elméletét dolgozhatja ki.

A létrejövő új Nemzeti Közszolgálati Egyetem képzési portfoliója folytán teljes egészében képes a fenti alapvetés mentén a hadtudomány általános és specifikus területeinek művelésére. Gondozhatja a fegyveres harc tudományát, a kialakulóban lévő rendvédelemmel kapcsolatos tudományt, valamint az állam működtetéséhez kapcsolódó tudományokat. Ha ezt a három területet vesszük vizsgálat alá, akkor azt a következtetést kell levonnunk, hogy a komplex biztonság összes elemét elméleti szinten magában foglalják ezen tudományok. A biztonság egyetemes voltából adódik, hogy tudományos megalapozottságát is egyetemes módon kell felfogni.

Az élet bármely területét vizsgálva azt kell megállapítani, hogy a hadtudomány szinte minden tudományból merít, interdiszciplináris tudomány is, a konkrét fegyveres küzdelem megvívásának tudománya mellett. Bármelyik más tudományt tekintjük át, az a hadsereg, rendvédelem, közigazgatás területén sajátos formában megjelenik. Csak pár példa a szemléltetés kedvéért. Az egészségtudomány elengedhetetlen a harctéri gyógyításban, az élelmiszer- és vízbiztonság a hadseregek, rendvédelmi szervezetek, állami és önkormányzati intézmények élelmezésében, a meteorológia, fizika, aerodinamika a repülésben, az építő- és gépészmérnöki tudás az erődítésben, harcjárművek, fegyverek gyártásában, alkalmazásában, a vegyi, biológiai tudományok a tömegpusztító fegyverek kifejlesztésében, illetve az ellenük való védekezésben, a rádióelektronikai, informatikai tudományok az összeköttetés és információbiztonság megteremtésében. De még véget nem érően lehetne sorolni az összefüggéseket.

Az egyetemes szemléletből fakad, hogy az új egyetemnek célszerű lenne kialakítania egy akadémiai kutatócsoportot a komplex értelemben vett biztonság elméleti téziseinek kutatására, törvényszerűségeinek feltárására, tudományos megalapozottságának megteremtésére.

A biztonság gyakorlati megvalósítása számos más tudományhoz, intézményhez kapcsolódik, amelyek a biztonság egy-egy részével, szeletével foglalkoznak, ezeknek a részterületeknek tudna az akadémiai kutatócsoport egységes koncepciót, egységes célkitűzést meghatározni.

Ha áttekintjük a kritikus infrastruktúra elemeit, akkor arra a megállapításra kell jutnunk, hogy az új Nemzeti Közszolgálati Egyetem képzési portfoliója szinte teljes egészében lefedi azokat a biztonsági területeket, amelyek a kritikus infrastruktúra védelmét szolgálják. [6]

Ebből fakad az a következtetés, hogy az új egyetem gyakorlati kutatási irányait a kritikus infrastruktúra védelem mentén célszerű felépíteni.

A kritikus infrastruktúra értelmezése is sokszínű, de abban minden kutató egyetért, hogy az állam működőképességét, a biztonságot szavatoló létesítmények, erőforrások, energiaforrások, információtechnológiák tartoznak a kritikus infrastruktúrák közé. [7]

Magyarországon a 2112/2004. (V.7.) kormány határozat a következő területeket sorolja a kritikus infrastruktúrák közé:[2]

- energiaellátás;
- közművesítés;
- közlekedés és szállítás;
- távközlés, elektronikus adatforgalom és informatikai hálózat;
- bankrendszer;
- szolgáltatások;
- média;
- ivóvíz es élelmiszer alapellátás;
- egészségügyi biztosítás.

Ha megvizsgáljuk a hon-és rendvédelem aktuális problémáit, akkor több olyan markánsan körvonalazódó kutatási területet lehet fellelni, amelyben az összes katonai- és rendvédelmi szervezet érintett.

Egyik ilyen terület a környezetvédelem és a vele szoros összefüggésben lévő katasztrófavédelem, amelyben a hon-és rendvédelem, valamint az államigazgatás egyrészt, mint környezetszennyező, másrészt, mint környezetvédő vesz részt. Említett szervezetek járműveket használnak, rengeteg energiát fogyasztanak, veszélyes anyagokkal dolgoznak, amelyek szennyezik a környezetet. Ha sikerül új technológiákat, alkalmazási eljárásokat és eszközöket kifejleszteni, akkor a környezetkárosítás, a környezetszennyezés nagymértékben csökkenthető, ezáltal az egyes katasztrófákat kiváltó okok is mérsékelhetők. De a felsorolt szervezetek hatáskörébe tartozik több tekintetben a környezetkárosítás felfedése, intézkedések meghozatala annak megszüntetésére. Szintén új technológiák, eljárások kutatásával, létrehozásával a felfedés hatékonysága jelentősen fokozható. [8]

Másik általános terület az informatikai védelem. A hon-és rendvédelemi szervek, az államigazgatási apparátus azok közé a célobjektumok közé tartozik, amelyek a támadások középpontjába kerülhetnek úgy a hackerek, mint a terroristák vagy az ellenséges hírszerzés tekintetében. Az egyéb célobjektumok (bankok, energiaellátás stb.) elleni támadás felfedésében, a bekövetkezett támadás elkövetőinek felfedésében a rendvédelmi szervek alapvető szerepet játszanak. Létező veszély, ha még látens állapotban is van az elektronikai harc, a kybertámadás, robothadviselés. [9], [10]

Szintén jelentős veszélyforrás az illegális migráció, a fegyver-, drog-, hasadóanyag- és emberkereskedelem. Ez a veszélyforrás kategória az egész társadalmat érinti, amelynek felfedésében, akadályozásában szintén a hon-és rendvédelemi szervek, az államigazgatási apparátus az, amelyek a fő szerepet játsszák.

A rendvédelem minden területén előtérbe kerül a biztonság fokozásának egyik eszközeként az automatikus terep- és létesítményfelügyelet.

A rendőrség a schengeni külső határok őrizetében alkalmaz mobil és telepített hő-kamerákat, repülőkre szerelt kamerákat az EU határőrizeti akciók során vet be, illetve az egyéb rendezvények biztosítása és a közlekedési jogsértések felderítése során térfigyelő kamerákat vesznek igénybe. Több rendőrjárőr autó el lett látva eseményt rögzítő kamerával. Ezen kívül más érzékelőket is alkalmaznak a tevékenységek során az objektumok védelmére, zárt területre való behatolás felfedésére, mint lézerkerítést, hang- és mozgás érzékelő

[2] 2080/2008 (VI. 30.) Korm. Határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

berendezéseket. Történtek kísérletek felfüggesztett léggömbre szerelt kamerákkal való terep- és esemény felügyeletre is.

A NAV szállítmányok, földbe rejtett tárgyak felfedésére alkalmaz különböző szenzorokat.

A BVI objektumvédelemre és fogvatartott követésre használ, illetve tervez használni szenzorrendszereket.

A rendvédelmi kutatás tárgyát képezhetné olyan átfogó térinformációs rendszer kiépítése is, amelyben az esemény bekövetkezése időpontjától kezdve az automatikus szenzorrendszerek felfednék az eseményeket, majd rögzítenék digitális térképen azok helyszínét, GPS rendszeren keresztül követnék és időbélyeggel ellátnák minden beavatkozó mozgását, ezzel biztosítva hatékony együttműködésüket, a rendszer az automatikus szenzorrendszerek folyamatos információközlése alapján térinformációs elemzéssel bevetési célszerűség, együttműködési és hatásmodellezést végezne.

Az egységes térinformációs rendszer alapját a határrendészeti, közterület felügyeleti, bevetés irányítási jelenleg működő térinformációs rendszerek, valamint a Robotzsaru képezné.

A katonai, rendvédelmi és államigazgatási szervek is nagy energiafogyasztók, ezért fontos lenne az alternatív és megújuló energiaforrások alkalmazási lehetőségeinek kutatása.

A parafa granulátum nanotechnológiai elegyítése a szénnel olyan hő-, hang szigetelő, korrózió gátló, kopásálló, infrasugár- és rádióhullám elnyelő anyagot képez, amelynek számtalan előnye kihasználható lenne a kritikus infrastruktúrák védelmében.

Ha áttekintjük a kritikus infrastruktúra védelem EU –ós megítélését, azt láthatjuk, hogy a fent nevesített kutatási területek jól illeszthetők az EU –s elképzelésekhez.[11]

A kutatói hálózatok és a klaszterek lennének azok a kapcsok, amelyek az egyetemi elméleti alapvetéseket és az egyes részterületek gyakorlati kutatómunkáját, tudomány alkalmazását harmonizálnák, a kutatási eredményeket közkinccsé tennék.

A KUTATÓI HÁLÓZATOK LEHETŐSÉGEI

A felsőoktatási intézmények számára a kutatói hálózatok hatékony működéséhez az infrastrukturális feltételek rendelkezésre állnak. A NIIF (Nemzeti Információs Infrastruktúra Fejlesztési Intézet), MIT (Magyar Internet Társaság) és a HUNGARNET Egyesület (Magyar Felsőoktatási, Kutatási és Közgyűjteményi Számítógéphálózati Egyesület) közreműködésével létrehozásra került egy nagy sávszélességű hibrid adathálózat, a HBONE+[3].[12]

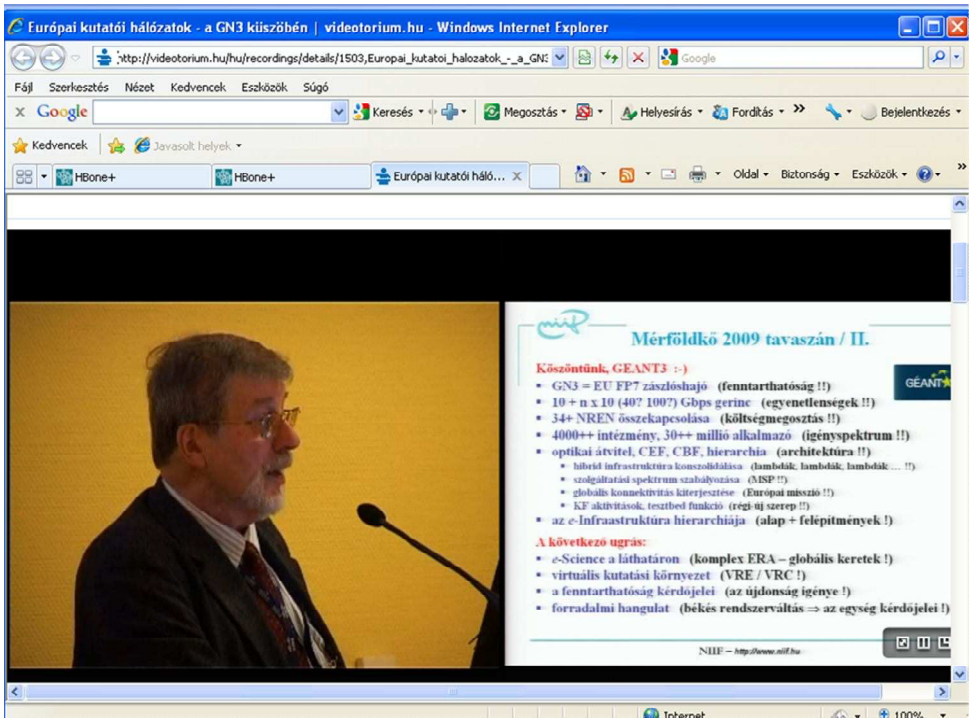
A HBONE+ egy országos gerinchálózat, amelynek feladata, hogy a HUNGARNET tagintézményeket egy nagyterületű, országos gerinchálózattal egymással összekapcsolja, továbbá biztosítsa számukra a nemzetközi kapcsolatot, a teljes Internet hozzáférést. A HBONE kialakítása, fejlesztése az NIIF Műszaki Tanácsa, illetve a HBONE hálózatot üzemeltető menedzserek által közösen kidolgozott és az NIIF vezető testületei által jóváhagyott terveknek megfelelően folyik.[4] [13]

A kutatói hálózatok nemcsak nemzeti, hanem nemzetközi szinten is kiépítésre kerültek.

Az európai kutató hálózat a GEANT3 ((Gigabit European Academic Networking Technológy) GN3).

Az európai kutató hálózatokról bővebben Bálint Lajos NIIF nemzetközi kapcsolatok igazgatóhelyettese Networkshop előadásából lehet ismereteket nyerni.[5]

3 http://www.hboneplus.hu/node/98 Dr. Nyitrai Zsolt infokommunikációs államtitkár átadta az NIIF Intézet új generációs hibrid hálózatát. 2010. december 9-étől elérhetővé válik Magyarországon az ún. hibrid hálózat.
4 https://nws.niif.hu/
5 http://videotorium.hu/hu/recordings/details/1503,Europai_kutatoi_halozatok_-_a_GN3_kuszoben



A TERENA *Trans-European Research and Education Networking Association* - Trans-Europai Kutató és Oktató Hálózati Egyesülés és az ERAB *European Research Area Board* – Európai Kutatási Terület Egyesület szintén a kutatói hálózatok közé tartoznak.

A GRNET (Greek Research and Technology Network - Görög Kutatás és Technológia Hálózat) és a GEANT projektek a grides alkalmazások közé tartoznak. Ezeket a projekteket az EU FP7 keretprogram támogatja.

Mi indokolja a kutatói hálózatok fejlesztését?

Ha megvizsgáljuk a 21. század fejlődési trendjeit, akkor számos olyan ismérv fedhető fel, amelyek az on-line együttműködés szükségességének irányába hatnak.[6]

- kialakulóban van a digitális társadalom, új IT (információ technológia) alapú közösségek jönnek létre;
- globális kényszer igényli a termelékenység növekedését, a hozzáadott érték fokozását, az IT tudásmenedzsment magas szintjét, a jó minőségű adatok és informatikai hálózatok meglétét;
- nemzeti populáció egyre heterogénebb lesz;
- nemzeti oktatási rendszerek produktivitása kezd elmaradni a gazdaság igényeitől;
- kreativitás, innováció növekvő hatalma;
- feldolgozói programok portál alapúvá válása (webes alkalmazások);
- strukturálatlan adatfeldolgozási technológiák terjedése;
- maga a technológia már nem elégséges, hanem az a lényeg, hogy a technológia milyen szolgáltatásra képes;
- ICT (infó kommunikációs technológiák) uralma;

[6] Networkshop 2011 konferencia Kaposvár 2011.április 27-29. plenáris előadások, Prof. Dr. Kroó Norbert akadémikus, MTA alelnök, Tázló József műszaki igazgató CISCO Systems Magyarország Kft., Veres Zsolt vezérigazgató IBM Magyarország

- digitális tartalmak terjedése (multimédia, tudásbázisok, videotorium[7], repozitorium, videokonferencia);
- grafikus processzorok szükségességének növekedése;
- tudásgazdaságok lesznek csak életképesek;
- az internet a tárgyak hálózata lett;
- az IT elérkezett a harmadik fejlődési mérföldkőjéig, a szuperszámítógépekhez[8] és cloud[9] –hoz (felhő).

A fenti trendek jól mutatják, hogy a gazdaság, az oktatás olyan környezetbe kerül, amelyben az információ, az új kommunikációs eszközök és az új technológiák játsszák a fő szerepet. A globális kényszer generál egy összefüggést. A gazdaság, a társadalom működéséhez egyre több, jó minőségű, gyorsan megszerezhető információra van szükség, de ezen információkat egy globális, hatalmas információhalmazból kell kinyerni, ugyanakkor az információ elévülési időtartama is erősen lecsökken. Lehet, hogy egy megszerzett pénzügyi információ, pár óra múlva már értéktelenné válik. Az innováció, hatékonyság sok esetben megköveteli a csoportmunkát, nagy számításigényű feladatvégzést, a legkorszerűbb eszközök és technológiák alkalmazását. Viszont a ráfordítás – létrehozott érték viszony annál jobb, minél nagyobb mértékben használható a meglévő eszközpark és technológia. Ezekből generálódik az ellentmondás, ha valaki nem használ újabb és újabb eszközöket, technológiákat, az lemarad az innovációs küzdelemben, de ha beruház új eszközökre és technológiákra, akkor a nyeresége csökken, illetve nincs is forrása beruházásra. Ez a probléma fokozottan jelentkezik a költségvetési szerveknél. Az igény nő a korszerűsítés, az állampolgárok számára nyújtott szolgáltatások minőségének javítására, de nincsen pénz beruházásokra.

Ezen ellentmondás feloldására látszik járható útnak az IT fejlődés harmadik mérföldköveként megjelenő szuperszámítógépek rendszere és a cloud (felhő).

ÚJ TECHNOLÓGIÁK ÉS MODELLEK (SZUPERSZÁMÍTÓGÉP, GRID, CLOUD / FELHŐ) A TUDOMÁNYOS KUTATÁS SZOLGÁLATÁBAN

„Az intézmények egyre gyorsuló ütemben növekvő adattárolási igényeinek a biztonságos kiszolgálásához megbízható, költséghatékony, nagy teljesítményű elosztott adattárolási infrastruktúrára van szükség. Ezt az adattárolási igényt a fejlesztés eredményeként egy - a közelmúltban világszerte újdonságként megjelent - "cloud computing" architektúra segítségével tudjuk majd a felhasználóink rendelkezésére bocsátani, pl. adatmentési és adatbányászati célokra. Nem tévesztjük szem elől, hogy a nemzetközi tapasztalatok szerint az európai kutatók meghatározó többsége (mintegy két-harmada) már 1 Tflops teljesítménynél nagyobb számítási erőforrásokhoz is hozzá tud férni, ami egyrészt jelentősen növeli Európa kutatási-fejlesztési potenciálját és versenyképességét, másrészt viszont kihívást is jelent a nemzeti - köztük a magyarországi - fejlesztések számára. A projekt eredményeként a Magyarországon elérhető kapacitás meg fogja haladni az 5 Tflops értéket, ami már biztosítani fogja a magyar kutatók versenyképességét. Mindezeken túl a szuper-számítástechnikai fejlesztések eredményeként Magyarország az európai szuperszámítógépeket és grideket integráló konzorciumoknak (PRACE, DEISA) is teljes jogú tagja lehet, így a hazai kutatók az

[7] http://videotorium.hu/hu/recordings/details/1503,Europai_kutatoi_halozatok_-_a_GN3_kuszoben
[8] Tázló József (műszaki igazgató CISCO Systems Magyarország Kft) előadása a Networkshop 2011 konferencia Kaposvár 2011.április 27-29. plenáris ülésén (első mérföldkő 1981 IBM PC –k megjelenése, második 1951 UNIVAC I kereskedelmi forgalomban megjelenő számítógépek)
[9] Később kifejtve

Európai Unió keretében elérhető kapacitásokhoz is az eddigieknél jóval egyszerűbben tudnak majd hozzáférni."[10]

A szuperszámítógépek óriási kapacitású, nagyon gyors számítógépek, amelyeknek a szolgáltatásai bérelhetők.

A cloud (felhő) olyan IT működési modell, amelyben a felhasználónak nincsen szüksége drága hardver eszközökre, alkalmazói szoftverekre, IT szakembergárdára, állandó fejlesztési beruházásokra, csak egy egyszerű monitorra, billentyűzetre és megbízható, nagy sávszélességű adatátviteli hálózatra.[11]

Mit takar ez a modell? Az összes hardver eszköz, alkalmazó program valahol a világban, jól védett, többszörös redundáns megbízhatósági szinten lévő szerverfarmokban nyer elhelyezést. A Microsoftnak konténer rendszere van, egy konténerben több száz szerver üzemel, amelyek meghibásodás esetén automatikusan átadják a processzeket a másik, működő szervernek, az alkalmazó ebből semmit nem vesz észre. Ha egy bizonyos százaléka meghibásodik a szervereknek, az egész konténert lecserélik egy új, teljes működő képességű konténerre.

Az IT szakembergárda is ezeken a szerverfarmokon található, a fejlesztés a szerverfarm üzemeltetőjének feladata, amely azt eredményezi, hogy mindig a legkorszerűbb eszközök és technológiák állnak a felhasználó számára.

A felhasználó egy bérleményen keresztül jut hozzá ezen szerverfarm szolgáltatásaihoz. Ha például az adott cégnek gépelési, számítási feladatai vannak, akkor szövegszerkesztői és táblázatkezelői szolgáltatásokat bérel, ha Microsoft környezetben van, akkor a felhőben lévő valamely szerverpark számítógépén fut a Word és az Excel is. A cég a monitorján és az adathálózatán keresztül a felhőben futtatja ezt a két szoftvert, az adatait is a felhőben tárolja, csak az eredményeket jeleníti meg a cég eszközein. [14]

Mit jelent ez az adott cég számára? Első sorban beruházási és működési költségmegtakarítást. A 2011. április 28.-án megtartott Microsoft Cloud konferencián bemutatott számvetések alapján a beruházáson 70% -t, a működtetésen 50% -t lehet megspórolni. Másod sorban ez a cég az innovációs versenyben állandóan az élen halad, hiszen szolgáltatásként mindig a legkorszerűbbet kapja.

Természetesen a felhőmodell kérdéseket is felvet. Egyik ilyen kérdés az informatikai biztonság, a másik a kiszolgáltatottság. A részletek elemzése nélkül is jól látható, hogy az adott cég teljes mértékben a felhő működtetőjétől függ, hiszen nála vannak az adatai, az adatokat feldolgozó eszközök is, nem a saját irodájában, ha kell vaslemez szekrényben jól elzárva. Másik ilyen kockázati tényező az adatkapcsolat, adatátviteli hálózat megbízhatósága. Ha megszakad az adatkapcsolat, az említett cég működésképtelenné válik.

A felhőt üzemeltetők az informatikai biztonság magas szintjének megteremtésére garanciákat adnak, a jogi környezetet is folyamatosan alakítják át, hogy az is garantálja a megbízhatóságot.

A világfejlődési trendeket figyelve, nem lesz más választása sem a cégeknek, sem a költségvetési szerveknek, mint a felhőbe való bekapcsolódás. Olyan rohamos a technikai fejlődés, olyan gyorsan jönnek ki a piacra az új, modern eszközök, hogy azokat nem lesz képes a cégek, a költségvetési szervek mindegyike megvenni, mivel az új eszköz megjelenési ideje töredéke a meglévő eszköz amortizációs idejének. De aki nem alkalmazza az újat, az lemarad a versenyben. Ezért nem lesz más alternatíva, mint a felhő alkalmazása.

A rendvédelmi szervek is előbb – utóbb rákényszerülnek a felhő használatára. Már most jelentkezik az a gond náluk, hogy a tíz éves számítógéppark egyre kevésbé tud helytállni az elvárásoknak, de fejlesztésre nincsen forrásuk.

[10] http://www.hboneplus.hu/node/25

[11] http://videotorium.hu/hu/recordings/details/2738,Szekelyi_Szabolcs_-_NIIF_Cloud_NorduGrid

A felsőoktatási intézmények és a közgyűjteményi intézmények számára a HBONE+ projekt teremti meg a felhő használatának lehetőségeit. A digitális tartalmak használata nélkül már nem képzelhető el egy korszerű oktatás, egy jól működő könyvtár, viszont a digitális tartalmak létrehozása, alkalmazása gyors, modern számítógépeket igényel, tárolásuk pedig óriási tárkapacitást. Ilyen fokú beruházásra kevés intézmény képes, ezeket a szolgáltatásokat a HBONE+ -tól kell igényelniük. Komolyabb, a K+F+I –t szolgáló kutatásokra sem lesz képes egy-egy egyetem, csak közösségek, amelyek nem nélkülözhetik a szuperszámítógépeket. A közös on-line munkát, a szuperszámítógépeket szintén a HBONE+ tudja adni a kutatóknak.

A felhasználó, például egy egyetem, egy önkormányzat nagyon kevés IT beruházással képes a legkorszerűbb, leggyorsabb, leg megbízhatóbb információrendszert működtetni. Természetes, ezen működtetés pénzbe kerül, de mennél többen használják a felhőt, annál kevesebb lesz a bérleti díj. Jelenleg egy általános szolgáltatás havi 100 euró alatt vehető igénybe.

Felhasználói attitűd váltás is kell a felhő használatához. Sokan még bizalmatlanok, mivel az infrastruktúrára, az adatok tárolására nincsen rálátásuk. A cloud –nak vannak szolgáltatási szintjei, nincs szükség a teljes kiszolgáltatottságra. Elsőként csak az alkalmazói szoftvereket lehet bérelni, majd az infrastruktúrát is, ha a tapasztalatok kedvezőek, az adatbázisok is kihelyezhetők a felhőbe.

A kutatói hálózatok infrastruktúráját is alapvetően a szuperszámítógépek és a grid (nagy sebességű adatátviteli hálózat) alkotják.

A szuperszámítógépek óriási teljesítményre képesek, első sorban a számításigényes feladatokat támogatják. Az űrkutatásban, az élettudományokban, fizikai, kémiai kutatásokban használják őket számítás intenzív modellezésre, szimulációra, adatelemzésre, bio informatikai feladatokra, orvosi képfeldolgozásra, tudományos munkafolyamat gráfok feldolgozására, elosztott számolási infrastruktúrát igénylő tevékenységekre, meteorológiai modellezésekre. Általánosságban egy szuperszámítógép ára 250 millió forint, 1024 processzor magot tartalmaz, vízhűtésű, nagy az áramfelvétele, 24 TB a memóriája, 50 PFlops számítási kapacitása van. Egy ilyen szuperszámítógép például a BlueGene/Q gép.

Magyarországi viszonylatban a felsőoktatási intézményeknek a NIIF Intézet biztosít négy szuperszámítógépet és a grid kialakítását lehetővé tevő HBONE+ nagysebességű adathálózatot. A négy szuperszámítógép a szegedi, pécsi, debreceni egyetemen és az NIIF Intézetnél került telepítésre. Ezen szuperszámítógépek főbb adatai: 50 teraflops teljesítmény, 1536 core 3,33 GHz, 6 TB memória, 500 TB háttértár, Linux operációs rendszer, vízhűtés, vizualizációs szerver erős grafikus kártyával a képi megjelenítéshez. Sajnos, a rohamos technikai fejlődés következtében ezen szuperszámítógépek elavulása 3-4 év alatt megtörténik, az 50 teraflops teljesítmény is jövőre kevés lesz, mivel a számítási kapacitás évente duplázódik.[12]

Vannak olyan feladatok, amelyekre egy szuperszámítógép nem elegendő, ezért kialakítják a grideket[13], amelyekbe több szuperszámítógépet kapcsolnak össze. Például ilyen a HPC projekt, amelyben bulgár, magyar, román és szerb szuperszámítógépek kerültek összekapcsolásra. Magyar részről a projektben az MTA SZTAKI, Óbudai Egyetem és a NIIF Intézet vesz részt. Az Óbudai Egyetem fejleszti az alkalmazói programokat, a DeepAlinger –t és a DiseaseGene –t.[14]

A hibrid technológia teszi lehetővé a gridek létrehozását, azaz IP kapcsolatok mellett pont – pont kapcsolatok is kiépíthetők, dedikált kapcsolatok hozhatók létre az adott kutatásban résztvevő szuperszámítógépek között. A kapcsolat létrehozása az úgynevezett „köztes réteg” (ARC-AREX, gLite) kialakításával és használatával valósítható meg. A köztes réteg

[12] Stefán Péter: Networkshop 2011. Kaposvár előadása
[13] http://videotorium.hu/hu/recordings/details/2738,Szekelyi_Szabolcs_-_NIIF_Cloud_NorduGrid
[14] Röczei Gábor NIIF Intézet: Délkelet-Európai Grid Projekt, Networkshop 2011. Kaposvár előadása

elkészítése bonyolult programozói feladat. Köztes réteg elfedésére portál megoldásokat használnak, ezzel az eszközzel a felhasználók könnyebben hozzáférnek a távoli grides erőforrásokhoz. Az MTA SZTAKI is fejleszt ilyen portálalkalmazást, a gUSE –t.

A desktop grid az önkéntes felajánlásból összeállított grideket foglalja magában. Azok az intézmények, amelyek rendelkeznek szabad kapacitással, ezt felajánlják mások részére a számításigényes feladataik ellátásához. A grid használatának megkönnyítésére kutatások folynak a desktop gridek párosítására a web2 –vel.[15]

Befejezésül elmondható az, hogy az új közszolgálati egyetem széles kutatási lehetőségekhez jut összetétele, felépülése alapján, a kutatás infrastrukturális háttere biztosított lesz a számára.

A karok, de főként az egyetem tudományszervező szakemberei előtt állnak azok a feladatok, amelyek során ki kell alakítani a kutatási koncepciót, meg kell találni azokat a közös hon- rendvédelmi és közigazgatási problémákat, amelyek mentén kialakíthatók a konkrét kutatási programok, létrehozhatók a kutatói hálózatok, klaszterek.

A ZMNE kutatási kapacitásai, eddigi tudományos eredményei, a KKV –kal kialakított jó kapcsolatrendszere és eredményes tudományos együttműködése, jól felkészült, jelentős tapasztalatokkal rendelkezői kutatói megfelelő kiinduló alapot teremtenek az új egyetem kutatási tevékenységének megszervezéséhez.

Mivel a biztonság megteremtésének legfőbb tudományos műhelye is az új egyetem lesz, alapul véve a biztonság globális és egyetemes ismérveit, nem lehet megfeledkezni a nemzetközi, főleg az európai kutatási programokba és kutatási hálózatokba való bekapcsolódásról sem.

Az új egyetem könnyen válhat az EU biztonság megteremtésének vezető tudományos bölcsőjévé. Hiszen, a kiépített biztonsági állapot csak akkor marad tartós, ha az megvédésre kerül. A megvédése állandó harcot, jól szervezett, célirányos tudományos kutatómunkát igényel. Európában kevés olyan intézmény van, ahol központosított stratégia, egységes elméleti alapvetések, közös tudományos és oktatási stratégia mentén lehet egy tudományos felsőoktatási intézményben gondozni a biztonság megteremtésének tudományát, elméletét, gyakorlati iránymutatását. Ezt a lehetőséget kell kihasználnia az új egyetemnek.

Felhasznált irodalom

[1] KÖSZEGVÁRI Tibor: A hadtudomány mai problémái, területei és új fogalma (Hadtudomány (Magyar Hadtudományi Társaság, Budapest XVII. Évfolyam 2007/1 szám) 13. oldal.

[2] Dr. Hadnagy Imre József: A biztonság korszerű értelmezése, http://www.vedelem.hu/letoltes/tanulmany/tan135.pdf

[3] Finszter Géza: A kriminalisztika elmélete és a praxis a büntetőeljárási reform tükrében, http://be.atw.hu/letoltes/Krimjegyzet.doc

[4] Dr. Balla Lajos: Adalékok a titkos információgyűjtés…, http://www.debreceniitelotabla.hu/doc/bunteto/TitkosAdatgyujtes.pdf

[5] Berek Lajos: A tudományos kutatás alapjai és módszertana, www.bereklajos.hu

[6] Kovács László: Hadmérnök, 2007. november 27. Különszám Kritikus információs infrastruktúrák Magyarországon

[15] Marosi Attila Csaba: Desktop Grid a Web 2.0 szolgálatában, Networkshop 2011. szekció előadás

[7] Varga Péter János Budapesti Műszaki Főiskola: A kritikus információs infrastruktúrák értelmezése Hadmérnök, III. Évfolyam 2. szám - 2008. június http://hadmernok.hu/archivum/2008/2/2008_2_varga.pdf

[8] Bukovics István: A katasztrófavédelem helye, szerepe a XXI. század elején http://www.vedelem.hu/letoltes/tanulmany/tan117.pdf

[9] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, (PhD) értekezés ZMNE

[10] Sik Zoltán Nándor, ENO Advisory Kft: A kritikus információs infrastruktúra védelem kormányzati feladatai az információs hadviselés korában, http://docs.google.com/viewe

[11] Précsényi Zoltán, Solymosi József: Kritikus infrastruktúrák azonosítása, körkép az EU-ban és az USA-ban tapasztalható nehézségekről, http://www.foodlawment.hu/downloads/kritikus_infrastrukturak_azonositasa_usa_eu.pdf

[12] Networkshop 2008-2011 konferenciák előadás anyagai https://nws.niif.hu/nws2011/ http://videotorium.hu/hu/

[13] HBONE+ architektúra, tenderek, eszköztenderek, hálózati eszközök: Jákó András jako.hujako.andras@eik.bme.hu

[14] MPLS alapú IP hálózat képességei: Gaál Géza PKI-FI Műszaki termékfejlesztési ágazat

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Halász László
halasz.laszlo@zmne.hu

Remetei Dóra
dorifly@freestart.hu

A KÖZÖSSÉGI KÖZLEKEDÉS SÉRÜLÉKENYSÉGÉNEK ELEMZÉSE BIOTERRORISTA TÁMADÁS ESETÉN
A KATASZTRÓFAVÉDELEM ÉS AZ EGÉSZSÉGÜGY SZEREPE

Absztrakt

A tömegpusztító fegyverek és hordozóeszközeinek proliferációja lehetővé tette CBRN eszközökkel végrehajtott terrorista támadás végrehajtását, amely többek között a kritikus infrastruktúra elemeit is veszélyeztetheti. Ilyen cselekményre láthattunk már példát az elmúlt évtized, de a közelmúlt eseményei során is. Magyarország nem tartozik a kiemelt kockázatú államok közé, de hazánkban sem lehet kizárni ilyen esemény bekövetkeztét.
A dolgozat elemzi a bioterrorizmus és a kritikus infrastruktúra néhány aspektusát, fel szeretné hívni a figyelmet a közösségi közlekedés sebezhető voltára bioterror támadás esetén, hangsúlyozza a már működő szisztémákat és protokollokat, kiemelten elemzi a katasztrófavédelem és az egészségügy feladatait, rávilágít néhány hiányosságra elsősorban az egészségügy területén.

The proliferation of the AMD's and their launching equipments made possible to make terrorist's attack using CBRN devices. These attacks may endanger the elements of the critical infrastructure as well as the public transport. The samples of such kind of events we see in the last decade as well as among the events of the near past too. Hungary does not belong to the countries having high risk, but the taking place of such an events can not be excluded in our country too.
This paper analyses some aspects of the bio terrorism and the critical infrastructure and calls the attention sensitivity of the public transport in case of a bio-terror attack. The study emphasizes the already existing systems, protocols and analyses the tasks of the disaster protection, public health and point to some of the imperfection especially on the field of the public health.

Kulcsszavak: *terrorizmus, bioterrorizmus, kritikus infrastruktúra, közösségi közlekedés, metró, reagáló erők, egészségügy ~ terrorism, bioterrorism, critical infrastructure, public transport, metro, reaction forces, public health*

BEVEZETÉS

A hidegháború befejezésével, a bipoláris világrend széthullásával, a tömegpusztító fegyverekkel megvívott háború esélye jelentősen csökkent. Ezzel párhuzamosan az 1990-es évektől a globalizáció kiteljesedésével, hazánk NATO tagállammá válásával, az európai integráció elmélyülésével a veszélyeztetettség mértéke és minősége megváltozott. Napjaink egyik fő kihívását a nemzetközi terrorizmus megjelenése jelenti. (Bedros J. R. 2004) Az államok nagy része szervezett, modern erőkkel ellátott hadsereget tart fenn, egyes államok és csoportosulások céljaikat terrorista akciók, bűncselekmények elkövetése útján akarják megvalósítani. Az ilyen támadások mind végrehajtóik, mind céljaik tekintetében előzetesen kevéssé ismertek. Lehetőségeik nem állnak arányban a megtámadott ország fegyveres erőinek, rendőrségének, elhárításának képességeivel, ezért folyamatos akciókkal, a feszültség fenntartásával igyekeznek fellazítani a szilárd társadalmi alapokat, megingatni és elbizonytalanítani a lakosság ellenálló erejét, állandó bizonytalanságban tartani a nemzet-, katasztrófavédelmi és egészségügyi szervezeteket.

A nemzetközi, globális terrorizmus logisztikai, pénzügyi és műveleti képessége századunk elejére jelentősen megnőtt. Fenyegető problémaként jelentkezik a terrorizmusnak és a tömegpusztító fegyverek proliferációjának összekapcsolódása. A terjedési folyamat nem csupán a tömegpusztító fegyverek, hanem a gyártási technológia és a szellemi kapacitás illegális elterjedését is jelenti. (Zsohár I. 2003) A veszteség növeléséhez, pánik és zavarkeltéshez a „hagyományos" módszereken kívül az egyik logikus és lehetséges út a CBRN (kémiai, biológiai, radiológiai, nukleáris) fegyverek és eszközök felhasználása. Ha visszatekintünk a XXI. sz. megvalósult hagyományos, és CBRN terrorcselekményeire, észrevehető a kritikus infrastruktúrához tartozó objektumok kiemelt fenyegetettsége. Ezek egy része az ún puha (kevésbé védett, civil) célpontok közé tartozik, az ellenük elkövetett merényletek a kisebb kockázati tényezők mellett kiemelten felkeltik a média és a közvélemény figyelmét. A közösségi közlekedés különösen vonzó célpont mind szerteágazó zavarkeltő hatása, mind pánikkeltő potenciálja miatt.

Napjainkban szinte mindenki által természetes, hogy szükségletei kielégítésére bármely időpontban rendelkezésre állnak a közösségi közlekedési rendszerek. Nem tervezett kiesésük, pl. katasztrófa vagy terrorcselekmény által, mind az egyénnek, mind a termelésnek és a szolgáltatásnak felbecsülhetetlen károkat okozhat, így az egész társadalom működésére kihatással van. (Tóth A., Tóth G. 2009.)

MAGYARORSZÁG TERRORFENYEGETETTSÉGE

Jelenleg Magyarország terrorfenyegetettségét a biztonságpolitikai elemzések stagnálónak, illetve alacsonynak értékelik. Hazánk NATO és EU tagsága, katonáink külföldi szerepvállalása kockázati tényezőként jelentkezhetnek. Nemzetközi békemissziókban vállalt szerepünk az elmúlt években növekedett, Magyarország több alkalommal engedélyezte légterének hadműveleti célú NATO felhasználását, illetve területeinek logisztikai támogatás célzatú igénybevételét. Ezek kiváltó okai lehetnek terrorcselekmények Magyarországon történő elkövetésének. (Tarján I. 2004.)

A biztonsági kockázatot jelentő tényezők vizsgálatakor figyelembe kell venni az euroatlanti térségen (így Magyarországon is) túlmutató új típusú kihívásokat, amelyek a katonai és a civil szférát egyaránt érintik. Az EU egyik határországaként hazánk a korábbi évekhez képest jelentősebb mértékben kitett a közel- és közép-keleti, valamint az egyéb válságövezetekből induló illegális migrációs folyamatoknak. Az ezt a jelenséget kihasználó, illetve a nemzetközi szervezett bűnözéssel kapcsolatban álló terrorista szervezetek és az őket támogató országok elleni hatékony küzdelemhez az euroatlanti térség államainak a feladatok

megosztásán, a képességek fejlesztésén és alkalmazásán alapuló összehangolt együttműködése szükséges. A nemzetközi-, így véleményem szerint Magyarország biztonsága szempontjából is az egyik jelentős kockázatot a radiológiai, továbbá a viszonylag könnyen és kis költséggel előállítható vegyi-, és biológiai fegyverek, valamint előállításukhoz és célba juttatásukhoz szükséges hordozó eszközök és technológiák proliferációja jelenti. Nem lehet biztonsággal kizárni, hogy ezek a tömegpusztító eszközök a nemzetközi békét és biztonságot veszélyeztető rezsimek, vagy terrorista csoportok kezébe kerülhetnek. (Pellérdi R. 2007)

2011-ben Magyarország lesz az EU soros elnöke. Az ekkor hazánkban tartózkodó kiemelt kockázatú személyek jelenléte, jelentős nemzetközi rendezvények lebonyolítása és a mindezek miatt megnövekedő média figyelem növelheti a terrorfenyegetettséget. Az esemény befolyásolhatja a hazánkban tartózkodó külföldi politikusok, közéleti személyiségek és a nagy létszámú vagy kiemelt rendezvények biztonságát, de a puha célpontok fenyegetettségének szintjét is. Fenti felsorolás mindegyikének van közösségi közlekedést érintő aspektusa, kockázatának csökkentése érdekében, hasonlóan a kritikus infrastruktúra többi szektorához a magasabb fenyegetettségi szintnek megfelelő protokollokat lehetne életbe léptetni.

A BIOTERRORIZMUS NÉHÁNY AKTUÁLIS KÉRDÉSE

Az Egészségügyi Világszervezet (WHO) adatai szerint a terroristák által harci eszközként bevethető mesterségesen kifejlesztett vírusok és baktériumok jelenleg a legolcsóbb tömegpusztító fegyverek, amelyek alkalmazásuk esetén tömeges megbetegedéseket, vagy járványokat okozhatnak. Különböző terrorista csoportok érdeklődése fokozódik biológiai, vegyi és radiológiai fegyverek megszerzése és alkalmazása iránt, fegyvertáruk tartalmazza a hagyományos fegyverek árának töredékéből, lényegesen kisebb technológiai háttérrel és szaktudással előállítható tömegpusztító fegyvereket. (Csehi G. 2009) Jelenleg mintegy 11-15 ország és több terrorszervezet rendelkezik biológiai fegyver előállítására alkalmas készletekkel, illetve szellemi tőkével. Mind a NATO, mind az EU szorgalmazza a tagországok CBRN fenyegetettségekre való válaszadási képességeinek kifejlesztését.

A következőkben néhány kiragadott példával szeretném bemutatni az általam legjelentősebbnek tartott eseményeket a teljesség igénye nélkül.

A biológiai terrorizmusról 1999-ben jelent meg egy mélyreható, nyílt forrásokra támaszkodó összefoglaló elemző jelentés, a Monterey Intézet (California, USA) kutatóitól. Az intézet a XX. Század szinte valamennyi terrorista cselekményét nyilvántartásba vette. A 151 biztosan igazolt akcióból 33 biológiai eszközzel végrehajtott támadás volt. (Pellérdi R. 2007) A biológiai fegyverek által jelentett fenyegetés értékelésekor példaként szolgál egy, a rendszerváltás óta nyilvánosságra került eseménysorozat. A hidegháború időszakában, Oroszországban alakult meg a Biopreparat nevű intézmény. Hivatalosan békés célú oltóanyag és gyógyszergyártással foglalkoztak, valójában például a lépfene, takonykór, pestis, himlő és Ebola kórokozóinak tömegtermelésével és fegyverbe illesztésével kísérleteztek. 1979-ben Szverdlovszkban egy eltömődött szűrőről történt feljegyzés a munkanaplóba nem került be, a gépeket elindították, és kevesebb, mint 1g anthrax (lépfene) spóra a levegőbe került. A kiülepedési zónában 68 helyi lakos halt meg tüdőanthraxban. (Ken A. 2000)

A hidegháború után a Biopreparatban alkalmazott mintegy harmincezer szakember és az addig előállított biológiai harcanyagok egy részének sorsa ismeretlen, amelyben egyik legjelentősebb példáját látom a szellemi kapacitás és a biológiai fegyver proliferációjának

Az Amerikai Egyesült Államokban 2001. szeptember 18-án öt, október 9-én pedig két lépfene-baktériummal fertőzött levelet postáztak New Yorki és Washingtoni címzetteknek. A levelek tartalma a biológiai fegyverekben használttal csaknem azonos minőségű szárított anthrax port tartalmazott, amelyek egymástól molekuláris tipizálási módszerekkel is megkülönböztethetetlennek bizonyultak. A levelekkel kapcsolatba került személyek közül

öten meghaltak és tizenheten megbetegedtek. Az amerikai kormánynak a válságkezelés közel másfél millió dolláros többlet kiadást okozott, pedig a terroristák mindössze 20 g baktérium spórát alkalmaztak. A szándékos anthrax expozíció által igazolt esetek új közegészségügyi veszély kialakulását jelezték. (Melles M. 2001)

Véleményem szerint ez az eseménysorozat minden kétséget kizáróan felhatalmazza az illetékeseket, hogy a bioterrorizmust, mint valós fenyegetést aposztrofálják. Valószínűleg az amerikai események hatására 2008-ban Magyarországon emelkedő számú „antrax gyanús fehér port" tartalmazó levél küldésével végrehajtott riasztási esemény vált ismertté. A tendencia 2009-ben is megmaradt. Ez az eseménysorozat az egyik kiváltó oka, hogy 2009 óta a BTK büntetni rendeli a terrorcselekménnyel való fenyegetést akkor is, ha az életellenes cselekmény nem valósul meg. Tapasztalatok szerint a fenyegetések számával egyenes arányban nő egy ténylegesen bekövetkező, valós bioterrorista akció bekövetkezésének valószínűsége. (Falus F. szóbeli közlése 2009)

Az Egyesült Államokban és Oroszországban feltehetően még megmaradtak azok az automatikus tenyésztő rendszerek és berendezések, amelyek lehetővé tették biológiai kórokozók előállítását. Az államok biológiai fegyvereik 80-85 %-át megsemmisítették, bizonyos mennyiséget azonban visszatartottak védelmi kutatások céljaira. Ezeket liofilizált állapotban alacsony hőmérsékletre hűtve tárolják. (Török T. 1995) Illetéktelen kezekbe kerülve duális felhasználásuk során a fagyasztva szárított kórokozókból a biofegyver gyártás napok alatt újra indítható.

Élettani szempontból a fertőzés legkönnyebben a légzőszerveken keresztül jut be a szervezetbe, ezért a biológiai fegyverekben alkalmazott ágensek legtöbbje 5-10 mikron méretű cseppek, vagy por formájában a levegővel kerül a tüdőbe. A harcanyag levegőben történő szétszórása történhet robbanószerkezettel, spray rendszerű eszközzel, vagy aerosolos berendezéssel. (Sergio B. 2007). A robbanószerkezet (hagyományos töltet köré töltött biológiai ágens, a radiológiai piszkos bomba analógiájára) detonációjakor általában a hatóanyag egy része ugyan megsemmisül, de a fertőzőképesen maradt mennyiség a levegőbe kerülve elszennyezi az élő és élettelen környezetet. A spray rendszerű lőszer a biológiai ágens mikroszkopikus részecskéit láthatatlan felhőként szórja szét, aerosol eszközöknél generátor végzi az ágensek levegőbe porlasztását. Utóbbi két módszer képes szabályozni a részecske méretét, és mivel detonáció nem szükséges, a hatóanyag becslések szerint 40-60 százaléka túléli a kijuttatást (Dobos G. 2007) Eddigi tanulmányaim szerint lépfene spóra alkalmazásakor a spóra több kísérletben is igazoltan extrém ellenálló képessége miatt ennél jobb túlélési mutató is becsülhető.

A fejezet végén összefoglalom a biológiai fegyver néhány, diverziós célokra is felhasználható tulajdonságát:

- Detektálása nehéz és körülményes;
- Csak élőerőre veszélyes, az építményeket és berendezéseket nem semmisíti meg, így megfelelő mentesítő intézkedések után a csapást szenvedett körzetet azonnal meg lehet szállni; (Pellérdi R. 2007)
- Jellemző lappangási idő után hat, lehetőséget adva az elmenekülésre;
- Másodlagos járványokat okozhat, akár földrésznyi területen széthurcolva a kórokozót;
- Rendkívül sokszínű tünet észlelhető a lehetséges ágensek nagy száma miatt, így a kórkép nehezen diagnosztizálható, amely komoly pánikkeltő potenciállal bír a lakosság körében;
- A megelőzés, védekezés, gyógyítás lehetőségei korlátozottak; (Faludi G. 1998)

- Gyártása egyszerű, rejtetten, akár házi laboratóriumban is megvalósítható, ezáltal megkönnyíti a terroristák hozzáférhetőségét; (Juhász L., Huszár A. 2009)

1. ábra. Lefoglalt házi labor. Forrás: Juhász L., Huszár A. (2009)

- Alkalmazásának fajlagos költsége 1 $/km2, szemben a kémiai 660 $/km2, a nukleáris 800 $/km2, a konvencionális fegyver 2000 $/km2 becsült értékével, mindezekkel szemben a hatékony védelem bonyolult és költséges. Sok publikációban ezért nevezik a biológiai fegyvert a „szegény ember atombombájának"(Bedros J. R. 2004)

A KRITIKUS INFRASTRUKTÚRA

A modern társadalmak nagymértékben függnek az infrastrukturális rendszerek működésétől, amelyek zavarai, ideiglenes kiesése vagy esetleges megsemmisülése kihatással vannak a gazdaság és a kormányzat hatékony működésére és a mindennapi életre egyaránt.

A kritikus infrastruktúra az infrastrukturális hálózaton belül kiemelt jelentőségű. Definíció szerint olyan elemek, létesítmények, szolgáltatások és folyamatok tartoznak e fogalomkörbe, amely az ország, (lakosság, gazdaság, és kormányzat) működése szempontjából létfontosságúak, és érdemi szerepük van egy társadalmilag elvárt minimális szintű jog-, és közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügy és környezeti állapot fenntartásában. Az állami és gazdasági szereplők valamint a lakosság részéről egyaránt elvárás, hogy a kritikus infrastruktúrák a lehető legnagyobb biztonsággal működjenek. Elsődleges jelentőségű, hogy ezen elemek üzemelésének terrorcselekmény, katasztrófa, vagy baleset általi megzavarása megelőzhető, kivédhető, időtartamában rövid és kezelhető legyen. Ellenkező esetben súlyos hatást gyakorolhat az állampolgárok szociális-, és gazdasági jólétére, a nemzetgazdaság és a kormány működésére. (2080/2008. (VI. 30.) Kormány Határozat a Kritikus Infrastruktúra Védelem nemzeti Programjáról)

A Nemzeti Kritikus Infrastruktúra Védelem (NKIV) célja egy széleskörű együttműködésen alapuló rendszer létrehozása, amely a folyamatos működés biztosítását, ennek megszakadása vagy kiesése esetén a helyreállítására vonatkozó képességek meglétét és folyamatos fejlesztését teszi lehetővé. Mindezek többek között a sebezhetőség és a kockázati tényezők tudatos felmérésével, beazonosításával valósulnak meg.[1] A nemzetközi és magyar KIV programok feladataik végrehajtásakor az összveszély megközelítés mellett a terrorizmus fenyegetését, mint elsődleges prioritást határozták meg. A KIV hatékony biztosítása a katasztrófavédelemmel összhangban, amelynek elsődleges feladata a hagyományos funkciói mellett a kritikus infrastruktúrák védelme és a terrorizmus elleni fellépés (Bukovics I. 2004) a nemzetbiztonsági szolgálatok, rendvédelmi szervek és a megelőző-, gyógyító egészségügy összehangolt, hatékony fellépését is igényli.

[1] Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról

A KÖZÖSSÉGI KÖZLEKEDÉS

A NKIV II. szektorának a közösségi közlekedést határozta meg.

Ha visszatekintünk a közelmúlt legsúlyosabb terrorcselekményeire, megállapíthatjuk, hogy a kritikus infrastruktúra érintettségén belül is több esetben a közösségi közlekedés, kiemelten a metró ellen irányultak.

1995. március 20-án Tokióban a Legfelsőbb Igazság szekta egy vegyi fegyverrel, Sarinnal hajtotta végre a 12 halottat, és ötezer gázmérgezettet, követelő metrótámadást. A terrorakció során 15 metróállomás vált vegyileg szennyezetté. (Rabiné A. 2006.) 2010. május 07-én Tokióban Aszahara Sokót, a szekta alapítóját kötél általi halálra ítélték. A szekta guruját összesen 13 bűntettben találták bűnösnek, amelynek 27 halálos áldozata és több ezer sebesültje volt.

2004. március 11-én Madridban és elővárosaiban tíz, hátizsákba rejtett pokolgépet robbantottak négy különböző helyszínen, a városközpontba tartó vasútvonalakon és a madridi pályaudvarokon. A merényletsorozatban 199-en vesztették életüket, csaknem 1500-an megsérültek. A terrorcselekmény is kihatással volt a regnáló kormány márciusi választási vereségére, az új kormányfő kivonta a spanyol csapatokat Irakból, amely rendkívül komoly bizonyítéka a terrorizmus nemzetközi politikára gyakorolt hatásának, és eredményességének.

2005. július 7-én Londonban, Pakisztánban kiképzett terroristák három metrószerelvényt és egy buszt robbantottak fel. A támadás 51 áldozatot követelt, London élete egy napra megbénult.

2010. március 29-én két öngyilkos merénylő robbantott a reggeli csúcsforgalomban a Moszkvai Ljubjanka téri metró állomáson. Az állomás felett található az Orosz Szövetségi Biztonsági szolgálat épülete. Negyven perccel később négy megállóval délebbre újabb robbantás történt, a két merényletnek összesen 43 halottja és közel 100 sérültje volt. Moszkvában gyakorlatilag leállt a közlekedés, akadozott a mobil telefon szolgáltatás.

E teljesség igénye nélkül történt felsorolásból is látható, hogy a metró több esetben is a terroristák kedvelt célpontja, és ebben az esetben már megvalósult tömegpusztító fegyver alkalmazása is.

A METRÓ VESZÉLYEZTETETTSÉGÉNEK NÉHÁNY SZEMPONTJA

A terrorszervezetek számára a metró járművei és létesítményei könnyen megismerhetőek, a szükséges adatok többsége megtalálható a világhálón. A nyilvános és tömeges igénybevétel miatt megközelítésük, célobjektumba jutásuk nem okoz nehézséget. Az adott város forgalmi helyzetét, közlekedési szokásait nagy vonalakban ismerve is viszonylag pontosan tervezhető és megbecsülhető az okozott személyi sérülés mértéke, a város közlekedésére gyakorolt globális hatása és a keletkező pánik nagysága is. A kötöttpályás közlekedési rendszerek üzemeltetésükkel összefüggően több egyidejű feltétel megléte esetén működőképesek, ezért megzavarásukra is több lehetőség kínálkozik. Mivel térben való elhelyezésük állandó, szinte valamennyi elemük részletesen és kellő pontossággal felderíthető. (Tóth A., Tóth G. 2009.)

Budapest közlekedésében a metró kulcsszerepet játszik, szerelvényeik 26-30 ezer utast képesek óránként és irányonként szállítani, 800-1000 ember egyidejű helyváltoztatására is alkalmasak. Napi utazóközönségük másfél millió emberre becsülhető. Többségében földalatti elhelyezkedése következtében a kimenekítés az áteresztőképesség fizikai korlátai miatt lassabban kivitelezhető, mint felszíni közlekedési rendszer esetében. Ez pánikkeltő potenciálját is növeli. Kiemelten fontos az alagutak és állomások levegő ellátása, amely a vonatok előtti túlnyomás és a mögöttük keletkező vákuum kiegyenlítése érdekében és a légcsere biztosítása miatt rendszeres távolságokban szellőző aknák építésével lehetséges,

ezeknek végpontjai a külvilágra nyílnak, a szellőző levegő egy felszíni, vagy felszín alatti nagyméretű műtárgyon áthaladva jut a szabadba. (Bata I. 2010) Légszállítási egységteljesítményük 1000-1600 köbm/h. (Greschik Gy. 2010) Ezen létesítmények az egyik legkritikusabb és legveszélyeztetettebb pontjai a földalatti közlekedésnek, mivel a szellőztető rendszeren keresztül az egész alagútrendszer ás az állomások levegője rövid időn belül szennyezhető, illetve mérgezhető.

Az infrastruktúrák egészének veszélyeztetettségét rendszerint csak általánosságban lehet megállapítani. Konkrét védelmi intézkedések megtételéhez elengedhetetlen az egyes objektumok - az adott objektum jellegére, feladatára és területére vonatkoztatott - valós fenyegettségének meghatározása. (Tóth A., Tóth G. 2009.)

Az eddig felsorolt szempontok miatt választottam hatástanulmányként egy metróállomás bioterror támadás szimulációját, amelyet lépfene spóra alkalmazásával hajtanak végre.

HATÁSTANULMÁNY

A következőkben megvizsgáljuk egy feltételezett biológiai terrortámadás hatásait.

Feltételezés szerint egy metró állomáson egy házilag készített anhtrax spórát tartalmazó bombát robbantanak. A CIA véleménye szerint hatásosnak látszik az anthrax spórák robbanó töltetekben való felhasználása, mivel irodalmi adatok szerint a robbanás után sem pusztulnak el és a fertőzött szilánkok súlyos lépfene fertőzést okoznak .A bomba 1 kg szemtex robbanóanyagot és 1 kg anthrax spórát tartalmaz. Ha egyszerű hengeres bombatestet feltételezünk, amelyben egy belső henger tartalmazza a robbanóanyagot és gyújtószerkezetet és a külső henger az anthraxot, akkor a sűrűségeket figyelembe véve egy 20 cm magas 8 cm külső és 4 cm belső sugarú hengert kapunk. A feltételezett metró állomás kb. 200 m^3 össz térfogatú (kb. 30-40 m hosszú és 5-6 m széles). A metró alagút átmérője 5 m. Az állomáshoz csatlakozó mozgólépcső rendszer 10-40 m hosszú és kb. 8 m átmérőjű.

A robbanást követő primer felhő mérete az alábbi összegfüggésből határozható meg (Halász L. Grósz Z. 2000)

$$R_0 = 6{,}37\sqrt[3]{G} + \frac{0{,}081}{\beta}\sqrt[3]{G} \qquad (1)$$

$$H_0 = 3{,}9\sqrt[3]{G} + \frac{0{,}029}{\beta}\sqrt[3]{G} \qquad (2)$$

Ahol G a robbanóanyag tömege (kg), β a robbanóanyag és az anhtrax tömegének aránya.. A feltételezett adatokkal a primer felhő sugara 6,46 m és magassága 4,2 m. Ebből következik hogy a robbanás után kialakult koncentráció1,81 g/m^3.

A következőkben meg kell vizsgálnunk, hogy mi az a koncentráció, amely még megbetegedést okoz. Kiindulópontként feltételezzük, hogy 10000 spóra az a mennyiség, amely még megbetegedést kiválthat. A spóra méretét 3 μm-nek vesszük (Medical Planning Guider 2000) Ezekkel az adatokkal egy spóra tömege $2*10^{-11}$ g, ami azt jelenti, hogy $2*10^{-7}$ g/m^3 koncentráció még fertőzőképes. A spórák kis mérete miatt az ülepedéssel nem kell számolni, mivel a spórák mérettartományában (1-5 μm) a maximális ülepedési sebesség 0, 05 m/s. A terjedést a következő egyszerű összefüggéssel írjuk le (Halász L. Grósz Z. 2000)

$$c(x,y,z) = \frac{c_0}{4\pi kx}\exp\left[-\frac{u}{kx}\left(y^2+{}^2\right)\right] \qquad (3)$$

Ahol c a koncentráció egy adott pontban, c_0 a primer felhő koncentrációja, k a légköri stabilitástól függő turbulens diffúziós állandó, u a szélsebesség, x, y, z a térkoordináták, x a metró alagút tengelye irányába mutató koordináta. A számításokhoz 0,5, 1,5, 1,5 és 5 m/s szélsebességeket vettünk figyelembe, a k érték a metró alagútra 4. Az 1. táblázat mutatja a

számítások eredményét 0,45 m/s szélsebességre, a 2. táblázat tartalmazza az adatokat, 1,5, 2,5 és 5 m szélsebességekre y = z = 1 m értékekre.

Távolság a primer felhőtől (m)	Koncentráció (g/m^3) y = z =1 m	Koncentráció (g/m^3) y = z = 2,5 m	Koncentráció (g/m^3) Y = z = 5 m
1	$5,95\ 10^{-2}$	$1,60\ 10^{-2}$	$7,62\ 10^{-3}$
5	$1,45\ 10^{-2}$	$1,11\ 10^{-2}$	$4,38\ 10^{-3}$
10	$7,45\ 10^{-3}$	$6,53\ 10^{-3}$	$4,09\ 10^{-3}$
20	$3,77\ 10^{-3}$	$3,53\ 10^{-3}$	$2,79\ 10^{-3}$
30	$2,53\ 10^{-3}$	$2,42\ 10^{-3}$	$2,07\ 10^{-3}$
50	$1,53\ 10^{-3}$	$1,48\ 10^{-3}$	$1,35\ 10^{-3}$
100	$7,62\ 10^{-4}$	$7,52\ 10^{-4}$	$7,18\ 10^{-4}$
500	$1,53\ 10^{-4}$	$1,52\ 10^{-4}$	$1,51\ 10^{-4}$
1000	$7,64\ 10^{-5}$	$7,63\ 10^{-5}$	$7,62\ 10^{-5}$
3000	$2,55\ 10^{-5}$	$2,55\ 10^{-5}$	$2,55\ 10^{-5}$
5000	$1,53\ 10^{-5}$	$1,53\ 10^{-5}$	$1,53\ 10^{-5}$
10000	$7,64\ 10^{-6}$	$7,64\ 10^{-6}$	$7,64\ 10^{-6}$

1. táblázat. Az antrax koncentráció 0,5 m/s szélsebességre, különböző távolságokban a robbanás helyétől

Távolság a primer felhőtől (m)	Koncentráció (g/m^3) Szélsebesség 1,5 m/s	Koncentráció (g/m^3) Szélsebesség 2,5 m/s	Koncentráció (g/m^3) Szélsebesség 5 m/s
1	$1,20\ 10^{-2}$	$4,38\ 10^{-3}$	$1,27\ 10^{-4}$
5	$4,39\ 10^{-3}$	$2,38\ 10^{-3}$	$9,25\ 10^{-4}$
10	$2,36\ 10^{-3}$	$1,35\ 10^{-3}$	$5,95\ 10^{-4}$
20	$1,23\ 10^{-3}$	$7,18\ 10^{-4}$	$3,37\ 10^{-4}$
30	$8,28\ 10^{-4}$	$4,89\ 10^{-4}$	$2,34\ 10^{-4}$
50	$5,02\ 10^{-4}$	$2,9810^{-4}$	$1,45\ 10^{-4}$
100	$2,53\ 10^{-4}$	$1,51\ 10^{-4}$	$7,45\ 10^{-5}$
500	$5,09\ 10^{-5}$	$3,05\ 10^{-5}$	$1,52\ 10^{-5}$
1000	$2,55\ 10^{-5}$	$1,53\ 10^{-5}$	$7,62\ 10^{-6}$
3000	$8,49\ 10^{-6}$	$5,08\ 10^{-6}$	$2,55\ 10^{-6}$
5000	$5,08\ 10^{-6}$	$3,06\ 10^{-6}$	$1,53\ 10^{-6}$
10000	$2,55\ 10^{-6}$	$1,53\ 10^{-6}$	$7,64\ 10^{-7}$

2. táblázat. Az antrax koncentráció a távolság függvényében a robbanás helyétől, különböző szélsebességek esetén

A két táblázat adatai azt mutatják, hogy ilyen mennyiségű antrax jelentős szennyezést okoz egy kb. 10 km hosszú metró szakaszon. Ez kb. a 2. metró kétharmad hosszának felel meg. Természetesen figyelembe kell venni a mozgó lépcsők és a szellőző rendszer hatását is. Az előbbi hatása becsülhető, ha feltételezzük, hogy a robbanás során kialakuló felhő bizonyos része a mozgólépcső irányában terjed. Így például feltételezve, hogy a felhő fele a mozgó lépcső felé terjed, úgy a fenti táblázatokban megadott koncentrációk felével kell számolni. Az így kapott koncentráció értékek még mindig nagyobbak a fertőzési koncentrációnál. Ez azt is jelenti, hogy a mozgólépcső és a szellőzők környezete is szennyeződik.

A VÉDEKEZÉS EGYES SZEMPONTJAI

A biológiai terrorizmus elleni felkészülés megköveteli az egyes ágazatok és országos hatáskörű szervezetek összehangolt, szervezett felkészítését és fellépését. Ezen a területen a legfontosabb feladatok a titkosszolgálatok, a rendvédelmi szervek, a katasztrófavédelem és a megelőző-, és gyógyító egészségügy összehangolt, kellő információcserén és pontos koordináción alapuló munkája. A fejezet során megkísérlem nagy vonalakban vázolni az érintett szolgálatok feladatait, kiemelt fontossággal kezelem a katasztrófavédelem és az egészségügy szerepét.

A titkosszolgálatok gyűjtik, értékelik és elemzik a terrorizmushoz köthető külső és belső kockázatokat, fenyegetéseket. Ezen a szinten - ha egy terrorcselekmény elkövetésének szándéka látótérbe kerül, - még nyílik lehetőség az elhárításra. Ezért fontosnak tartom az illetékes szakterületek megerősítését a legeredményesebb megelőző tevékenység érdekében, hiszen ezekben az esetekben a támadás nem valósul meg.[2]A támadás következményeinek felszámolása során a rendőrség feladata a helyszínen a bioterror cselekmény kriminális jeleinek értékelése, a terület lezárása és a nyombiztosítás. Bár a helyszínen van lehetőség a fertőző ágens identifikációját (azonosítását) segítő gyorstesztet végezni, a zárlat csak az OEK laboratóriumában végzett 48 órás tenyésztéses vizsgálat negatív eredménye esetén oldható fel.

Katasztrófavédelmi és egészségügyi szempontból egy terrorcselekmény megvalósulása esetén szükségessé váló intézkedések alapvetően nem különböznek a katasztrófa és Rota események (nem katonai csapásból származó ABV vészhelyzet) során szükséges lépésektől. (Rabiné A. 2006) A katasztrófavédelem feladata általánosságban terrorcselekmények elhárításának protokollok szerinti tervezése, az érintett szervek és a lakosság felkészítése a váratlan helyzetekre. Ezen kívül ügyeleti szolgálatokat és azonnal bevethető készenléti egységeket szerveznek és tartanak fenn, ellátják technikai eszközökkel. Részt vesznek a kritikus infrastrukturális elemek fizikai védelmében, minősített időszakokban ezeket igény szerint megerősítik. (Varga I. 2006)

Konkrét terrorcselekmény bekövetkeztekor feladatuk az ionizáló és toxikus anyagok jelenlétének gyors felderítése és kizárása (vegyi-sugár felderítés), a biológiai szennyezésre pl. lépfenére gyanús minták megfelelő csomagolása, valamint a helyszín és a személyek mentesítése. (Falus F. 2009) A munkálatokhoz személyes közlésük alapján 100 fő/óra kapacitású mentesítő sátor telepítésével, a szennyezett járművek dekontaminálásával tudnak segítséget nyújtani. (2009-es adat) A megfelelően csomagolt mintát (háromrétegű, légmentesen zárt plasztik zacskó) a katasztrófavédelem szállítja az illetékes ANTSZ-nek, és jegyzőkönyvvel dokumentáltan adja át. A helyszínen a beavatkozó erők feladatot csak egyéni védőfelszerelésben végezhetnek, amelyekkel jelenleg az Országos Katasztrófavédelmi Főigazgatóság Vészhelyzeti Felderítő Csoportja, az MH szakalegységei és az OEK Járványügyi Felderítő Csoportja rendelkezik, a rendőrség és az ÁNTSZ kivonuló munkatársai nem. (2009-es adat)

Az egészségügy szempontjából a védekezés és következmény felszámolás alapja a megfelelő informáltság. A 10/2005. (IV. 12.) EÜM rendelet minden egészségügyi szolgáltató számára előírja az ÁNTSZ területileg illetékes szervének szóban haladéktalan, írásban 2 órán belüli értesítését. A helyi jelentés az Országos Tisztifőorvosi Hivatalhoz, onnan az Egészségügyi Minisztériumhoz jut tovább. (A tanulmány megjelenésekor már Humán Erőforrás Minisztérium) Ha az esemény súlyossága indokolja, a Minisztérium jelenti azt a 2008-ban létrehozott Kormányügyeletnek.

Az információáramlás érdekében az EU a 9/11 és az anthrax levéltámadások hatására létrehozta a RAS-BICHAT (Rapid Alert System –Biological Chemical Agent Attacks)

[2] Honvédelmi Minisztérium Védelmi Hivatal belső kiadványa 2009

rendszerét, amelyen keresztül a tagországok minősített adatok átvételére kijelölt képviselői és egészségügyi kontaktpontjai időben megkapják a szükséges információkat a konkrét biológiai ágenssel kapcsolatban. (Csehi G. 2009) A kataszrófavédelem által az ANTSZ-hez jutott minták BSL (Biology Safety Level) 3-4-es fokozatú laboratóriumban kerülnek elemzésre és verifikálásra, az ő kompetenciájuk a zárlat feloldása, pozitív estben a mentesítés protokoll szerinti elrendelése és a szükséges preventív gyógyszerelés.

A Mobil Biológiai Labor Komplexum a biológiai mintavevő, valamint diagnosztikai képességével részt vehet az adatgyűjtésben és értékelésben. (Honvédelmi Minisztérium Védelmi Hivatal 2009)

A reagálás során a következő lépés az esetleges fertőtzöttek ellátása.

Magyarországon, az oktatás terén szoros kapcsolat van a katasztrófavédelem és az egészségügy között, a szükséges megelőző és gyógyító protokollokat a Honvéd-, Katasztrófaorvosan, Oxyológia szakvizsga keretében öt éves kurzuson képezik a már diplomás orvosokat a SOTE Katasztrófa tanszékén. A Zrínyi Miklós Nemzetvédelmi Egyetem Védelem-egészségügy tanszékén is folyik hasonló jellegű oktatás. A katasztrófa egészségügy a működő egészségügyi ellátó rendszerre és a rendelkezésre álló tartalékokra épül.

Az MH Mobil Orvoscsoport részt vesz a sérültek, fertőzöttek helyszíni ellátásában, szükség esetén a kárhely közelébe Mobil Katasztrófa Segélyhelyet telepítenek.

További kapacitáshiány esetén elrendelhető Mobil Katasztrófa Kórház telepítése.

A kórházak katasztrófaterveik szerint a váratlanul, tömegesen érkező sérültek és fertőzöttek ellátása érdekében:

- a sürgős esetekre korlátozzák a betegfelvételt,
- néhány órán belül ágyfelszabadítást hajtanak végre a nem sürgős esetek soron kívüli hazabocsátásával, illetve osztályok átprofilírozásával.

A kiemelten veszélyes kórokozók által fertőzött betegek ellátására jelenleg a Szent László Kórház rendelkezik egy izolációs kórteremmel. Ezt a kapacitást a későbbiekben feltétlenül bővíteni kell. Amennyiben katasztrófahelyzet elrendelése válik szükségessé, azt egy megyére az Országos Tiszti Főorvos, az ország egész területére az Egészségügyi Miniszter hirdetheti ki.

Katasztrófahelyzetben a rendelkezésre álló tartalékok bázisát az Állami Egészségügyi Tartalék képezi, amelyet az Egészségügyi Készletgazdálkodási Intézet tárol az ország különböző raktáraiban. Innen történik fogyóanyagok, gyógyszerek, eszközök biztosítása a kórházak részére. Az Országos Vérellátó Szolgálat, és az Egészségügyi Készletgazdálkodási Intézet a nap 24 órájában elérhető. Az egészségügyi dolgozók a 158/1999. (XI. 19.) Kormányrendelet szerint átvezényelhetők profil, és név szerint is a katasztrófa sújtotta területre. (Honvédorvostan, Katasztrófaorvostan tanfolyam anyaga 2008)

A fent ismertetett intézkedés sorozat természetesen meghaladja a hatástanulmányban felvázolt bioterror támadás egészségügyi és kataszrófavédelmi igényét, a protokoll egy több régiót érintő katasztrófahelyzet, Rota esemény vagy terrortámadás esetén lépne működésbe.

Jelen esetben, ha a biológiai támadás ténye ismert, az eljárásrend szükségszerinti elemei aktivizálódnak. Amennyiben a terrorcselekmény során biológiai ágens bevetésére nem derül fény, az ÁNTSZ csak néhány nap múlva szerezne tudomást a fekvőbeteg ellátás fertőző beteg jelentési kötelezettségén keresztül. Ilyenkor visszamenőleg kell elrendelni a lehetséges fertőzöttek keresését, preventív gyógyszerelését, amely igazolt anthrax expositio esetén minimum 60 nap időtartamú, a spórák vegetatív alakba kerülésének jelen tudásunk szerint időtartamához igazodva. Ilyen esetekben kötelező fekvőbeteg osztályon való elhelyezés, mivel a kialakult tüdőanthrax csaknem minden esetben letális. (Szalka A., Tímár L., Ludvig E., Mészner Zs. 2005) A terület azonosítása, lezárása, mentesítése, amely a szennyeződés széthurcolásának, a fertőzöttek számának esetlegesen exponenciális növekedésének

megakadályozása miatt elkerülhetetlen, jelentős humán és gazdasági erőforrás lekötést igényelne, amelyet tovább súlyosbítana a valószínűleg kialakuló pánikhelyzet.

Ilyen esetekre a reagáló erők nemzetközi szinten is fejlesztik protokolljaikat, reményeim szerint dolgozatom is bizonyítja az eljárásrendek folyamatos aktualizálásának, fejlesztésének, illetve a részt vevő szolgálatok közötti folyamatos koordinációjának szükségességét.

KÖVETKEZTETÉSEK

Hatástanulmányunkban bemutattunk egy feltételezett, de részeiben már előfordult bioterror akciót, amelyben bizonyítás nyert, hogy a metró területének kb. 10 km-es szakasza válna fertőzötté, a biológiai ágens a külvilágba is kijutna a mozgólépcső és a szellőző rendszer közvetítésével.

Az eredmények, és a dolgozat általános elemző fejezeteinek ismeretében, a de biztonságpolitikai elemzők következtetéseit, és az eddig látótérbe került, vagy megvalósult bioterrorista támadások következtetéseit is figyelembe véve összegezhetjük, hogy a bio-, (és tágabb értelemben a CBRN) fegyverek illetéktelen kezekbe kerülésének és terrorista célokra való felhasználásának ténye új, globális kihívást jelent, érinti az EU és a NATO szövetséges tagállamait, így Magyarországot is. A biológiai ágensekkel, fegyverekkel végrehajtott terrortámadások készülődéseinek leleplezésére, a fenyegetések felderítésére és bekövetkezés esetén a károk lehető legnagyobb mérvű enyhítése céljából sürgető feladat a védekezési stratégiák alapelveinek és módszereinek meghatározása. A hatékony reagálás a nemzetbiztonsági, rendvédelmi, jogalkalmazói hatósági, katasztrófavédelmi és az ÁNTSZ közegészségügyi - járványügyi hatósági szakterületek összehangolt munkáját igényli, összekötve a jog, hadtudomány és a gyógyító valamint megelőző orvostudomány ágait. (Faludi G. 2001)

Az elsődleges célok egyikeként kitűzhetjük a katasztrófavédelmi szervek és az egészségügyi intézmények tevékenységének további összehangolását, mivel ez a kapcsolat már jelentős, működő alapokra épül. A védelmi képesség növelése érdekében bővíteni kell a katasztrófavédelmi szakemberek, gyógyító és megelőző területen dolgozó orvosok (toxikológusok, katasztrófaorvosok) számát, mert ezeken a szakterületeken jelenleg szakember hiány tapasztalható. Az eddigieknél nagyobb súlyt kell helyezni az alap, illetve az elméleti és gyakorlati továbbképzésére. Folytatni kell a szükséges válságtervek kidolgozását, meg kell szervezni nagy létszámú fertőzött beteg befogadására és ellátására alkalmas egészségügyi központokat. (Tatár A. 2005)

Az ÁNTSZ átszervezésekor analitikai kapacitásának egy részét elvesztette, ezért CBRN események diagnosztikai feladatainak elvégzése kevésbé hatékony, nem egy kézben összpontosul. A probléma megoldása kívánatos lenne az ÁNTSZ a reagálásban betöltött központi szerepe miatt.

Az új kihívások szükségessé teszik a gyógyszernormák felülvizsgálatát is az Állami Egészségügyi Tartalék keretein belül, mert elsődleges védekezési iránnyá a katasztrófákra, a terrorizmusra és a járványokra való felkészülés vált. (Falus F. 2009) Ennek az igények a gyógyszernormák változásában is tükröződnie kellene.

Mindezek ütemezésekor figyelembe kellene venni Magyarország soros elnökségi pozícióját 2011. első felében.

Felhasznált irodalom

[1] Bata I. (2010) Szellőztetés; www.metros.hu/szellőztetés; Letöltve: 2010.05.03.

[2] Bedros J. R. (2004): Kiemelt fontosságú egészségügyi intézmények bioterror-támadások elleni védelmének néhány alapkérdése PhD Doktori értekezés Budapest ZMNE

[3] Bukovics I. (2004) A katasztrófavédelem helye, szerepe a XXI. sz.elején. http://www.vedelem.hu/letoltes/tanulmany/tan117.pdf; Letöltve: 2010. 05. 18.

[4] Csehi G. (2009): A bioterrorizmus jelentette fenyegetés egészségügyi kihívásai és Magyarország felkészültsége Biztonságpolitika.hu Biztonságpolitika Portál http://www.biztonsagpolitika.hu/?id=16&aid=814&title=A_bioterrorizmus; Letöltve 2010. 03. 18.

[5] Dobos G. (2007): Honvédelmi Minisztérium Magyar Honvédség honlapja: A biológiai, vegyi és radiológiai fegyverek hatása a nemzetközi stabilitásra http://www.hm.gov.hu/hirek/kiadványok/uj honvédségi szemle/a biológiai vegyi…/ Letöltve: 2009. 02. 17.

[6] Faludi G. (1998): A biológiai fegyver jelentőségének megváltozása, Honvédorvos 50. szám..38-69 oldal

[7] Faludi G. (2001): A bioterrorizmus Bolyai Szemle. 4. szám 133-169 oldal

[8] Falus F. szerk. (2008) Módosított eljárásrend az anthrax - gyanús levelekkel kapcsolatos járványügyi teendőkről Budapest ÁNTSZ-OEK belső kiadvány

[9] Halász L., Grósz Z. (2000): ABV védelem, ZMNE jegyzet, Budapest

[10] Honvédelmi Minisztérium Védelmi Hivatal (2009) Tájékoztató az Országgyűlés Egészségügyi Bizottsága Részére A bioterrorizmus és a klímaváltozás egészségügyi kihívásai, az egészségügyi ágazat katasztrófa helyzetekre való felkészülése (belső kiadvány)

[11] Greschik Gy. Alagút és metróépítés 2010.; www.mtm-magazin.hu/metró (letöltve 2010. 05. 03.)

[12] Juhász L., Huszár A.: (2009) Biohalál és bioetika, Gondolatok Ken Alibek: Biohalál című könyve kapcsán; 2009.10.17.htm (letöltve: 2009. 10. 17.)

[13] Medical Planning Guider of NBC casualties (2000): VOL II AMedP-8, US Army (http://nsa.nato.int/NSALogin/main.html); Letöltve 2010.05.30.

[14] Melles M. (szerk) (2001) Johan Béla Országos Epidemiológiai Központ Epinfo Epidemiológiai Információs Hetilap 8. évfolyam 42. szám 473-488 oldal

[15] Pellérdi R. (2007) Az ABV védelem kihívásai háborús és békeműveletekben, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi doktori Iskola Doktori (PhD) értekezés

[16] Rabiné Skripeczky A. (2006): Az Európai unió közegészségügyi politikájának fejlődése a fokozódó biológiai és kémiai terrorveszély hatására Európai Tükör 2006/3. március 110-135. oldal

[17] Sergio B. (2007): International Biobefense Handbook An inventory and international biodefense practicies and policies Center for security Studies, ETH Zurich

[18] Szalka A., Tímár L., Ludvig E., Mészner Zs. (2005)

[19] Infektológia Medicina Könyvkiadó Rt. Budapest

[20] Tarján I. (2004) Magyarország, és azon belül a Magyar Honvédség terrorveszélyeztetettsége; http://www.pecshor.hu/periodika/2004/Tarjan.pdf Letöltve: 2010. 05. 24.

[21] Tatár A. (2005): A nemzetközi terrorizmus elleni küzdelem repülésbiztonsági és katasztrófavédelmi aspektusai. Doktori (PhD) értekezés. 193.224.76.4/download/konyvtar/digitgy/nek/2005_3/04_tatar.pdf Letöltve: 2010. 04. 06.

[22] Tóth A., Tóth B. (2009) A nagyvárosok felszíni közlekedési rendszereinek vizsgálata a terrorfenyegetettség tükrében Hadmérnök IV. Évfolyam 4. szám Budapest 108-120. oldal

[23] Török T. (1995): Védelmi Tanulmányok, A tömegpusztító fegyverek létéből és elterjedéséből adódó veszélyek Stratégiai és védelmi kutatóintézet Budapest Szerkesztette Dr. Tálas Péter

[24] Zsohár I. (felelős kiadó: 2003)

[25] NBH Évkönyv 2003 Magyarország terrorfenyegetettsége www.nbh.hu/oldpage/evk2003/bmenu7.htm; Letöltve: 2010 05. 02.

[26] Varga I. (2006): A katasztrófavédelem válaszai a XXI. sz. kihívásaira, Kiskunfélegyháza; Powerpoint előadás

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Pápai Tibor
tibor.papai@gmail.com

AZ EGÉSZSÉGÜGYI TISZTEK, TISZTHELYETTESEK KATONA-KATASZTRÓFA EGÉSZSÉGÜGYI ISMERETEI BEGYAKORLOTTSÁGÁNAK KÉRDŐÍVES FELMÉRÉSE

Absztrakt

A Magyar Honvédségben a nem orvosi végzettséggel rendelkező egészségügyi tisztek és tiszthelyettesek szerepe egyre jobban előtérbe került. A jelenlegi rendszer szerint ezek a szakemberek alapképzettségüket a polgári életben szerzik, ahol speciális honvéd- katasztrófa egészségügyi ismereteket és kompetenciákat a jelenlegi oktatási struktúra alapján nem kapnak. Feltételeztem, hogy az egészségügyi tisztek és tiszthelyettesek katona- katasztrófa egészségügyi ismeretei hiányosak, nem kompetencia szintűek. A feltételezéseim bizonyítása céljából elöljáróim engedélyével 2011. április, május hónapban egy önkéntességen és anonimitáson alapuló, kérdőíves felmérést végeztem a Magyar Honvédség állományában szolgálatot teljesítő egészségügyi tisztek és tiszthelyettesek körében. A felmérés során kiemelt jelentőséggel fókuszáltam a célcsoport lőtt-, robbantásos sérült ellátásával kapcsolatos ismereteire, készségeire, melynek részeredményeit az alábbiakban osztom meg az olvasóval.

In the Hungarian Army, the role of medical officers and warrant officers, having no medical degree, come more and more into limelight. According to the present system, these experts get their basic education in civil life, where they do not get special army-catastrophe medical knowledge and competence, based on the existing educational structure. I suppose that the medical officers and warrant officers' knowledge of medical military-catastrophe is insufficiant and is not on the competence level. In order to prove my supposition, I got permission from my superiors to make a volunteer, anonym questionnaire in April and May 2011, among medical officers and warrant officers who work in the Hungarian Army. During this testing I focused more on the abilities and knowledge of handling the bullet-and-exploded-wound, I share the results with the readers in the following chapter.

Kulcsszavak: *egészségügyi tiszt, egészségügyi tiszthelyettes, katona egészségügyi ismeret, lőtt-robbantásos sérültellátás ~ army-catastrophe medical, medical officers, warrant officers, bullet-and-exploded-wound, competence*

BEVEZETÉS

A Magyar Honvédségben több éve folyamatosan zajló strukturális átalakítás valamint az új feladatok és kihívások eredményeként a főtiszti, tiszti, tiszthelyettesi, legénységi állomány aránya jelentősen megváltozott. Az utóbbi évek változásai és az életbe lépett rendelkezések, melyek a kompetencia- és feladatszintek átalakulását, eltolódását eredményezte, a ma már nagy történelmi múlttal rendelkező honvédegészségügy valamennyi területére is kihatással vannak.

A Magyar Honvédségben a nem orvosi végzettséggel rendelkező egészségügyi tisztek és tiszthelyettesek szerepe egyre jobban előtérbe került. Ennek oka igen összetett, több tényezővel magyarázható, a továbbiakban az első három prioritással bíró okot említeném. Első tényezőként a hazai lakosság jelenlegi és várható egészségi állapotának mutatóit (születéskor várható élettartam, egészségben eltöltött évek száma) kell megnevezni, melyek sajnálatos módon igen rossz tendenciát mutatnak. Ezen rossz prognózisú mutatók a honvéd egészségügyi ellátásra igényjogosultak körét is ugyan olyan arányban érintik, mint a polgári lakosságot. A honvéd egészségügyi ellátásra igényjogosultak köre 2007. július 01-től a Honvédelmi Minisztérium Állami Egészségügyi Központ megalakulásával, az igényjogosultság rendeleti szinten történő módosításával, igen jelentős mértékben megemelkedett. Az egészségi állapot mutatóinak javulásában kizárólag az érintett állomány egészségi állapotának fejlesztése, valamint a jól szervezett és valamennyi szinten hatékonyan működtetett egészségügyi ellátás és prevenciós tevékenységek eredményezhetnek sikert.

Ma már kiemelt jelentőséggel bírnak az egészségügyi katonák külföldi missziós szerepvállalásai, melyet a magyar egészségügyi katonák minden esetben példamutató helytállással, szakmaisággal teljesítenek.

Hazai viszonylatban meg kell említeni az egészségügy katonák szerepét az egyre gyakrabban előforduló, különböző nagyságú és súlyosságú minősített helyzetekben, (pl. vörös iszap katasztrófa, árvízvédelem stb.) akár a helyszíni, akár a kórházi ellátás során.

A három kiemelt prioritású feladatban az ellátandó feladatokat tekintve megállapítható, hogy legnagyobb arányban a nem orvosi végzettségű egészségügyi tisztek, tiszthelyettesek vesznek részt.

AZ EGÉSZSÉGÜGYI TISZTEK, TISZTHELYETTESEK FELADATAI, KOMPETENCIÁI

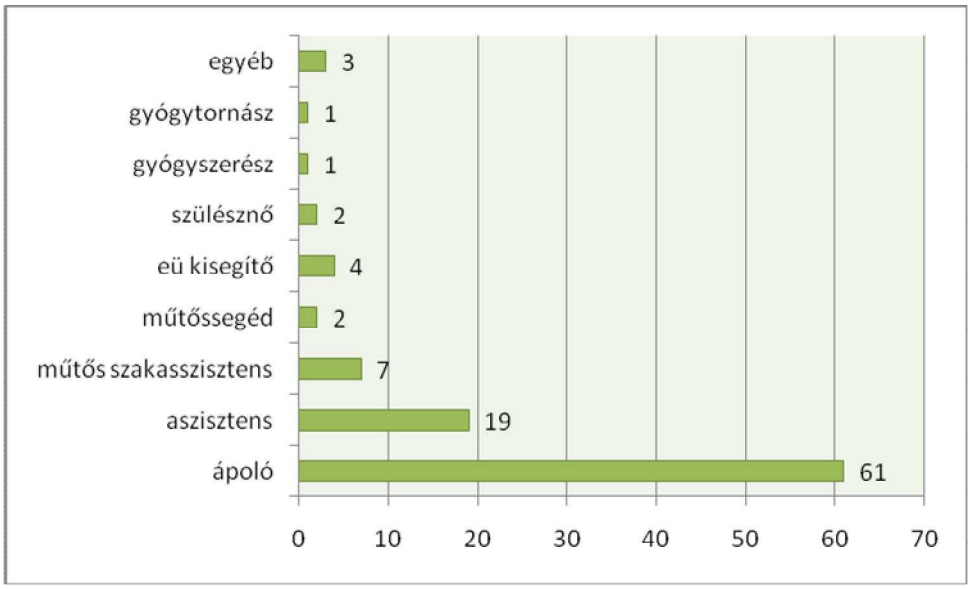
Az egészségügyi tisztek és tiszthelyettesek feladata szolgálati helytől és beosztástól függően rendkívül összetett, változó, melyet a teljesség igénye nélkül az alábbiakban törekszem meghatározni.

Békeidőben szolgálati helyüktől, beosztásuktól függetlenül elsősorban ápolói, asszisztensi, gondozói, rehabilitációs, orvos írnoki feladatok ellátása. Az MH különböző progresszivitású egészségügyi biztosításainak szervezése, szakmai elveinek kidolgozása, mozgó egészségügyi biztosítások teljesítése. A béke- és missziós egészségügyi biztosítási feladatok szervezése, végzése. A katonai pálya egészségi, fizikai, pszichikai alkalmasságának elbírálása, szervezése, irányítása. Szűrővizsgálatok szervezése, az egészségi állapotra vonatkozó adatok beszerzése, feldolgozása. A megelőző, a gyógyító-megelőző, a rehabilitációs, az egészségügyi-tudományos, az egészségügyi technikai fejlesztési és szakanyag ellátási feladatok irányítása. A felkészülés biztosítása rendkívüli, háborús, katasztrófa eseményekre, anyaggazdálkodási, közegészségügyi-járványügyi tevékenységgel. A katasztrófamedicinával kapcsolatos feladatok végzése, felkészítés, kiképzés. Vezetőként vezetői, irányítási, egészségügyi kiképzési, oktatási feladatok ellátása. Beosztástól függetlenül folyamatos

önképzés a feladatok kompetencia szintű ellátása és az elsajátított ismeretek szinten tartása érdekében. [1]

A felsorolt feladatok jól tükrözik, hogy a Magyar Honvédség valamennyi intézményében, alakulatánál jelenlévő egészségügyi katonák feladatai igen speciálisak és sokrétűek.

A honvéd egészségügy valamennyi területén szolgálatot teljesítő felsőfokú, középfokú képzettséggel rendelkező hivatásos, szerződéses egészségügyi tisztek, tiszthelyettesek és a honvédségi közalkalmazotti állomány a jelenlegi hazai képzési rendszer szerint alapképzettségüket a polgári életben szerzik, ahol speciális katona- katasztrófa egészségügyi ismereteket a jelenlegi oktatási struktúra alapján nem szereznek meg.



1. ábra. A felmérésben részt vett egészségügyi katonák polgári végzettség szerinti megoszlása (forrás: saját felmérés)

A grafikon jól szemlélteti, hogy az állomány java ápoló végzettséggel bír. A jelenlegi nomenklatúra szerint ebbe a csoportba tartozik a középfokú végzettséggel rendelkező ápoló, és az arra ráépülő különböző szakápoló (pl.: intenzív szakápoló sürgősségi szakápoló) képesítések, a mentőápoló, valamint a főiskolai szintű diplomás ápoló és az egyetemi végzettségű okleveles ápoló képesítések. Az asszisztensek csoportjában általános asszisztensek és szakasszisztensek (pl.: kardiológiai szakasszisztens, radiológiai szakasszisztens, fogászati szakasszisztens stb.) tartoznak. Az egészségügyi kisegítő csoportba a betegszállítókat soroltam. A többi csoportnál már nem jellemző az ilyen fokú heterogenitás.

A hazai közép- és felsőfokú egészségügyi képzési struktúrát jól ismerve kijelenthetem, hogy sajnos a jelenlegi rendszerben az OKJ szintű mentőápoló, sürgősségi ápoló és a főiskolai szintű mentőtiszt képzéseken kívül egyik végzettséggel sem bocsájtunk ki a képzőintézményekből olyan szakembereket, akik megfelelő sürgősségi szemlélettel és készséggel rendelkeznek. Az egészségügyi szakdolgozók nagy része békeidőben, a mindennapi munkája során sem képes a rendkívüli sürgősségi helyzetekhez adaptálódni. Egy hirtelen fellépő egészségkárosodás, baleset gyakran stressz és pánik választ vált ki belőlük, nem képesek a kompetenciájuknak megfelelő ellátást nyújtani a sérültnek, betegnek. Ennek oka a képzési struktúrában keresendő, bár ma már valamennyi egészségügyi képzésben, főleg a képzés elején szerepel az elsősegélynyújtás, azonban a képző intézmények financiális okokból, csökkentett óraszámban, nagy csoportokban végzik az oktatást és a képzés befejeztével már a szinten tartás az érintett alkalmazott és munkahelyének motivációjától függ. Ezért az elsősegélynyújtás készség szintű alkalmazásáról nem beszélhetünk. 2007-ben kérdőíves felméréssel vizsgáltam az egészségügyi szakdolgozók újraélesztési ismereteit, a

felmérés elvégzésére motiváló hipotézisem, mely szerint -az egészségügyi szakdolgozók újraélesztési ismeretei hiányosak- sajnos bebizonyosodott.[2] A felmérés 2010-ben történt megismétlése során sem volt jelentős változás értékelhető.

Ezen empíriák alapján feltételeztem, hogy az egészségügyi tisztek és tiszthelyettesek (beleértve magam is!) katona-, katasztrófa egészségügyi ismeretei hiányosak, nem kompetencia szintűek a nem megfelelő képzés és szinten tartás miatt. A feltételezéseim bizonyítása céljából elöljáróim engedélyével 2011. április, május hónapban egy önkéntességen és anonimitáson alapuló, kérdőíves felmérést végeztem a Magyar Honvédség állományában szolgálatot teljesítő egészségügyi tisztek és tiszthelyettesek körében. A kérdőív 52 különböző (zárt, nyitott, rangsor, osztályozó) típusú kérdést tartalmazott. A kérdéseim a témával kapcsolatos kompetenciákra, ismeretre, képzésre, képzési igényre, és karrier modellre vonatkoztak. Az értékelhető kérdőívek száma 207 darab volt, mely a vizsgálandó célcsoport létszámához viszonyítva jónak mondható, ennek ellenére az eredményt reprezentatív jellegűnek tekintem.

A LŐTT- ROBBANTÁSOS SÉRÜLTEK HELYSZÍNI ELLÁTÁSÁNAK JELENTŐSÉGE

Feltételezéseim bizonyítására a széleskörű kérdőíves felmérésem során kiemelt jelentőséggel fókuszáltam a célcsoport lőtt-, robbantásos sérült ellátásával kapcsolatos képességek végzésére, békeidőben a mindennapi munka során, a harctéri speciális körülmények között és a felkészítő gyakorlatok során. Az ilyen jellegű sérülésekkel az egészségügyi tisztek, tiszthelyettesek gyakran találkozhatnak elsősorban békefenntartó missziókban (KFOR, ISAF). Az egyéni védőeszközök és a páncélozott gépjárművek fejlődése és széles körben történő alkalmazása miatt, a lőfegyveres támadásokkal elkövetett sérülések száma jelentősen emelkedett. Sajnos hasonló mechanizmusú sérüléssel békeidőben is szembesülhetünk, különböző ipari jellegű robbantások, visszamaradt nem hatástalanított háborús robbanószerkezetek, vagy különböző terrorcselekmény, alvilági leszámolás formájában. Ezen sérülési mechanizmusok tanulmányozásával megállapítható, hogy a lőtt-robbantásos- és repeszsérülések arányai a lőfegyverek fejlődésének függvényében változnak. A súlyos, többszörös sérültek aránya, a repeszsérülések arányának növekedésével párhuzamosan jelentősen megemelkedett. Az előidézett sérülésekre a lágyrész sérülések, jelentős vérzések, fedett hasi sérülések, mellkasi sérülések, nyílt és szilánkos csonttörések, valamint koponyasérülések jellemzők. A mechanikus traumákon túl a robbanáskor keletkező hő és láng égési sérüléseket, a gáztermékek toxikus ártalmakat okozhatnak.

A felkutatott szakirodalmi adatok arra utalnak, hogy a béke és háborús körülmények közt előforduló lőtt-robbantásos sérülések miatti halálozást az életfontosságú szervek roncsolódása, a heveny vérveszteség és annak következményeként kialakult sokk és légzési elégtelenség okozza. A halálesetek oka az első 10 percben az életfontosságú szerv, szervek nagyfokú roncsolódásában, 2-3 órán belül a nagyfokú vérveszteségben, 4-12 órán belül a sokk miatti szervi elégtelenségben jelölhető meg. [3] Ezen ismeretek birtokában megállapíthatjuk a sérültek letalitásának és a maradandó károsodások számának csökkentése érdekében, döntő szerepe van a sérülés – kimentés - segélynyújtás folyamat időintervallumának, a magas kompetenciaszintű, jól szervezett segélynyújtásnak, valamint az első sürgősségi segélyhelynek. Ennek az ellátási folyamatnak valamennyi szintjén helyet kell, kapjon a jól képzett, kompetenciáit készség szinten alkalmazó egészségügyi katona. Ezen állítást alátámasztja, hogy a sérültek kiszállítási időtartamának és az első szakszerű sürgősségi segély fejlődésének köszönhetően a harcmezei primer letalitás 10-12%-ra csökkenthető, így a kórházat élve elérő súlyos sérültek aránya lényegesen jobb. [4]

A LŐTT- ROBBANTÁSOS SÉRÜLÉSEK HELYSZÍNI ELLÁTÁSÁNAK ALGORITMUSA

A felmért képességek és kompetenciák értelmezéséhez elsőként fontos megismerni a lőtt-robbanásos sérülések helyszíni (prehospitális) ellátása során alkalmazható kompetenciákat. Az ellátási taktikát a helyszín biztonsága, a sérültek száma, állapota, és a mentésben résztvevők száma, kompetenciája és a rendelkezésre álló mentéstechnikai eszköz jelentősen befolyásolhatja, módosíthatja. [5]

- Az esemény jellegének tisztázása:
  - pontos helyszín, veszélyforrások
- A biztonságos helyszín, mentési környezet biztosítása:
  - biztosítás (elektromos tevékenységek beszűntetése, mobil telefonok kikapcsolása)
  - műszaki mentés
  - mentesítés (fém és kémiai anyagok)
  - a fel nem robbant eszközök felügyelete
  - bizonyos esetekben a mentésben résztvevők számát minimalizálni kell
- Helyszíni betegosztályozás (triage):
  - a sérültek számának, súlyossági állapotának meghatározása
- 4. Helyszíni beavatkozások elvégzése a körülményekhez adaptálva:
  - keringés fenntartása, újraélesztés - csak kapacitás függvényében!
  - a nyaki gerinc rögzítése speciális rögzítő eszközzel - minden sérültnél!
  - légútbiztosítási alternatívák alkalmazása - sérülés függvényében
  - feszülő légmell ellátása - szükség esetén
  - lélegeztetés túlnyomás nélkül
  - vérzéscsillapítás (műveleti területen torniquet-el, lokális vérzéscsillapító szerekkel)
  - folyadékpótlás mielőbbi elkezdése perifériás véna- vagy intraosseális kanülálással
  - fájdalom csillapítása
  - sebellátás, égés esetén égési kötszer alkalmazása
  - sérült védelme a kihűléstől izolációs fóliával
  - a sérült rögzítése vákuummatracba, gerinchordágyon
  - sérült megfigyelése eszköz nélkül, eszközzel (lehetőségek alapján) a transzportig
- A sérült transzportja.

AZ EGÉSZSÉGÜGYI TISZTEK ÉS TISZTHELYETTESEK LŐTT, ROBBANTÁSOS SÉRÜLT ELLÁTÁSSAL KAPCSOLATOS ISMERETEI, KOMPETENCIÁI

A kérdőívben a célcsoport lőtt, robbantott sérült ellátás, légútbiztosítás, vénabiztosítás-infúzió bekötés, intraosseális kanülálás, kompetenciák kiképzéseken történő gyakorlásának gyakoriságát vizsgáltam.

2. ábra. Lőtt, robbanásos sérült ellátás gyakorlásának gyakorisága kiképzéseken; (forrás: saját felmérés)

Az ilyen mechanizmussal sérültek ellátási menetének készség szintű ismerete minden egészségügyi katona alap kompetenciája közé kell, tartozzon. Itt kellene elsajátítani a szituáció során a gyors helyzetfelismerést és felmérést, a helyszín biztonságos megközelítését és a biztonságos környezet kialakítását, a sérültek elsődleges vizsgálatát és állapotfelmérését, az ellátási prioritás felállításának (triage) módszerét és a helyszíni ellátás menetét, taktikáit.

A grafikonok elemzése alapján megállapítható, hogy a válaszadók 33,4 %-a soha nem gyakorolta, 44 %-a csak egyetlen egy alkalommal gyakorolta a lőtt, robbantott sérült ellátásának menetét. Csak a válaszadók 22 %-a vett részt már több alkalommal ilyen gyakorlaton. A felmérés egyik kérdéséből kiderül, hogy a válaszadók 95-96 %-a még soha nem vett részt sem békeidőben, sem harctéri körülmények közt ilyen jellegű sérült ellátásában, azonban ez nem mentesíti őket ezen képességek alkalmazása alól.

A téma kiemelt jelentősége miatt a megfelelő gyakorlattal rendelkezők száma igen alacsonynak mondható. A kritikus állapotú sérültek kompetencia szintű, minőségi ellátásának egyik kulcspontja az új ismeretek, készségek elsajátításán túl a rendszeres gyakorlás, szinten tartás a valós körülményekhez legjobban igazodó szituációkkal. Az elsajátított kompetenciák szinten tartásához, beosztástól függetlenül évente legalább egyszer ismétlő gyakorlaton kellene részt vennie az állomány valamennyi tagjának.

3. ábra. A légútbiztosítás gyakorlásának gyakorisága kiképzéseken; (forrás: saját felmérés)

Valamennyi súlyos sérülés és rosszullét következménye lehet az eszméletlenség. Az eszméletlen sérült ellátásának egyik legfontosabb feladata a szabad légutak biztosítása, és szabadon tartása, melynek eszköz nélküli és eszközös módjait kell ismerni valamennyi egészségügyi katonának. Az eszköznélküli légútbiztosítás módja a stabil oldalfekvő helyzet, annak tilalma esetén a fej hátrahajtása, az áll előre emelése. Az eszközös légútbiztosítás alternatívái széleskörűek a garatba bevezetett pipa, légcsőbe bevezetett cső (intubácio) vagy a légcsőmetszés alkalmazása lehetséges megfelelő kompetenciákkal. Az eszköz nélküli légútbiztosítás és a garatba vezetett pipa alkalmazása valamennyi egészségügyi katona kompetenciája kell, legyen. A felmérésből kiderül, hogy a megkérdezett állomány 26 %-a soha nem gyakorolt speciális szituációban semmilyen légútbiztosítási eljárást. Az eszközök alkalmazásának feltétele a megfelelően elsajátított technika Az eszköz nélküli légútbiztosítás életmentő beavatkozás a polgári életben valamennyi elsősegélynyújtó vizsgán követelmény!

4. ábra. Véna biztosítás gyakorlásának gyakorisága kiképzéseken; (forrás: saját felmérés)

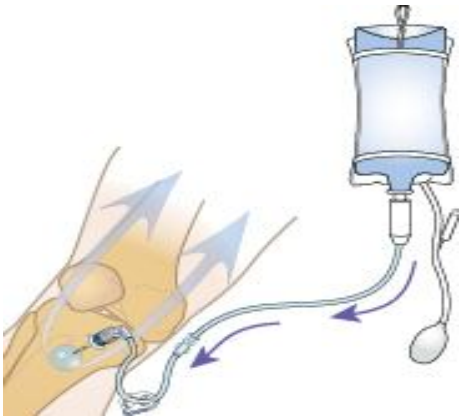
A vénabiztosítás a polgári életben megszerzett képesítések közül csak az ápolók és szülésznők csoportjának kimeneti kompetenciájában jelenik meg és leggyakrabban a békeidős betegellátás során is csak ők alkalmazhatják megfelelő munkahelyi felhatalmazás alapján.

Azonban valamennyi esetben a kritikus állapotú betegek, sérültek sürgősségi ellátásban idejekorán alkalmazott korrekt folyadékterápiának, gyógyszeradagolásnak kiemelkedő jelentősége van, ezért a minősített, rendkívüli körülmények között valamennyi egészségügyi katonának alkalmaznia kell a vénabiztosítást. Ahogy ez a felmérés során bebizonyosodott az egészségügyi katonák 48 %-a soha nem, 33 % egyszer gyakorolta a vénabiztosítást, speciális és harctéri körülmények között. Tekintettel arra, hogy a felmérésben résztvevők közel 60%-a az ápolói végzettségű csoportba tartozik, így ezzel a kompetenciával rendelkezik, figyelemfelkeltő, hogy miért nem gyakorolják rendszeresen a beavatkozást speciális körülmények közt.

5. ábra. Az intraosseális kanülálás gyakorlásának gyakorisága kiképzéseken; (forrás: saját felmérés)

Perifériás vénabiztosítás a kritikus állapotú, rossz perifériás keringésű betegek esetében igen nehéz, időigényes lehet, és megfelelő rutint kíván, ezért fontos megismerni az intraossealis kanülálás módját. Ez a technika biztonságos, gyors (10 sec.) és a tapasztalatlan kézben is könnyű vénás hozzáférést biztosít.

Napjainkban az intraossealis kanülálást az intravénás bejuttatás elsődleges alternatívájaként ajánlják az újraélesztés és a kritikus állapotú betegek ellátása során. Maga az intraosseális bejuttatás módszere nem új. A II. világháborúban a súlyosan sérült katonák volumenpótlása során több mint 4000 esetben alkalmazták sikeresen, így napjainkban is a hadműveleti területen, szükség esetén ezt a módszert alkalmazzák a harctéri ellátást végző katonák. A beavatkozást a válaszadók 81,5 %-a nem alkalmazta még soha. Ennek oka lehet, hogy a beavatkozást hazai viszonylatban főleg a prehospitális ellátásban (mentésben) alkalmazzák, ott sem napi rutin beavatkozásként. A harctéri ellátás során alkalmazott inraosseális kanülálás jelentősége egyenértékűnek mondható a vérzéscsillapításra alkalmazott torniquet-el, így ennek a módszernek az ismerete is kiemelt jelentőséggel kell, bírjon az egészségügyi katonák képzése során. [6]



6. ábra. Infúzió bejuttatás intraosseális kanülön a csontba

A kérdőíves felmérés során természetesen a célcsoport speciális katona-, katasztrófa egészségügyi feladatainak ellátáshoz szükséges további kompetenciákkal kapcsolatos ismereteket is felmértem. Mentés terepen, lövészárokból, magasból, segélyhely telepítés, hadszíntéri ismeretek és feladatok, katasztrófavédelmi ismeretek, ABV ismeretek, járványügyi ismeretek témaköröket érintettem, melyekben hasonló eredmények voltak mérhetők.

ÖSSZEFOGLALÁS

A szemléltetett válaszok alapján megállapítható, hogy rendkívül bonyolult és összetett feladatkör, valamint a hadtudományban, orvostudományban, ápolástudományban zajló gyors és folyamatos szakmai és technikai fejlődésnek elsajátítása, szinten tartása, fejlesztése érdekében elengedhetetlen lenne az egészségügyi szakdolgozói állomány speciális képzése, továbbképzése. Az alábbi összefoglaló táblázat jól szemlélteti, hogy a kérdőíves felmérésben résztvevők érzik a témával kapcsolatos hiányosságaikat.

a képesség megnevezése	a képességek gyakorlásának százalékos megoszlása				
	soha	egyszer	2-5	6-10	10-nél
lőtt-robbantott sérült ellátása	33,4 %	44,5 %	11,2 %	3,8 %	7,5 %
légútbiztosítás	26 %	51,9 %	11,2 %	7,5 %	3,8 %
véna biztosítás	48,2 %	33,4 %	7, 5 %	3,8 %	7,5 %
intraosseális kanülálás	81,5 %	14,9 %	3,8 %	0	0

1. táblázat. A kérdőíves felmérés adatainak összefoglaló táblázata; (forrás: saját felmérés)

A válaszadók hajlandóak lennének rendszeres gyakorlatokon, képzéseken részt venni. Egyre nagyobb igény jelentkezik a katona- és katasztrófa egészségügyi ismeretek főiskolai, egyetemi szintű képzésére, melyhez harmonizálni kellene a szakmai és rendfokozati előmenetelt.

A honvéd egészségügy valamennyi területén szükségszerű olyan korszerű kiképzési struktúra kidolgozása az egészségügyi tisztek, tiszthelyettesek felkészítésére, melyekkel az ellátandó feladat hatékonysága növelhető. A cél az egészségügyi állomány részére korszerű alapismeretek átadása, az elsajátított ismeretek folyamatos bővítése, készség szintre emelése, hogy mindennapi munkájuk során és rendkívüli helyzetekben, a béke viszonyokhoz kevésbé hasonlító nehézségek mellett is megfeleljenek annak az elvárásnak, miszerint lehetőleg minél több sérültet legyenek képesek az egységes ellátási elvek alapján magasabb szintű ellátásban részesíteni.

A megfelelő képzési program kidolgozásához elengedhetetlen a háborús körülmények, fegyveres konfliktusok, természeti katasztrófák, ipari és közlekedési katasztrófák egészségre gyakorolt hatásainak, azok ellátási módjának, főbb következményeinek tanulmányozása,

statisztikai módszerekkel való elemzése. Tanulmányozni kell a NATO és Európai Unió katona egészségügyi szolgálatainak rendszerét, működését, az adott rendszerben működő egészségügyi tisztek, tiszthelyettesek kiképzésének módjait, hogy a kidolgozott képzési módszerrel NATO és EU kompatibilis szakmai és karrier kiépítésének lehetősége biztosítva legyen az egészségügyi tisztek és tiszthelyettesek számára.

Felhasznált irodalom

[1] Dr. Svéd László: A Magyar Honvédség egészségügyi biztosítása elvének és gyakorlatának változásai, sajátosságai, különös tekintettel a haderő átalakításra, a NATO-ba történő integrálásra, a különböző fegyveres konfliktusok, valamint a békefenntartó, béketeremtő és –támogató tevékenységre." – Doktori értekezés ZMNE (2003)

[2] Pápai Tibor: Az egészségügyi szakdolgozók újraélesztési ismeretei 2007-ben. Ápolásügy, 21. évf. 4. szám.(2007) 8-11.

[3] William Winkler: Egészségügy és a korszerű harc. – NATO's sixteen nations:& partners for peace, 1986, 4: 50-53

[4] Creanier Ian: Sebesült szállítás a központi hadszíntéren, a központi körzetben. - NATO's sixteen nations: & partners for peace, 1989, 7: 62-65

[5] Dr. Várhelyi Levente: Robbanásos sérülések sebészi ellátásának kérdései – Doktori értekezés ZMNE (2010)

[6] Jones and Bartlett: Combat Medic Field Reference, 2005, 13-23, 209-214.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Potóczki György
vamsped@chello.hu

VANNAK-E TOVÁBBFEJLESZTÉSI LEHETŐSÉGEK A KATASZTRÓFÁKAT MEGELŐZŐ IDŐSZAK LAKOSSÁGFELKÉSZÍTÉSI TEVÉKENYSÉGÉBEN?

Absztrakt

A nem kívánatos események bekövetkezte előtti lakossági felkészítés fontossága vitathatatlan. Más védelmi területeknél (pl. egészségügy, kriminológia) is felismert tény: a megelőzésre többet, a következményre kevesebbet kellene költeni, a helyzet mégis fordított. Kérdés: Mi jellemzi a mai állapotokat? Létezik-e, működik-e egy optimális lakosságfelkészítési metodika? Ha nem, akkor már az ideális állapotokhoz történő közelítés is jelentős eredménynek számíthat. Szükségesnek tűnik a lakosságfelkészítés mai gyakorlatának felülvizsgálata, esetleg átalakítása, ezt erősíti a jelenleg folyamatban lévő jogszabályi korrekció is. A szerző – a jelenlegi helyzet vázlatos áttekintése mellett – keresi a korunk viszonyaihoz jobban illeszkedő megoldásokat, elsősorban a megelőző időszakban végzett megelőző felkészítésre koncentráltan.

The importance of raising public awareness in periods that precede any unwanted event is beyond doubt. In other areas of protection (e.g. healthcare, criminology) it has been acknowledged that more extensive funds should be spent on prevention than on the consequences; still, the situation is just the opposite. The question is: What are the attributes of the situation today? Does an operable optimum methodology raising public awareness exist? If not, any approach towards the ideal situation can be considered a major result. It seems that the review, or possibly, the transformation of the practice in raising public awareness is necessary; this is also supported by the proposed amendment of the applicable statutes, currently under way. The author – in addition to providing a draft overview of the current situation – seeks solutions better adjusted to the conditions of our time, mainly focusing on the preparatory activities carried out in preceding periods.

Kulcsszavak: *lakossági felkészítés, katasztrófavédelem, megelőző időszak, felkészítési módszerek és eljárások ~ raising public awareness, disaster recovery, preceding period, preparation methods and procedures*

BEVEZETÉS

A katasztrófavédelem sokat változott az 1989-90-es politikai és gazdasági rendszerváltás óta. A változás részben külső körülmények hatására, részben a belső működés korszerűsítésének igénye okán zajlott le mind szervezeti, mind tevékenységi értelemben. E folyamat eredményeként az ezredfordulón átalakultak a katasztrófavédelmi szabályok és fogalmi rendszerek.

A ma már közismert megelőzés, védekezés, helyreállítás hármas feladatrendszerén belül a megelőzés is több részre tagolódik, nevezetesen

- előzzük meg a nem kívánatos esemény bekövetkeztét,
- csökkentsük a károsító hatást, ha már akaratunktól függetlenül is bekövetkezik a nem kívánatos esemény,
- biztosítsuk a védekezés személyi, tárgyi, gazdasági feltételeit (ide sorolható a lakossági felkészítés)

A vizsgált lakossági felkészítés alapvetően megelőző időszaki teendő, amely egyaránt vonatkozik a megelőzés, védekezés és helyreállítás feladataira is. A katasztrófa megelőzés szakaszát a néhány nemzetközi szakirodalmi forrás felkészülési és figyelmeztetési szakaszra osztja, azonban a hazai jogszabályokban nincs ilyen osztályozás.

Jelen cikk nem az egyébként fontos szakmai felkészítést[1] vizsgálja, inkább egy meghatározó részterületet: a lakossági felkészítést, annak is a megelőző időszaki funkcióit elemzi-értékeli a használatos módszerek, eljárások áttekintése útján.

A témakör régi, de most is aktuális és állandó kihívást jelent. A szakterület nem kellően kutatott, sok a megoldatlan probléma. A legnagyobb dilemma nem a szakmai tartalom összeállítása, vagy szervezeti-technikai kérdések megoldása, az állomány szervezése, hanem éppen a megóvandó emberi közösség szakirányú érdeklődésének felkeltése, befogadó készségének biztosítása, részvételi hajlandóságának elérése és a változások „utánkövetése”.

Felmérésekből tapasztalható, hogy a lakosság széles rétegei nem kívánnak aktívan részt venni felkészülési feladatokban. Az ok nem az elutasító magatartásban, hanem az emberi agytevékenységben keresendő. Nevezetesen: az emberi agy a kisvalószínűségű, időben távolinak tűnő, különösen negatív kihatású eseményeket szinte automatikusan „kilöki” tudati bázisából, kb. 15-30 napon belül. Az emberek többsége fel sem ismeri saját kockázati érintettségét, vagy a védelmet – a jogszabályi kötelezettségek ellenére is – egy-egy rendvédelmi és/vagy közigazgatási szervezet kizárólagos feladatának tartja. Pedig szinte bármely felkészítés igényelné az érintettek személyes közreműködési készségét is. Igazolható, hogy a lakosságnak instabil társadalmi-gazdasági viszonyok között szinte automatikusan fokozódik a belső indíttatású önvédelmi igénye (élelmiszertartalékolás, stb.).

Minden igényt kielégítő, garantáltan hatékony és olcsó felkészítési eljárást nem lehet találni sem a jogszabályi környezetben, sem a releváns szakirodalomban, ezért már a kívánt felkészítési állapotokhoz történő közelítés is jelentős eredménynek számíthat. Jogszabályaink egy-két évtizeddel korábbi társadalmi-gazdasági viszonyokat tükröznek, így módszereikben nem használhatják az időben később megjelenő technikai eszközöket. Jelen cikk írásának idején új szakirányú koncepció létezik [1] és folyamatban vannak a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló új törvénytervezet jogalkotási,

1 A szakmai felkészítés fogalmán itt a lakossági felkészítést végző hatósági/közigazgatási/pedagógusi apparátus oktatását, kiképzését, tehát „a felkészítők felkészítését” értem. Tudom, hogy nagyon nehéz a kettőt szétválasztani, hiszen a szakmai felkészültségre épül a lakossági felkészítés, a rendszerek egymást feltételezik.

döntés-előkészítési munkálatai. [2] Vajon célszerű-e fenntartani az egyes elemeiben párhuzamosnak tűnő jogszabályi rendszert2. [3] [4]

Fentiek alapján segíteni és keresni kell a felkészítés új módozatait, korunk infokommunikációs adottságainak figyelembevételével.

A MEGELŐZŐ IDŐSZAKI LAKOSSÁGFELKÉSZÍTÉS HELYZETE, HASZNÁLATOS MÓDSZEREI

A katasztrófavédelmi felkészítés korábbi szakasza leginkább a légoltalom megszervezésével jellemezhető, kiemelve a Vöröskereszt, az iskolák, a munkahelyek és a lakóházak szerepét, de ezek elsősorban háborús védelmi indítékúak voltak. A rendszerváltás, az ENSZ, a NATO és az EU tagság kezdete a felkészítési funkciók, célok változását is magával hozta, hiszen a háborús védelem szempontjai helyett a békeidőszaki – természeti és civilizációs – veszélyek, kockázatok, illetve kihívások kerültek a gondolkodás középpontjába.

Napjaink helyzet elemzésekor a következőkből lehet kiindulni: *„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."* [5] Bár a hatályos törvény értelmező rendelkezéseiben a katasztrófavédelem „*a katasztrófa kialakulásának megelőzését* … is *szolgálja*"[3], mégis úgy tűnik, hogy a katasztrófaveszély állampolgár általi megismerése jog, de nem kötelezettség, a védelmi közreműködés azonban mindkettő. Nyelvtanilag ez úgy is értelmezhető, hogy a felkészítésben történő személyes részvétel nem kötelező, a konkrét védelemben pedig igen.

A védekezésre és a következmények felszámolására kijelölt szervek, szervezetek, intézmények, köztestületek, gazdálkodók, szolgálatok, önkormányzatok, okozók és előidézők között szerepelnek az állampolgárok is. Az állampolgári kötelezettséget jogszabály konkretizálja: „*A katasztrófavédelemben részt vevők feladataikat - ha jogszabály másként nem rendelkezik - e törvény alapján, illetőleg a polgári védelmi kötelezettség keretében látják el."* [6] Az idézett törvényhely a polgári védelemről szóló 1996. évi XXXVII. törvény szerinti kötelezettségre utal, amely pontosabban definiálja az érintett állampolgárok körét, a kötelezettségek (adatszolgáltatás, bejelentés, megjelenés, szolgálatadás) tartalmát és az azok alóli mentességeket is. [7] Itt érhető tetten a lakosság megelőző időszaki felkészítésében történő – címzett kivételekkel tarkított – személyes állampolgári részvétel kötelező jellege, azonban e kötelezettség kikényszeríthetősége, gyakorlati szankcionálása viszont erősen kérdéses. Nem elégséges a lakossági felkészítés jelen állapota, hiszen az nincs arányban sem a biztonsági kockázatokkal, sem azok változásaival. A helyzet kissé hasonlítható egyes kötelezővé tett egészségügyi szűrővizsgálati (pl. tüdőszűrés) eljárások állapotához.

A jogi háttér vizsgálata vegyes képet ad. Több jogforrásból állítható össze a jogok és kötelezettségek halmaza, de az egyes fejezetekről találhatóak olyan elemzői megállapítások is, hogy a joganyag rendelkezései „*hiányosak, elavultak, nem tartalmaznak olyan elemeket, amelyek nélkülözhetetlenek a lakosságfelkészítés jó működéséhez, mint például a felelősök,*

---

[2] Itt arra gondolok, hogy a szervezete, működése szempontjából katasztrófavédelem néven egységbe integrált tűzoltóság és polgári védelem jogi háttere nem kis mértékben még mindig az elkülönítetten létező és hatályos törvényekben szabályozott. Érdekes, hogy az EU szabályok (pl. Lisszaboni szerződés [3], [4]) címzetten a polgári védelmet említik, a tűzoltóság szakmai tevékenységet egységesen nem szabályozzák és nem használják a katasztrófavédelem integrált fogalmát sem.

3 Lásd az 1999 évi LXXIV Törvény I. Fejezet 3 § e) részében.
http://www.katasztrofak.abbcenter.com/?id=30319&cim=1
Letöltve: 2011.05.16.

felkészítési tartalmak, anyagi források megjelölése. Hiányolom a polgármesterek, a tanulóifjúság, valamint a lakosság szélesebb köre felkészítésének jogi szabályozását." [8]

A felkészítéstől való állampolgári tartózkodás, vagy idegenkedés elvileg felfogható úgy is, hogy a kiértesítések ellenére távolmaradók önmaguk viseljék saját döntésük későbbi következményeit, de a feladat az interdependenciák[4] miatt sokkal komolyabb annál, minthogy a kérdéskör személyekre vonatkoztatott kockázatáthárítási logikával megoldható legyen.

Közismert, hogy minősített helyzetben az ún. legitim (állami) erőszak puhább verziója érvényesíthető (értsd: veszélyhelyzeti, vagy helyreállítási időszakban), de kérdéses, hogy ez egészében vállalható-e a megelőző időszaki lakossági felkészítésre? A megelőző időszaki lakossági felkészítés nem technikai, vagy szervezési feladat, hanem olyan folyamatos feladatellátást igénylő össztársadalmi ügy, amelynek nemzetközi vonatkozásai is vannak.

A jelen feladatokat alapvetően a polgári védelemről szóló törvény[5] határozza meg. A polgári védelmi feladatok szervezésében, irányításában, végrehajtásában – törvényben szabályozott módon és szervezeti felépítésben - részt vesz az Országgyűlés, a Kormány, a Belügyminiszter, a Megyei Közgyűlés Elnöke, a Főpolgármester, a Polgármester, a Védelmi Bizottság, akik feladataikat államigazgatási jogkörben láthatják el.

Napjainkban „*A katasztrófák elleni védekezés irányítása, feladatainak végrehajtása*

- a nem hivatásos katasztrófavédelmi szervezetek (állami szervek, közigazgatás, bizottságok), a
- hivatásos katasztrófavédelmi szervezetrendszer (OKF területi és helyi szervei) és
- az együttműködő szervek segítségével (fegyveres erők, rendvédelem, egészségügy, karitatív szervek, mentők, tisztiorvosi szolgálat, meteorológia, egyes gazdálkodó szervezetek, egyesületek, stb.), valamint
- a KV ágazati irányításának különböző területei (a védekezési bizottságokba kijelölt, hatáskörökkel rendelkező koordinációs szervezetek alaposan eltérnek egymástól pl. a közlekedési, vízügyi, nukleáris, környezetvédelmi, egészségügyi, vagy migrációs igazgatás tekintetében)

koordinált munkáján keresztül valósulhat meg." [9]

A közelmúlt két „nevezetes" hazai eseménye (a 2010. május-júniusi borsodi ár-és belvíz, valamint a Kolontári, Devecseri vörös iszap áradat) több tanulsággal szolgált. Az elismerésre méltó társadalmi összefogás, a komoly áldozatvállalás, valamint védekezésben érintett szervek példás együttműködése jelentős eredményt hozott a védekezésben és a kárelhárításban. Azonban kérdéses: Fel volt-e készülve a közvetlenül, vagy közvetetten érintett lakossági szféra ilyen méretű, kihatású és időben elhúzódó eseménysorozatra? Nyilvánvalóan nem, hiszen még a mentésben, kárelhárításban hivatásszerűen/önkéntesen résztvevő egységek számára (katasztrófavédelem, rendőrség, honvédség, önkormányzatok, karitatív szervezetek, stb.) is megfeszített feladatot jelentett a helytállás, a helyzet kezelése. Az érintett lakosság ismeret-, vagy tájékoztatáshiánya – a két említett konkrét eseménytől elvonatkoztatva és általánosítva - rámutathat a megelőző időszaki felkészítés hiányosságaira és korszerűsítésének szükségességére is. A védelmi rendszer - működés közben - meglehetősen sokszereplős, így külön figyelmet kell fordítani az esetleges párhuzamosságok kiszűrésére is.

[4] Az interdependencia kifejezés alatt az azonosított kapcsolati összefüggéseket értem. Témánk szempontjából azt hangsúlyoznám, hogy a megelőző lakossági felkészítés nemcsak az érintett személyek előzetes tájékoztatását, célirányos kiképzését, hanem sok további – itt nem részletezetett, de ezzel összefüggő - teendőt is tartalmaz.

[5] Lásd: A polgári védelemről szóló 1996. évi XXXVII . sz Törvény 4 §. a)-m) pontok
http://www.otm.gov.hu/kok/inside/joganyagok/1996_XXXVII.pdf
Letöltés: 2011.05.06

Elgondolkodtató, hogy „a polgármesterek többsége nem rendelkezik még a védekezés, védelmi szervezés alapismereteivel sem, az ezzel összefüggő jogszabályi kötelezettségeiket nem ismerik, így azok végrehajtása hiányos.” [10] Ez elég komoly és mielőbb orvosolandó problémát jelenthet - ha marad a hatályos szabályozás -, hiszen kulcsszereplőkről van szó.

A katasztrófavédelemre kidolgozott új szakmai koncepcióban[6] az szerepel, hogy „a hatósági jogköröket a polgármesterektől és a megyei közgyűlés elnökeitől részben, vagy egészben át kell telepíteni a katasztrófavédelemhez. Indok: így elkerülhető az időszakonként változó hatáskört gyakorló személy” újbóli betanítása, a gyakorlatlanságából származó többletköltség ráfordítás és az ismerethiányból származó szakszerűtlen beavatkozás.

A demokráciák jellemzője, hogy általában a választott tisztségviselőkhöz van telepítve a döntési jogkör, de esetükben a választhatóság kritériumaként nincs megjelölve képesítési követelmény, mint jelöltállítási előfeltétel. Ez a szituáció előfordul a polgármesteri munkaköröknél is, ahol sok szakma[7] döntésigénye koncentráltan egy kézbe fut össze (a szakma csak javasol, de a polgármester, vagy a szintén választott tisztségviselőkből álló képviselő testület dönt). Az a körülmény, hogy a döntési pozícióban lévő polgármester kis- és közepes településeken nem alkalmazhat minden (általa felügyelt) területhez szakembert, előrevetíti a későbbi problémák jelentkezését.

A polgármesteri munkakör leterhelt, összetettsége közismert, politikai tartalommal is telített, ezért hatékonyabb munkára lenne szükség a polgármesteri hivatalok kijelölt tisztviselői és a területi szakmai szervezetek (polgári védelmi szervezet, védelmi bizottságok) között. Tovább növeli ennek fontosságát, ha az önkormányzatok egy részénél ismerethiány, eszközhiány és módszertani problémák (akár egyidejűleg) is jelentkeznek.

Fontos a települések polgári védelmi besorolása[8] is, hiszen egyedi helyzetekről van szó. (Az I.-II. besorolású települések száma igen magas /ezer felett van/, de a nem besoroltak /939/ esetében is szükség van megelőző időszaki felkészítésre).

A lakosságfelkészítésnek a katasztrófavédelmi tevékenység minden területén jelen kell lennie. Erről jó áttekintést található Veresné Hornyacsek Júlia értekezésében. [11]

A felkészítés szakmai tartalma az általános és helyi kockázatoktól, veszélyhelyzetektől, a korábbi extrém eseményeknél szerzett tapasztalatoktól, a definiált célcsoportoktól, valamint a pánik körülmények eseti megítélésétől függ, legfontosabb követelményei:

- alkalmazkodni kell a jogszabályokhoz,
- be kell tartani az pénzügyi kereteket,
- meg kell felelni az általános és a helyi szakmai elvárásoknak,
- növelni kell a korszerű megoldások arányát,
- követni kell kockázatok változó összetételét,
- koordinálni kell a felkészítő szervezetek munkáját,
- mérni kell a felkészítés eredményességi oldalát,
- biztosítani kell a felkészültség közel azonos szakmai színvonalát,
- figyelemmel kell lenni nemzetközi kapcsolatainkra és kötelezettségvállalásainkra is.

[6] Lásd: [1] szakirodalmi hivatkozás III. Fejezet d) pontjában p. 12.

[7] Itt arra gondolok, hogy az önkormányzatokhoz nagyon sok különféle funkció telepített (egészségügyi, közlekedésigazgatási, építésügyi, oktatási, környezetvédelmi, jogi, katasztrófaigazgatási, közgazdasági, stb.), amely más-más szakmai képzettséget igényel.

[8] Lásd bővebben: A települések polgári védelmi besorolásának szabályairól és védelmi követelményekről szóló 114/1995 (IX.27) Korm. sz. rendeletet
http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500114.KOR
Letöltés: 2011.05.08.

A használatos módszerek – felsorolásszerűen – az alábbiak: előadások, tájékoztatók, pályázatok, kiállítások, tankönyvek, védelmi eszközbemutató, prevenciós kiadványok, internetes anyagok, önkéntesek, CD kiadványok, média jelenlét, stb. E módszerek már nem elégségesek, nem elég hatékonyak. A felkészítést végzők nem használják ki megfelelően pl. az utóbbi 5-10 év technikai fejlődésében rejlő új lehetőségeket (ennek jogi akadályai is voltak/vannak).

Alaphelyzetben a lakosság polgári védelmi felkészítésénél legalább a következő témákat kell feldolgozni és ismertetni:

- Milyen veszélyforrások, kockázatok vannak a közvetlen lakóhelyen és a környezetben? Időbeni változások követése.
- Katasztrófatípusok, jogaink és kötelezettségeink.
- Milyen riasztási formák, jelzések vannak alkalmazásban?
- Hogyan kerülhetőek el az önmagunk által generált veszélyhelyzetek?
- Milyen helyi lehetőségek vannak a védekezésre? Segélykérési lehetőségek.
- Milyen magatartási szabályokat kell követni veszélyhelyzetben, katasztrófa bekövetkezése esetén? Elsősegély nyújtási formák.
- Milyen egyéni, illetve csoportos (helyi, távolsági) védekezési formák lehetségesek? (otthoni lehetőségek, kimenekítés, kitelepítés tervezett rendje)
- Milyen ön- és kölcsönös segélynyújtási formák ismertek?
- Melyek a helyi feladatok és -eszközök a helyreállítás folyamatában.
- Milyen szervezetek végzik a különböző feladatokat? Kik segíthetnek?
- Kapcsolattartási formák és lehetőségek (a hiteles információ szerzés forrásai).

A témakörök ismertetése (esetleges bemutatása) még vázlatszerűen is több órát igényelhet, gyakorlott előadó esetén is. Az időtartam rövidíthető szemléltető segédeszközökkel, de a tematika helyi sajátosságokkal történő bővítése viszont növelheti azt. Több megoldás egyidejű alkalmazása célszerű.

Napjaink megelőző időszaki lakossági felkészítésének gyakorlatát[9] – az elért eredmények tiszteletben tartása és a folyamatos fejlesztések (például: a legveszélyeztetebb körzetekben kiépített lakossági tájékoztatórendszer, stb.) mellett – még mindig több hiányosság és anomália is jellemzi, nevezetesen:

- Hiányzik az egységes, önálló lakosságfelkészítési szabályozás, amely mindhárom időszakra (megelőzés, védekezés, helyreállítás) adna módszertani útmutatót, s finanszírozási biztonságot nyújtana.
- Nincs kellő koordináció a felkészítésben részes különböző ágazatok, szervezetek között. Itt nemcsak a rendvédelmi szervek, hanem az önkormányzatok, a munkáltatók, a közreműködő (civil) szervezetek és a médiák szerepvállalására is gondolok.
- A felkészítés gyakorlata nem feltétlenül követi az új kockázatokat, vagy a korábbi veszélyszituációk időközbeni változásait.
- Kevés a meglévő ismeretterjesztő anyag és tartalma sokszor nem aktualizált.
- Időszakonként újra kellene definiálni a felkészítendők célcsoportjait és analizálni kellene a felkészítés szakmai tartalmát.
- Gondok vannak a logisztikai háttér működésével.

[9] Lásd bővebben: Veresné Hornyacsek Júlia: A lakosság katasztrófavédelmi felkészítésének elméleti és gyakorlati kérdései. I. kötet. Doktori (PhD) értekezés. ZMNE. Budapest,2005.- p. 46-48.

- Nem alakult ki eléggé a tanulóifjúság és a felnőtt lakosság felkészítésének metodikája, a katasztrófavédelmi ismeretek nem szerves részei az iskolarendszerű tananyagnak.
- A civil szervezetek ismerethiányosak és anyagi problémákkal is küzdenek.
- Nem mindig megfelelőek a pánikkezelési mechanizmusok és a kríziskommunikáció.
- Az elméletileg ideális állapotok és az átlagpolgár által tapasztalható valóság között nagy a különbség. A jelen állapotok egyszerű „szondázása" a következő: A véletlenszerűen megkérdezett 45 felnőtt személy (fővárosiak és nem fővárosiak, férfiak/nők, fiatalok/idősebbek.) közül nem válaszolt 6 személy. A válaszadók közül 2 fő tudott „valamit említeni" az őt körülvevő kockázatokról, nem volt elképzelésük a nem kívánt esemény bekövetkezése esetén követendő magatartásformákról, szinte senki nem vett részt sem munkahelyi, sem önkormányzati tájékoztatókon, sem gyakorlatokon az utóbbi 5-6 évben, s nem ismerte polgári védelmi jogszabályi kötelezettségeit sem. Senkinek nem volt hiányérzete, vagy belső késztetése önálló védekezési, megelőzési módszerek alkalmazására. (A felmérés nem reprezentatív, ezért az eredmény nem általánosítható a lakosság, vagy a munkavállalói állomány egészére, de a válaszoknak azért van piciny jelzésértéke.)

A fentiek ellenére azért megállapítható, hogy a megelőző időszaki lakossági felkészítés nem alapvetően elhibázott és sok területen folynak érdemi erőfeszítések a hatékonyság javítása érdekében. A jelenlegi rendszert is lehetne jobban működtetni, ha arra a folytonosság, és nem az alkalomszerűség lenne inkább jellemző. Foglalkozni kell a rendszer fejlesztésével, finanszírozásával, jogi hátterével, szakmai tartalmával és korszerűbb módszereivel. Ezt indokolja egy korábbi felmérés[10], amely szerint nagyságrendileg a „káros" események 50 %-a emberi hiba, 25%-a műszaki hiba, 10 %-a szabályozatlan kémiai/fizikai reakció, 15%-a külső tényező miatt keletkezik. Ha legalább az előforduló esetek felében lehet érdemben, értelmes dolgot tenni a megelőzési időszakban, akkor e funkciónak óriási szerepe lehet.

A kockázati kérdések és biztonsági dilemmák összefüggésben vannak a gazdasági fejlődéssel. A megoldatlan problémák gazdaságfejlesztést gátló elemmé válhatnak, más oldalról a lakosság túldimenzionált és állandósuló fenyegetettség érzése további nemkívánatos jelenségekhez vezethet. Fordítva is igaz: egy biztonságos, stabil társadalmi és gazdasági környezet pótlólagos humán erőforrásokat generálhat. A megelőző lakossági felkészítés metodikájaként tehát azt a kényes egyensúlyt kell megtalálni, amely már megfelel a jogszabályi előírásoknak és a szakmai elvárásoknak, de még elviselhető formában/ideig/tartalommal terheli a lakosságot, nem kelt látens elutasítási formákat.

GONDOLATOK A MEGELŐZŐ IDŐSZAKI LAKOSSÁGFELKÉSZÍTÉS KORSZERŰSÍTÉSÉRŐL

A kezdő lépés a célcsoportok meghatározása és a tematika, vagy az alkalmazott módszer kiválasztása. Megfelelő az a gyakorlat, amely a felkészítési célcsoportokat elsősorban felnőttekre és gyermekekre (értsd: tanuló ifjúságra) osztja fel.

A megelőző időszaki felkészítésnek több lakossági „elérhetőségi metszete" létezik, nevezetesen:

[10] Lásd a Polgári Védelem „Velünk" veszélyhelyzeti lakossági ügyfélszolgálati információs központ tájékoztató anyaga.
http://pv.battanet.hu/pv4.htm
Letöltés: 2011.05.11.

- Az egyik metszet az önkormányzati szféra: a legfontosabb szerep itt a polgármestereknek jut, hiszen ők érhetik el a helyi lakosság közel minden rétegét, s számukra hatósági jogkör is biztosított.
- A másik metszet a munkáltatói elérési oldal, amely nem rendelkezik hasonlóan erős jogosítványokkal, de itt jobb a személyes elérés esélye.
- A harmadik metszet az oktatási, pedagógusi közreműködés.
- A negyedik metszet az érintett lakossági körök, az állampolgárok önkéntes felkészülési szerepvállalása és a saját érdekből elvárható megelőzési magatartásforma követése. Ide tartozónak vélem az önkéntes- és karitatív szervezetek tevékenységét is.
- Az ötödik metszet a média és a tájékoztatás hagyományos és legkorszerűbb formáinak együttes, akár település kategórianként differenciált alkalmazása.

A felsorolt „metszetek" együttes működése esetén is nehéz biztosítani a lakosság minden rétegének, tagjának elérhetőségét felkészítési célokra, hiszen pl. a munkanélküliek, a hajléktalanok, az ismeretlen helyen tartózkodók esetében lehetnek problémák. Nyilvánvaló, hogy pl. a hazánkban hosszabb ideig tartózkodó turisták, vendégek, tulajdonosok, munkavállalók, üzletemberek megelőző felkészítése – amennyiben erre egyáltalán szükség lehet - sem gondok nélküli.

A./ Önkormányzati szféra

A felnőtt lakosság megelőző felkészítésében kulcsszerepet játszó szervezet, amelynél azonban – a sok más funkció és feladat mellett – a katasztrófa helyzetek megelőzése, vagy a megelőző időszaki felkészítés nem kap vezető prioritást. A polgármesterek felkészítésére jó példa a ZMNE Kézikönyve[11], amely útmutatást ad a lakosságfelkészítés elméletéről, gyakorlatáról.

Ha felmérésre kerülne hazánkban a háztartások katasztrófavédelmi tűrőképessége, vagy öngondoskodási hajlama, bizonyára kellemetlen eredmények születnének. Az igazi problémák meglétét (felkészületlenség, alternatív megoldások hiánya, tartalékolási gondok, ösztönszerű cselekedetek, pánik jelenségek, stb.) pedig egy-egy nem kívánatos esemény bekövetkezése tehetné igazán nyilvánvalóvá mindenki számára.[12] A családok többsége nem képes megítélni saját veszélyeztetettségét, még azt sem, hogy milyen segítséget kaphatnának számukra ismeretlen szervezetektől. Bekövetkező rendkívüli esemény alkalmával viszont minden érintett azonnal elvárná a teljes körű gondoskodást, mentést, kárelhárítást, stb., amely (legtöbbször idő hiányában és a kialakuló pánik miatt) szinte lehetetlen előzetes felkészültség és együttműködési készség nélkül. A megelőzés, védekezés, helyreállítás szempontjából kulcsfontosságú lenne a helyes lakossági magatartásforma. Fontos feladat, hogy a magyar családok kilábaljanak a katasztrófavédelmi tájékozatlanság, felkészületlenség és a téma iránti közöny veszélyes állapotából.

Az önkormányzatok egy-egy kistérség területén kísérletet tehetnének arra, hogy egy nagyobb rendezvényen gyűjtsék össze a különféle lakosságfelkészítési szervezetek képviselőit konzultációra, tapasztalatcserére.

[11] Lásd: Önkormányzati vezetők felkészítése a védelmi feladatokra. Kézikönyv polgármesterek részére a települési védelmi feladatok ellátásához. ZMNE Védelmi Igazgatási Tanszék. Budapest, 2010. ISBN:978-963-7060-76-2.

[12] A felkészületlenség nyilvánvalóvá válásához tapasztalatok szerint nem is kellenek katasztrófák, elég egy felhőszakadás, egy komoly havazás, fagy, áramszünet, vagy vízellátási fennakadás. Budapesten még egy baleset miatti többórás metrószünet is okozhat komoly fennakadást több területen.

A napokban a szokásosnál nagyobb és nemcsak helyi feltűnést keltett egy rövidhír. *„Ötven helybéli férfinak postázott polgárvédelmi behívót a sátoraljaújhelyi önkormányzat. A város védelme érdekében helyezték őket készenlétbe. A polgármester szerint egy ilyen intézkedés ugyan nem túl gyakori, de a védelmi bizottság vezetőjeként joga van hozzá. Azt szeretnék, ha árvíz idején felkészült emberek irányítanák a védekezést...Szamosvölgyi Péter, Sátoraljaújhely polgármestere elmondta: ennek nem az a lényege, hogy itt valamiféle kötelező, és parancsszerű feladatot kell végrehajtani. Ez egy jó szándékú segítségkérés…. Tavaly júniusban a felsőzsolcai árvíznél Sólyom László, akkori köztársasági elnök beszélt arról, hogy legalább a polgármestereket árvízvédelmi képzésben kellene részesíteni..Borsodban eddig 10 helyen tartottak képzést a védelmi bizottságok."*[13]. E cikkből is érződik a felkészítés tényszerű hiánya, a jogi bizonytalanság, de a helyi példamutatás és a felelősségérzet is. A polgári védelmi kötelezettség általános érvényű kötelezettséget takar, de megelőző időszaki lakosságfelkészítési szempontból szerencsésebb lenne a kötelezettségek nevesített formában történő jogszabályi megjelenítése.[14] Az általános jellegű, állampolgárra vonatkoztatott kötelezettség be nem tartásának érdemi, visszatartó erejű szankciói nincsenek, így (az előrelépés érdekében) célszerű lenne ezekre javaslatot tenni. A szankcionálás indokait, mértékét, alkalmazható típusait előzetesen széles körben meg kell vitatni, de nem felejtendő, hogy az egyik oldalon egy kötelezett személy általi jogsértés (nem teljesítés) áll szemben azzal, hogy egy valódi katasztrófahelyzetben az állam nem mondhatna le (személymentés, kárelhárítás, stb.) a kibúvókról sem. Itt tetten érhető a megelőző időszaki lakossági felkészítés egyik sajátossága, mégpedig: a tevékenység sikere azokon múlhat, akiknek egyben ez az érdeke is.

Vannak olyan országok[15], ahol a hazai célkitűzéseknél komolyabb előzetes felkészítési szisztéma van és az jól működik a gyakorlatban (pl. lakossági csomagok, gázálarcok kiosztása, földrengési veszélyek, stb.) anélkül, hogy ezt bárki zaklatásnak minősítené, vagy céljait nem venné komolyan.

Fontos a megelőző lakossági felkészítés politikamentes, tisztán szakmai jellegének megőrzése annak ellenére, hogy a civilizációs eredetű megjelenési okok között világszerte meghúzódhatnak politikai természetű szándékok is. Általában tapasztalható, hogy a felkészítési tematika jórészt a természeti eredetű okokra fókuszál, s meglehetősen elhanyagolja a civilizációs eredetű problémakezelést.

Az önkormányzat a munkaviszonyban nem lévők részére lakossági tájékoztatással, tömegkommunikációs eszközök bevonásával, kiállítások, bemutatók, versenyek szervezésével is bővítheti felkészítési eszköztárát.

B) Munkáltatói szféra

A munkáltatók[16] jelenleg nem rendelkeznek az önkormányzatokéhoz hasonló jogszabályi felhatalmazással a polgári védelem területén, de náluk sokkal nagyobb esély van az érintettek elérésére, akár gyakoribb időközökben is.

---

[13] Lásd: Behívó- készül az árvízre Sátoraljaújhely.
http://www.hirado.hu/Hirek/2011/05/12/19/Behivo__keszul_az_arvizre_Satoraljaujhely.aspx
Letöltés: 2011.05.13

[14] Bár az előző lábjegyzetben foglalt idézet kifejezetten az ár- és belvíz elleni védekezésről szól, de a törvény szerint ez sok más típusú katasztrófa esetére is alkalmazható lenne. (pl. földrengés, extrém időjárási viszonyok, vagy ipari katasztrófák elleni felkészülés).

[15] Például Japán, vagy Izrael (utóbbinál fokozottabb háborús szituáció veszélye miatt is).

[16] Itt munkáltatók kifejezés alatt értem a gazdasági társaságokat, vállalkozókat, az intézeteket, intézményeket, szövetkezeteket, társulásokat, alapítványokat, érdekképviseleteket, kamarákat, költségvetési szerveket, nemzetközi társaságokat, stb.

A munkáltatók között különbséget kell tenni azon az alapon, hogy folytatnak-e termékeikkel, szolgáltatásaikkal valamilyen közvetlen, vagy közvetett veszélyt előidéző tevékenységet. Ha igen, akkor a vonatkozó szabályok teljes szigorával kell eljárni saját munkavállalóik tekintetében és speciális, helyi ismereteiket fel kell ajánlaniuk a polgári védelmi szerveknek (azért, hogy a környék más munkáltatói is felhasználhassák a rájuk tartozó részeket felkészítési célokra). Az ún. „update" jellegű foglalkozásokat minimum évente meg kell szervezni saját munkavállalók részére, dokumentált formában. A hálózati szervezetként (több közigazgatási helységben, vagy országrészben) működő munkáltatók felsővezetőinek – a saját szervezetük által térben előidézett veszélyek ismeretében - kell dönteniük arról, hogy az adott területen állandó jelleggel foglalkoztatott munkatársaik felkészítését mely kategória szerint teljesítik.

A környezetre fenyegetést, veszélyt nem jelentő tevékenységet végző munkáltatóknál célszerű lenne bevezetni minimumként, hogy az egyébként kötelező munka- és tűzvédelmi oktatás kerüljön kiegészítésre megelőző katasztrófavédelmi felkészítéssel, dokumentált formában. A felkészítés tematikáját védelmi szakemberek határozhatnák meg és bocsátanák a munkáltatók rendelkezésére. A kockázati változások miatt az ismereteket legalább 2 naptári évenként frissíteni kell.

A távollétek egyszeri pótlására lehetőséget kell adni. Állami feladat révén a megelőző időszaki felkészítésen történő részvételt a törvényes munkaidő részének kell tekinteni, így az esetleges kibúvás, vagy távolmaradás szankcionálhatóvá válhat a munkajog eszközeivel (erre célszerű lenne kormányzati részről gyakorlati iránymutatást kiadni a munkáltatók részére).

A munkahelyi felkészítés megtörténtéről kiadott igazolás, annak dátumától számított 2 naptári évig mentesítést adhatna az érintett állampolgár számára az önkormányzat által szervezett megelőzési időszaki lakóhelyi felkészítésen történő részvétel alól, ha a munkahely és az állandó lakóhely szerinti önkormányzat illetékességi területe azonos településen, vagy annak földrajzi közelében (pl. vidéken 15, Budapest környékén 30 km-en belül) van. Ehhez szükség lenne arra, hogy a felkészítés szakmai lényegét illetően a két megoldás egyenértékű legyen.

C) Oktatási, pedagógusi szféra

A megelőző felkészítés e „metszete" pedagógusok részvételével, alapvetően a tanulóifjúság részére zajlik. A speciális didaktikai és tematikai részletek ismertetése itt nem feltétlenül szükséges, de jelezhető, hogy Veresné Hornyacsek Júlia értekezésének megfelelő fejezetében[17] foglalt javaslatok elfogadhatóak. Néhány kiegészítő (megerősítő) gondolat:

- Célszerű lenne kötelezővé tenni minden általános (felső tagozat) és középfokú oktatási intézményben, hogy a tanév megkezdésének valamely korai időszakában (pl. osztályfőnöki órán) a tanulók kidolgozott tematika szerinti tájékoztatást kapjanak katasztrófavédelmi alapismeretekből (nem távoktatásos formában). Célszerű szituációs játékok szervezése.
- A felsőoktatási intézmények, valamint az OKJ-s képzést végző intézmények vezetői is gondoskodjanak hallgatóik megelőző időszaki felkészítéséről tanulmányi évenként legalább egy alkalommal, dokumentált formában, kb. egy tanórányi időkeretben.
- az általános-, a középiskolai és felsőfokú (valamint OKJ-s képzésben) tanulmányaikat /nappali tagozaton/ folytató tanulók felkészítése csak oktatási intézményi formában történjen.

[17] Veresné Hornyacsek Júlia: A lakosság katasztrófavédelmi felkészítésének elméleti és gyakorlati kérdései. I. kötet. Doktori (PhD) értekezés. ZMNE. Budapest,2005.- 4. Fejezet. p. 75-94.

A fenti gondolatok talán megfontolhatóak lehetnek az új köz- és felsőoktatási törvénytervezet jelen cikk írásakor zajló széles körű szakmai vitájában.[18] Az ifjúság felkészítésének módszerei továbbra is lehetnek a különböző versenyek, pályázatok, táborok, hétvégi, vagy vakációs alkalmak és kiállítások.

D) Önkéntes, karitatív szféra felkészülési szerepvállalása

Az önkéntesség nagy felelősségtudatról tesz tanúbizonyságot önmagunk, családunk embertársaink védelmében. Az önkéntesek szerepe szerencsére hazánkban is több már a marginális mértéknél, de létszámbeli kisebbségük még sajnos ténykérdés.

A tájékoztatást, a racionális gondolkodásmód terjedését az egyes témákban megjelenő cikkek komolyan befolyásolhatják.[19] A különféle fenyegetések (mint a terrorizmus, a természeti katasztrófák, a fertőző betegségek, stb.) elleni felkészülés közös felelősség. Jobban fel kell készíteni családtagjainkat, szeretteinket, mert ellenállóbakká tehetjük őket kritikus pillanatok esetére is.

Az önkéntes felkészülési szerepvállalást erősíteni lehet hatósági, önkormányzati oldalról. Erre itt az egyik példa: feliratkozási lehetőség olyan internetes honlapok hírleveleire, vagy SMS küldő szolgálataira, amelyek családi felkészülésre és reagálásra adnak jól használható tippeket és útmutatásokat[20]. Tartalmilag biztosítani célszerű pl. a következőket:

- saját otthoni készlet készítése,
- családi szempontú védelmi terv összeállítása,[21]
- ismeretszerzés a saját környezet veszélyeztetettségi körülményeiről,[22]
- a segélynyújtási lehetőségek megismerése,
- tájékozottság a saját környezet hatósági, mentési szerveiről, azok elérhetőségeiről,
- felkészültség váratlan eseményekre, esetleg mások segítésére.

Bár jelentősen bővül hazánkban is az internet és a mobil penetráció/ellátottság, mégis vannak olyan földrajzi területek, vagy érintett személyek, akik nem érhetőek el ezen az úton. Részükre más megoldások is rendelkezésre állnak, de szükség lenne az ő kezdeményező együttműködésükre is. A folyamatban lévő infokommunikációs technológiai fejlesztések[23] jelentősen segíthetik az önkéntes szerepvállalási szférát, itt az igényt kell felkelteni az emberekben, majd segíteni az öngondoskodásuk kiteljesedő folyamatát.

E) Média és a tájékoztató rendszerek szerepvállalása

A média felhasználása nem új keletű, de messze nem kihasznált lehetőség. Itt elsősorban az írott sajtóra, az elektronikus híráramra, a szórólapokra, a helyi honlapokra, kábelcsatornás műsorközlésre gondolok. Sok új módszer és eljárás kidolgozása nem szükséges, a hangsúlyt a meglévő eszköztárral történő hatékonyabb üzemeltetésre, a lehetőségek teljesebb

[18] Tudomásom szerint jelenleg csak 4-5 olyan felsőoktatási intézmény üzemel, ahol tanterv szerint van katasztrófaigazgatás, vagy kritikus infrastruktúra védelem oktatás a hallgatók részére.
[19] Pl. „Mi lesz velünk egy nukleáris katasztrófa esetén?" Bihari Ádám http://www.fn.hu/belfold/20110426/mi_lesz_velunk_egy_nuklearis/; Letöltés: 2011.04.27.
[20] Lásd: Department of Homeland Security honlapja https://public.govdelivery.com/accounts/USDHS/subscriber/new?topic_id=USDHS_111; Letöltés: 2011.05.16
[21] Lásd példaként: http://www.ready.gov/america/makeaplan/index.html; Letöltés: 2011.05.16.
[22] Lásd példaként: http://www.ready.gov/america/beinformed/index.html; Letöltés: 2011.05.16.
[23] Itt kiemelten gondolok a Nemzeti Digitális Közmű (NDK) lehetőségre, amely céljai szerint közmű ellátottsági szinten tervezi megvalósítani az elektronikus, szélessávú vezetékes elérhetőséget és kommunikációt bárhol az országban.

kihasználására kell helyezni. A nagy példányszámú, vagy országos sugárzású (közszolgálati) médiák feladata lehet az általános, minden területre érvényes felkészítési anyagok terjesztése, a helyi szolgáltatók pedig a specialitásokkal kiegészített anyagot közölhetnék az érintettekkel. A megelőző lakossági felkészítés – mint állami feladat és nemzeti ügy – nem minősülhet reklámnak, így egy-egy aktuális szakmai tartalom időnkénti ingyenes sugárzása is lehetővé válhat változó idősávokban és 15-30 mp-es időtartamban, feliratozott formában is. A megjelenített hivatkozások sokszorozhatják az információs hatást. (Ismeri Ön saját környezetének veszélyforrásait, vagy veszélyhelyzeti tennivalóit? Gondolt már magára és szeretteire? Nézze meg a .. honlapot, vagy érdeklődjön … szervnél!)

A megelőző lakossági felkészítés korszerűsítése érdekében a következő pótlólagos kérdések problémák megfontolása is javasolható:

Adatvédelem

Közös érdek, hogy a felkészítés céljára minden állampolgár, de több esetben még a hazánkban tartózkodó nem magyar állampolgár is elérhető legyen. De kérdés: Vannak-e jelenleg adatvédelmi akadályai annak, hogy minden érintett állampolgárt elérjen a megelőző időszaki lakossági felkészítés valamely „metszete"? A jelenleg hatályos jogi szabályozás szerint személyes adatot csak akkor lehet felhasználni, ha az érintett kifejezetten hozzájárul, vagy ha a vonatkozó törvényi szabályozás ezt címzetten előírja. Tekintettel arra, hogy a védelem állami feladat és nemzeti ügy – az elérésnek nem lehet adatvédelmi akadálya, tehát elérendő, hogy ilyen célokra személyes adatokat is fel lehessen használni. (Tehát pl. a népesség-nyilvántartás is segítségül hívható a felkészítés során.) Az elérésnek lehetnek anonim (személyes adatfelhasználást nem igénylő) módozatai, pl. az írott sajtó, vagy elektronikus média, vagy postai úton címezetlen nyomtatvány kézbesítése mindenki számára egy-egy területen, azonban e lehetőségek nehezen dokumentálhatóak, eredményességük alig mérhető és költségigényesek. Megfontolandó: Elérhetővé kell-e tenni, hogy egyes reklámhordozókon kötelezően, vagy kampányszerűen szerepeljen lakosság felkészítési információ, vagy hivatkozás (hasonlóan a dohánytermékekhez)?

Biztosítás

A katasztrófakockázatok pénzügyi kockázatai nem teljesen feltártak, azok biztosítási kérdései legfeljebb csak részben megoldottak. E tekintetben a PSZÁF korábban megjelentett már rendkívül hasznos és probléma feltáró anyagot [12].

Az okok közül az egyik:

„A kockázat biztosíthatóságának általános feltételei ugyanis az alábbiak lehetnek:

- *nagyobb számú megfigyelési egység, hogy valószínűség számítási alapon elemezhető legyen, illetve tényleges kockázatmegosztás lehessen,*
- *homogének legyenek a kockázatok,*
- *az esetleges károk véletlenszerűek legyenek,*
- *az esetleges kár egyértelműen leírható és megbecsülhető legyen,*
- *az esetleges ügylet mindkét fél (szerződő, biztosító) számára gazdaságos legyen."*[24]

Az idézett általános biztosíthatósági feltételek közül nagyon kevés teljesíthető és tisztázatlan az a határ is, ameddig, illetve amelytől állami, vagy tulajdonosi/üzemeltetői

[24] Idézet a [12] irodalmi hivatkozásban szereplő PSZÁF anyagból p. 4.

feladatnak kell tekinteni a kockázatviselést. Szinte folyamatosan szükség lenne a biztosítási időszak alatti kockázati újrapozícionálásra. A szélsőségesen nagy kárérték előfordulási veszélyek miatt a viszontbiztosítási szerepvállalás is mérsékeltebb, ezért nagyobb figyelmet érdemel. Az állami szerepvállalásban az állam, mint a kockázatok biztosítója helyt állhat költségvetési források terhére, vagy – nem természeti okok miatti kockázatokra - szedhet ezért díjat is. Többek között erre is utalhat az a jogalkotási elképzelés is, hogy egyes esetekre és a veszélyforrást üzemeltetőkre bevezetnék a katasztrófavédelmi hozzájárulást is.[25]

KÖVETKEZTETÉSEK

Jelen cikk tartalmi mondanivalója az alábbi következtetésekben összegezhető:

Idézet a katasztrófavédelmi rendszer javítására és fejlesztésére készített koncepcióból: *„Mindenki egyetért abban, hogy a veszteségek jelentősen csökkenthetőek, ha a szakma kellően felkészült a védekezésre, a lakosság pedig kellően tájékozott és motivált a katasztrófák megelőzésében, veszélyhelyzetekben pedig a megfelelő viselkedésmódok megtartásában. A jogok, kötelezettségek, védekezési lehetőségek ismerete, a megszerzett tudás szinten tartása, begyakorlása, készségszintre fejlesztése jelenti a felkészültséget."*[26] Ez a feladat és nem is kevés.

Sok a megoldatlan, vagy jogi szabályozásra váró témakör. Koncepció szinten felmerült, hogy a hatósági jogköröket a polgármesterektől, illetve a megyei közgyűlés elnökeitől, részben, vagy egészben át kell telepíteni a katasztrófavédelemhez. Ez megváltoztatna nagyon sok elvi és gyakorlati vonatkozást, átstrukturálná a finanszírozást és a hatósági ügyintézés jó részét. Szigorítanák a megelőző időszaki felkészítés (és nemcsak e terület) szabálysértési és/vagy büntetőeljárási szabályait. Szükséges az önkéntes, karitatív szervezeteke fokozottabb bevonása a felkészítésbe. Fejleszteni kell a védelem informatikai rendszereit, bővíteni kell a finanszírozási formákat, erősíteni a logisztikai háttér-támogatottságot.

A III. fejezetben felsorolt „metszetek" szinte mindegyikében problémát jelenthet, hogy nincs meg komplex módon pl. a kritikus infrastruktúra elemek országos azonosítása.

Természetesen kiemelt helyeken van jól működő előzetes lakossági felkészítés (lásd pl. Százhalombatta, Paks, stb.). De hogyan lehet megelőző időszaki lakossági felkészítést végezni olyan helyeken, ahol még nem készültek el a komplett háttéranyagok? Egy jogszabály készítői elképzelés szerint[27] kockázatelemzést kell készíteniük a kritikus infrastruktúra üzemeltetőknek. Az erre épülő biztonsági tervben ki kell térni arra: hogyan biztosítják létesítményeik védelmét, hogyan előzik meg a működési zavarokat és mit tesznek a rendszer esetleges sérülése esetén a szolgáltatás helyreállítása érdekében. Ehhez szükséges lenne az indikátorok teljes és előzetes feltérképezése (a modellezhetőség) és a nem valószínűségi elven működő kockázatelemző módszer céltudatos alkalmazása.

Abszolút biztonság nem volt, nincs és belátható ideig nem is lesz. Minden lehetséges eseményre, vagy körülményre nem lehet felkészülni, már pl. gazdasági, finanszírozási okokból sem. Vannak természeti erők, amely ellen az emberiség mai tudásával nem lenne képes védekezni. Sajnos egyre többet lehet számítani rendkívüli, vagy extrém eseményekre, ezért a megelőző időszaki felkészítésnek a jövőben bővülő szerepet kell adni.

Minden eshetőséggel racionálisan kalkuláló megelőző lakossági felkészítési tematika, vagy módszer jelenleg érzékelhetően nem létezik. Ez egy tudományos igényességű, államilag finanszírozott kutatási projekt keretei között lenne kifejleszthető. Javasolható a döntéshozók számára, hogy embertársaink, anyagi javaink és természeti környezetünk megóvása érdekében

[25] Lásd a [1] irodalmi hivatkozás anyagában p. 21.
[26] Lásd a [1] irodalmi hivatkozás anyagában p.5.
[27] Lásd: Törvény készül a kritikus infrastruktúráról
http://www.nol.hu/belfold/20100823-torveny_keszul_a_kritikus_infrastrukturarol; Letöltés: 2011.05.16

fordítsanak erre nagyobb figyelmet és biztosítsák a kutatáshoz szükséges anyagiakat. A katasztrófavédelem területén a jogkövetést (okkal) elvárják a szakterület minden művelőjétől, ugyanakkor célszerű lenne az is, hogy jogalkotók is fokozottabban vegyék figyelembe a szakirányú kutatások tudományos eredményeit.

A megelőző időszaki lakossági felkészítés átlátható és az egyes „metszetek" között is arányos finanszírozása egy másik cikk témaköre lehet. Sajnos nem elhanyagolható a valószínűsége annak, hogy a megelőző időszaki lakossági felkészítésen történő „spórolás" valaha megbosszulhatja magát. Szakmai körökben elfogadott álláspont, hogy eredményes felkészítés esetén kb. 20-25 %-al csökkenthetőek még azon katasztrófa károk is, amelyeknek keletkezési okára nincs érdemi befolyásunk, vagy amelyek ellen nehéz érdemben védekezni. Mindent meg kell tenni időben, amíg ez nem késő.

Felhasznált irodalom

[1] Szabályozási koncepció a katasztrófavédelmi rendszer javítására és fejlesztésére. http://www.kormany.hu/download/8/e0/00000/Katasztrofavedelmi_koncepcio_20101116_vegleges_tuzv%20_2_.pdf#!DocumentBrowse; Letöltés: 2011.05.05.

[2] 2011 évi törvénytervezet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról (előterjesztés a Kormányülés előtt). http://www.kormany.hu/download/8/43/30000/katv%C3%A9d.pdf#!DocumentBrowse Letöltés: 2011.05.05.

[3] Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról. Lisszabon, 2007. december 13. 230 oldal, pp 49. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:0042:0133:HU:PDF Letöltés: 2010. május 27.

[4] Lisszaboni Szerződés az Európai Unióról szóló szerződés és az Európai Közösséget létrehozó szerződés módosításáról. Lisszabon, 2007. december 13. 230 oldal, pp 90-91. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:0042:0133:HU:PDF Letöltés: 2010. május 27.

[5] A katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény / I. fejezet, Alapvető rendelkezések, Általános szabályok 1.§. /1/-/2/ bekezdés http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99900074.TV; Letöltés: 2011.05.02

[6] A katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény / I. fejezet, Alapvető rendelkezések, Általános szabályok 2.§ /2/ bekezdés) http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99900074.TV; Letöltés: 2011.05.02

[7] A polgári védelemről szóló 1996 évi XXXVII. törvény. 2§ (1) bekezdés b) pont, illetve IV. Fejezet Polgári védelmi kötelezettség 20§-32§. http://www.otm.gov.hu/kok/inside/joganyagok/1996_XXXVII.pdf; Letöltés: 2011.05.02

[8] Veresné Hornyacsek Júlia: A lakosság katasztrófavédelmi felkészítésének elméleti és gyakorlati kérdései. I. kötet. Doktori (PhD) értekezés. ZMNE. Budapest,2005.- p. 42. http://193.224.76.4/download/konyvtar/digitgy/phd/2005/veresne_hornyacsek_julia.pdf Letöltés: 2011.05.06.

[9] Dr. Bukovics István – dr. Potóczki György: Helyzetkép a nemzetközi katasztrófavédelmi elvárások hazai teljesítéséről és továbbfejlesztési lehetőségeiről,

különös tekintettel az ENSZ, NATO és EU tagságunkra. Védelem on-line kiadvány, 2010. május.
http://www.vedelem.hu/letoltes/tanulmany/tan273.pdf; Letöltés: 2011.05.06

[10] Bukovics István: Általános katasztrófavédelmi rendszermodell koncepciója. „Klíma-21" Füzetek. 2010.61. szám. Kiadja: MTA KSZI Klímavédelmi kutatások koordinációs iroda. ISSN 1789-428X p. 167.

[11] Veresné Hornyacsek Júlia: A lakosság katasztrófavédelmi felkészítésének elméleti és gyakorlati kérdései. I. kötet. Doktori (PhD) értekezés. ZMNE. Budapest,2005.- p. 25-26.
http://193.224.76.4/download/konyvtar/digitgy/phd/2005/veresne_hornyacsek_julia.pdf Letöltés: 2011.05.06.

[12] A katasztrófakockázatok biztosításának kérdései. Nemzetközi kitekintés I. Pénzügyi Szervezetek Állami Felügyelete Budapest (2006. október 29.)
http://www.pszaf.hu/data/cms355142/A_katasztr__fa_kock__zatok_biztos__t__s__nak_k__rd__sei.pdf; Letöltés: 2011.05.16.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Schüller Attila
schuller.a@gmail.com

AZ Y GENERÁCIÓ ÉS AZ INFORMÁCIÓBIZTONSÁG

Absztrakt

Az információbiztonság egyik kulcskérdése az adatok bizalmasságának biztosítása. Tapasztalataim alapján a felhasználók sokszor nincsenek tisztában az általuk birtokolt és kezelt információk értékével, illetve nem feltételezik, hogy mások azokhoz hozzá akarnak jutni. Annak ellenére, hogy a fiatalabb generáció már az informatika világában nőtt fel, ez a korosztály sincs tisztában a digitális világ veszélyeivel. A cikk a felhasználói szokások közötti különbségeket vizsgálja az életkor függvényében.

Guarantee of confidentiality of the data is one of the key issues of the information security. The users often do not know the value of the handled information possesed by them, and they do not assume that others want to obtain them. In spite of the fact that the younger generation has already grown up in the world of informatics, this age group is not aware of the digital world's dangers either. The article examines the differences between the user habits in the respect of the age.

Kulcsszavak: *Y generáció, információbiztonság, emberi tényező ~ Y generation, information security, human factor*

BEVEZETÉS

Ahogy a biztonságtechnika egészére igaz, úgy az információbiztonság részterületére is, hogy a legnagyobb veszélyt az emberi tényező jelenti. Míg a technikai eszközök megbízhatósága egzakt módon mérhető, addig a humán erőforrás – a sokszínűsége miatt – jelentős bizonytalansági faktorként szerepel a rendszerekben.

Egy 2009-es felmérésem [1] eredménye azt mutatja, hogy az információbiztonság több kérdésében jelentős eltérések jelentkeznek a különböző korosztályok között. Részben ez az eredmény ösztönzött a cikkben ismertetni kívánt vizsgálat elvégzésére, részben pedig az a tapasztalatom, hogy a serdülőkorú fiatalok a legnagyobb természetességgel kezelik ugyan napjaink informatikai eszközeit, az esetek többségében azonban csupán kapcsolattartásra és

szórakozásra, nem pedig hasznos, értéknövelő tevékenységre. Ez az informatikai látókör beszűküléséhez vezet, így a számukra elérhető lehetőségek helyett egyre nagyobb veszélyekkel kell a jövőben szembenézniük.

Aktuális felmérésemben az úgynevezett Y generáció felhasználói szokásait mértem, akik az informatika és az Internet világának gyermekei. Arra voltam kíváncsi, hogy valóban tapasztalható-e szignifikáns eltérés a jelenleg serdülőkorú fiatalok információvédelmi szokásaiban a társadalom egészéhez viszonyítva. Mennyire különbözik a korábbi mérés átlagos eredményeitől a jelszóhasználat, az adat- és információvédelem, a közösségi oldalakon való részvétel és a személyes adatok bizalmas kezelése.

A vizsgált nemzedéknek kisebb a felelősségtudata, ezért az emberi tényező által generált kockázatok közül csak a nem szándékos károkozás témakörével foglalkozom. Ezen belül is elsősorban arra irányult az elemzésem, hogy tisztában vannak-e az általuk birtokolt információk értékével és fontosnak tartják-e az adatok bizalmasságát.

A következőkben bemutatom, hogy a társadalmon belül milyen generációkat különböztetünk meg. Ismertetem a korábbi információbiztonsággal foglalkozó felmérésem eredményét, majd összehasonlítom a kifejezetten fiatalok szokásaira irányuló vizsgálat következtetéseivel.

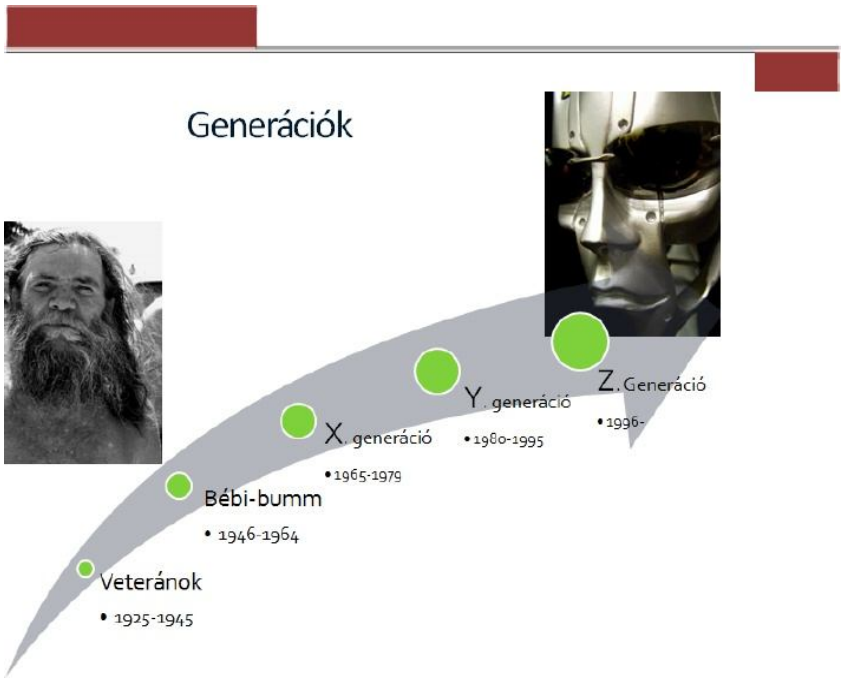
GENERÁCIÓINK

Az információs társadalom korát éljük. Ennek megfelelően a szociológia is figyelembe veszi az informatika hatásait, az Internet használati szokások alapján is differenciál. A fenti szempontok szerint öt különböző generációra osztjuk a jelenlegi társadalmat, minél fiatalabb egy nemzedék, annál nagyobb szerepet töltött/tölt be az informatika és a világháló az életében. Az Internet által biztosított szolgáltatások (World Wide Web, e-mail, azonnali üzenetküldő szolgáltatások stb.) olyan új kommunikációs csatornákat teremtettek, amelyek az emberek közötti kapcsolatok értékét is átdefiniálták.

Internet használat alapján a mai társadalom résztvevőit a következő generációkba soroljuk [2][1]:

- Veteránok: Idős korban találkoztak először az Internettel. Számukra a számítógép használat önmagában is kihívás; nehezen tudnak megbirkózni a digitális társadalom kihívásaival.
- Bébi-bumm: Életük derekán találkoztak az Internettel. A munkavégzésükbe hellyel-közzel beépült ugyan az internet használata, de nem hozott radikális változást.
- X generáció: Ez a hírnöknemzedék, az átmeneti generáció. Kamasz- és ifjúkorukban találkoztak az Internettel, munkavégzésüket alapvetően határozza meg a web. Életvitelükben hellyel-közzel van jelen az Internet. Jelenleg ők dominálják a munkaerőpiacot.
- Y generáció: Gyermekkorukban találkoztak az Internettel. Ők jelentik a digitális nemzedék első hullámát. Mostanra kezdenek megjelenni a munkaerőpiacon, komoly kihívást jelentve az X. generáció számára. Minőségileg új szintet képvisel a hírnöknemzedékhez képest.
- Z generáció: Ez a nemzedék soha nem élt olyan társadalomban, ahol nem volt Internet.

1 A különböző generációk meghatározására különböző megfogalmazások léteznek. Vannak olyanok is, amelyek nem a digitális világgal hozzák összefüggésbe a korosztálybeli különbségeket, olyan definíciót kívántam azonban bemutatni, amely jelen vizsgálatom tárgyával szoros összefüggésben van.



1. ábra. Társadalmunk különböző generációi [2]

Természetesen az 1. ábrán is bemutatott csoportokon belül találunk kivételeket, például olyan „veteránokat”, akik a fiatalokat megszégyenítő módon értenek a számítógépekhez, azokkal minőségi, értékes munkát végeznek, szemben az új nemzedékek chatelésben és a közösségi oldalakon tanúsított aktivitásában kifulladó informatikai tevékenységével. A besorolás azonban mindenképpen fontos, ha a különböző életkorú felhasználók szokásait kívánjuk elemezni.

Korunkban a tudás alapú társadalmat tekintjük az eddigi legfejlettebb társadalomnak. A tudásra és tudományra épülő, magas gyártástechnikai színvonalat képviselő információs termelési korszakban az előállított termékek és kifejlesztett szolgáltatások összetevőinek részaránya: 80 %-ban szellemi összetevő, vagyis tudás és tudományos hányad, 20 %-ban pedig anyagi és energia összetevő, vagyis hardver és hajtóerő. [3] Ezzel szemben az Y generáció tagjai a mai huszonévesek és fiatal harmincasok, az információs kor gyermekei. Világukban mélyen megváltoztak az érintkezési szokások, és átalakultak olyan hagyományos fogalmak, mint értékrend, tudás és tekintély. [4]

Látható, hogy az Y generáció a kapcsolati tőkét fontosabbnak tartja a tudásnál, és mivel a tudás alapú társadalom eme felnövekvő nemzedékre épül, komoly társadalmi veszélyhelyzet elé nézünk a közeljövőben. Aktuális felmérésem során ezért is vizsgáltam kifejezetten ezt a korosztályt.

ÁTFOGÓ ELEMZÉS

A korábbi kvantitatív felmérésem [1] során már több kérdéskör kapcsán kimutattam, hogy a különböző korosztályoknak eltérő a véleményük, felhasználói szokásuk. A válaszadók életkora nem igazodott szorosan az országos demográfiai megoszláshoz, 10,5 % volt a 21 év alattiak száma, 54,7 % a 21-40 év közöttieké, 29,1 % a 41-60 év közöttieké és 5,8 % a 60 éven felülieké. Az akkori analízisnek nem volt célja a korok szerinti differenciálás, mégis több helyen is jelentkezett olyan eredmény, amely azt mutatta, hogy célszerű ilyen aspektusból is megvizsgálni a kérdéskört. A korábbi felmérésből olyan részeredményeket mutatok be, amelyeknél látható eltérés tapasztalható a különböző életkorú felhasználók viselkedésében.

Arra a felhasználói viselkedésre vonatkozó kérdésre, hogy a dokumentumokat, iratokat jól látható helyen tartják-e, a 21 év alatti korosztály 55,6 %-a az „általában igen”-t válaszolta, 44,4 %-a pedig az „előfordul”-t (1. táblázat). A 21-40 év és 41-60 év közötti megkérdezetteknél a feleletek folyamatosan megoszlottak az öt választási lehetőség között, de közelítettek az „általában nem” felé. A 61 éven felüli korosztály válaszai voltak a legpozitívabbak, 60,0 %-uk általában nem, vagy soha nem hagy elérhető helyen iratokat a saját bevallásuk szerint.

Válasz	Korosztály (%)			
	-20	21-40	41-60	61-
mindig	0,0	13,0	7,7	20,0
általában igen	55,6	34,8	26,9	0,0
előfordul	44,4	32,6	26,9	20,0
általában nem	0,0	17,4	30,8	40,0
soha	0,0	2,2	7,7	20,0

1. táblázat. Az elérhető helyen levő iratokra vonatkozó kérdésre adott válaszok életkoronkénti eloszlása %-os arányban

Szintén jelentős, életkor szerinti megoszlást tapasztaltam a jelszóhasználat tekintetében. A 21 év alattiak közül mindenki, a 61 éven felüliek 60,0 %-a és a köztes korcsoportok több mint fele nem használ jelszót a saját számítógépén. Úgy gondolják, hogy csak ők használják az eszközt, ezért felesleges védeni, holott számtalan esetben másoknak is megengedik a géphasználatot, esetleg tudtukon kívül hozzáférhetnek vendégek a rendszerükhöz.

Válasz	Korosztály (%)			
	-20	21-40	41-60	61-
nem használ jelszót	100,0	51,1	52,0	60,0
csak induláskor kér jelszót a gép	0,0	31,9	28,0	20,0
többszörös védelmet alkalmaz	0,0	17,0	20,0	20,0

2. táblázat. A számítógép jelszóhasználatának megoszlása korosztályok szerint

A közösségi oldalak és az azokon keresztül nyilvánossá tett személyes adatokra vonatkozó kérdést emelem még ki korábbi munkámból.

A megkérdezettek mindegyike ismer közösségépítő oldalakat, 80,2 %-a tagja valamelyiknek, 17,4 %-a elvből nem regisztrál ezekre. Az elemzés során a korosztály szerinti bontást figyelemre méltónak tartottam, különösképpen a korosztályokon belüli százalékos megoszlásokat. A 21 év alatti korosztály válaszadói kivétel nélkül tagjai valamelyik közösségépítő oldalnak. A 21-40 évesek 17,0 %-a, a 41-60 évesek 20,0 %-a, míg a 61 évestől kezdődő korosztály 40,0 %-a zárkózik el ezektől a honlapoktól. Azonban ahogy ez az adat is növekedő tendenciát mutat az életkor előrehaladtával, úgy az egyre idősebb korosztályokban egyre nagyobb arányban osztják meg minden személyes adatukat a válaszadók. Azok, akik tagok, de személyes adataikat nem hozzák nyilvánosságra, inkább a fiatalok köréből kerülnek ki, a következő korosztályoknál fokozatosan csökken ez az arány.

Válasz	Korosztály szerint (%)			
	-20	21-40	41-60	61-
elvből nem regisztrál	0,0	17,0	20,0	40,0
nem tag, de még lehet	0,0	0,0	8,0	0,0
tag, de személyes adatok nélkül	66,7	48,9	24,0	0,0
minden adat publikus	33,3	34,0	48,0	60,0
nem ismeri a közösségépítő oldalakat	0,0	0,0	0,0	0,0

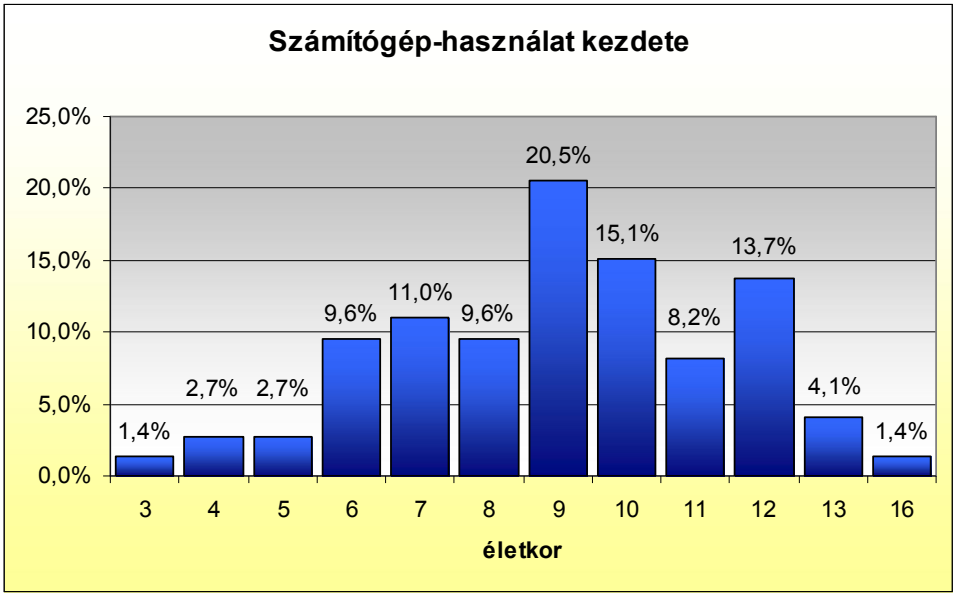
3. táblázat. A közösségépítő oldalakon való részvétel korosztályon belüli százalékos megoszlása

Az eredmények azt mutatták, hogy az emberi tényező által jelentett kockázat elemzésekor az életkornak kiemelt szerepet kell tulajdonítani. A fiatalabb nemzedék tagjaiban jobban kell tudatosítani az információvédelem jelentősségét és az ahhoz szükséges rezsimintézkedések betartásának, végrehajtásának fontosságát. A pontosabb felmérés érdekében kifejezetten a 20 év alatti korcsoport elemzésével folytattam a vizsgálatokat.

AZ Y GENERÁCIÓ ELEMZÉSE

Az Y generáció felhasználói szokásai elemzéséhez 16-19 év közötti középiskolás diákokkal töltettem ki kérdőívet. A korlátozott terjedelem miatt a beérkezett adatoknak és azok analízisének csak egy részét ismertetem.[2]

Mivel a tanulók anyagi lehetőségei meglehetősen nagy szórást mutatnak, így van, akinek már születésétől fogva van otthon számítógépe (a vizsgált sokaság 11,0 %-ának), de a megkérdezettek 2,7 %-a csak 17 éves korukban jutott hozzá saját eszközhöz. Átlagosan 8,3 éves koruk óta rendelkeznek számítógéppel (szórás: 4,1 év) és 9,1 éves koruk óta kezelik[3] (szórás: 2,5 év). A megkérdezett tanulók 3-16 éves korukban kezdték a számítógép-használatot, ennek megoszlását mutatja a 2. ábra.



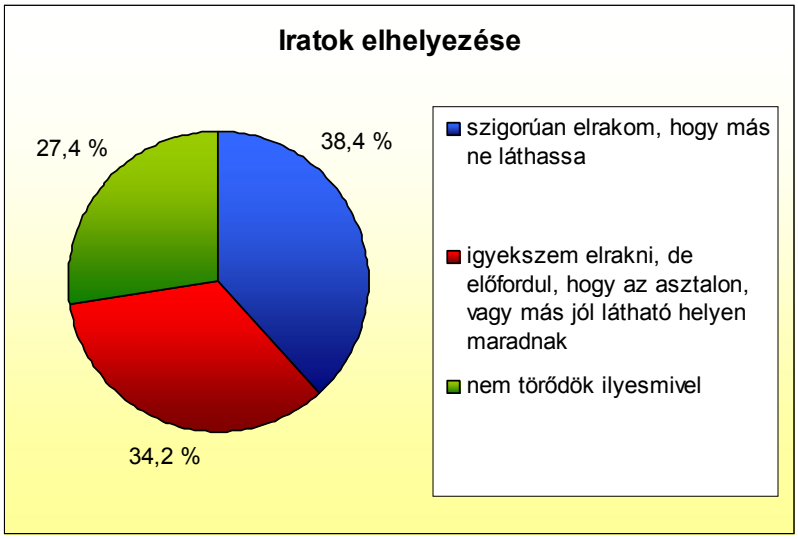
2. ábra. A megkérdezettek életkora a számítógép-használatuk kezdetekor

Meglehetősen szórt az eredmény, de igazolja az Y generáció meghatározásának azt a részét, hogy a vizsgált korcsoport gyermekkora során informatikai felhasználóvá válik.

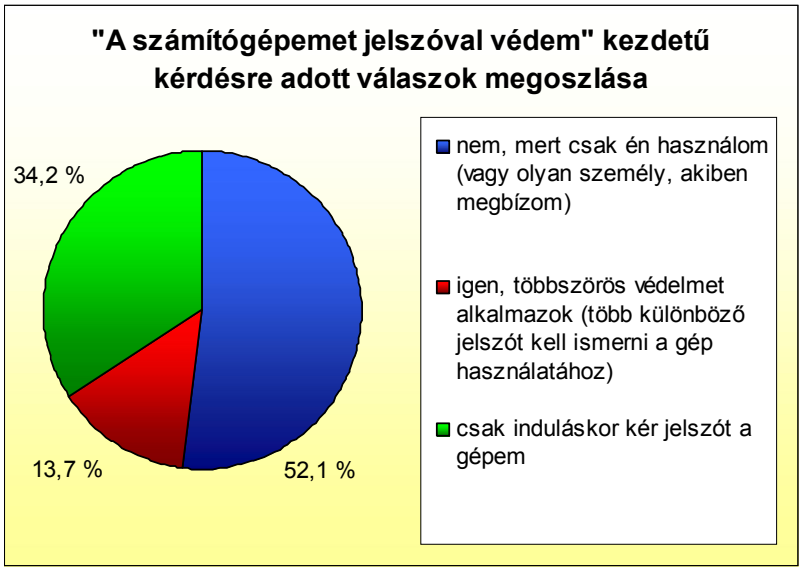
A tiszta asztal politika ismeretére és betartására vonatkozó kérdés abszolút megosztotta a vizsgált személyeket. Körülbelül harmad-harmad arányban figyelnek rá, nagyjából alkalmazzák vagy nem törődnek vele. A megoszlás pontos arányszámai a 3. ábrán láthatóak.

[2] A kvantitatív elemzéshez egy 16 kérdésből (4 kérdéskörből) álló kérdőívet készítettem. Az egyszerű és a többszörös választás esetében a lehetséges feleletekhez – annak megfelelően, hogy mennyire közelít az információbiztonság szempontjából elvárt viselkedés felé - értékeket rendeltem, így azok megoszlása mellett egyszerű módon tudtam további statisztikai következtetéseket leszűrni.

[3] A számítógép-használatnál az iskolai foglalkozásokat is bele kellett érteniük a válaszadóknak.



3. ábra. Az iratok elhelyezésére vonatkozó válaszok megoszlása



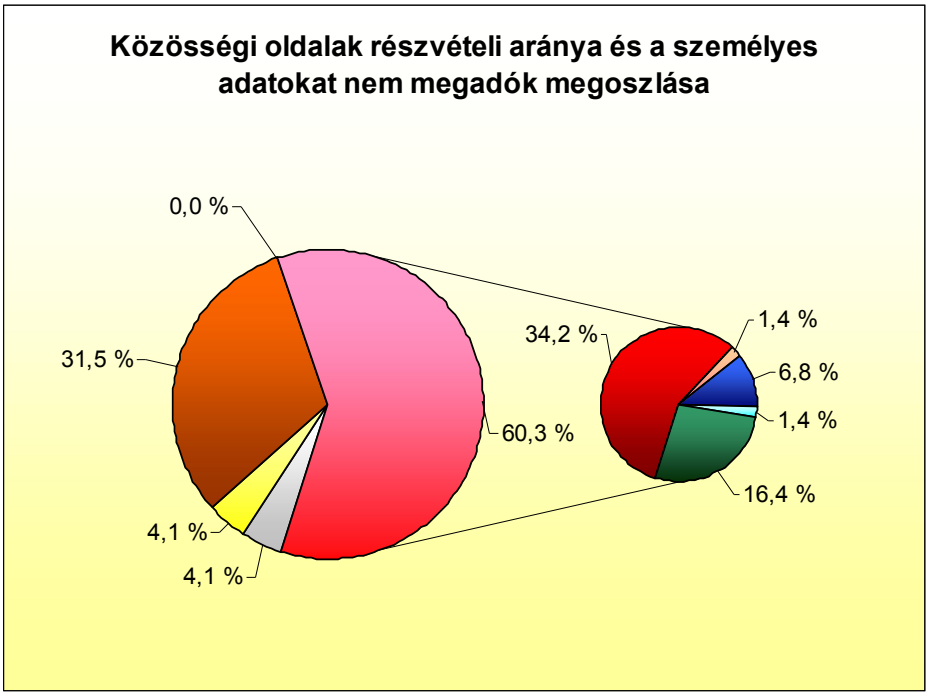
4. ábra. „A számítógépemet jelszóval védem” kezdetű kérdésre adott válaszok megoszlása

Mindkét felmérés során voltak olyan válaszadók, akik a számítógépüket zárolják, ha rövid időre magára hagyják, ellenben nem alkalmaznak jelszavas védelmet. Ők vagy nem ismerik a zárolás jelentését[4], vagy hamis biztonságérzetük van a funkcióval kapcsolatban. Ha a fiatal korosztály mérésénél ezeket a válaszokat aggregáljuk azokkal a feleletekkel, ahol a megkérdezett felhasználók a rövid időre magára hagyott számítógépen semmifajta védelmet nem aktiválnak, akkor azt kapjuk, hogy 65,8 %-uk gépéhez gondtalanul hozzáférhetnek illetéktelen személyek.

A 16-19 év közötti felhasználók elenyésző hányada nem szerepel közösségi oldalakon. Minden személyes adatát megadja a megkérdezettek 31,5 %-a, míg a 60,3 %-a azt állítja, hogy személyes adatot nem ad meg. Részben a kérdőívek kitöltése során jelezték, részben pedig tapasztalat, hogy ezeket az adatokat szerepeltetik, de úgy jelölik be, hogy csak ismerősök láthassák. Ez szintén hamis biztonság érzetét kelti, hiszen egy másik kérdésből

[4] A lehetséges válaszok között szerepelt a „nem értem a kérdést” opció, de ezt csupán egyben jelölték meg a 159 adatközlésből.

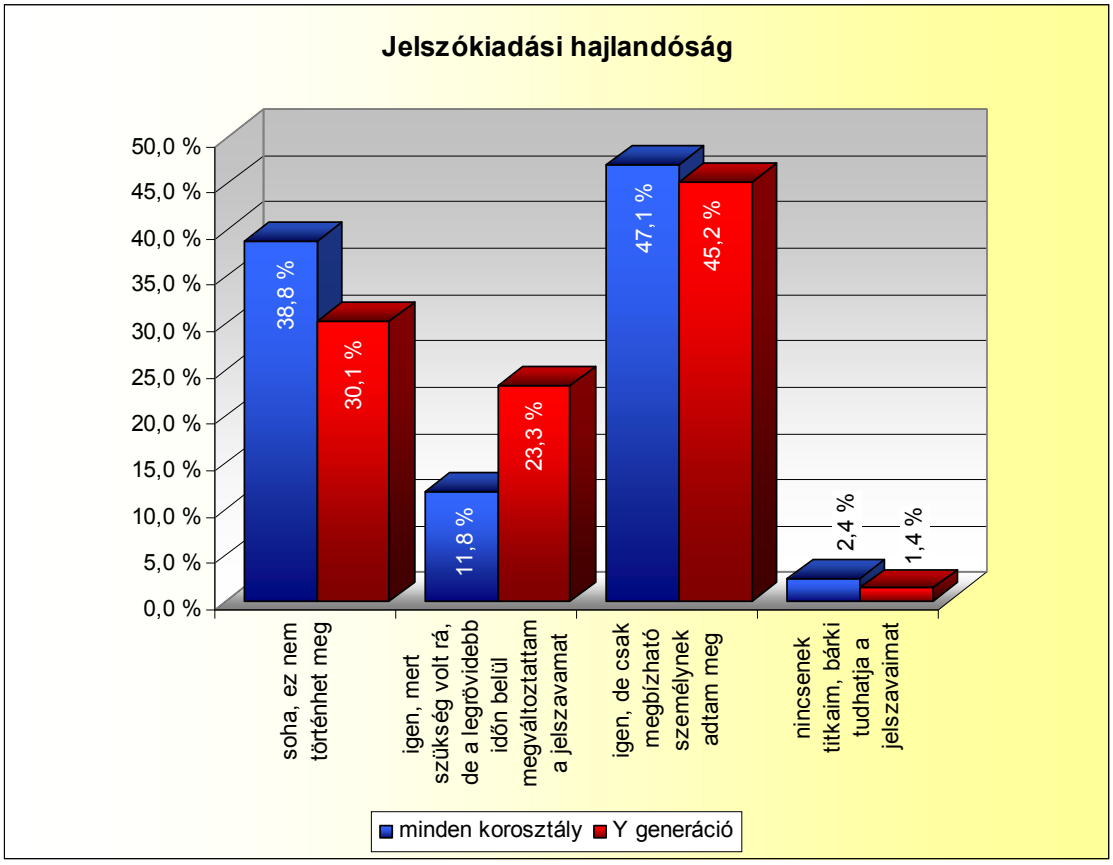
kiderül, hogy a fiatalok 42,5 %-a visszaigazolja azokat, akiket ismer (akkor is, ha hamis a profil), 32,9 %-uk azokat az ismeretleneket is, akikkel van közös ismerősük, 5,5 %-uk pedig mindenkit, akár ismeretlen személyeket is. Csupán 4,1 % válaszolta azt, hogy senkit nem igazol vissza, 8,2 % megválogatja, hogy melyik ismerőst fogadja el, 4,1 % pedig személyesen, telefonon, vagy egyéb módon egyezteti, hogy valóban az igazi személy kereste-e meg. Az 5. ábrán a személyes adatokat nem megadó csoportot továbbontva látható, hogy ezen belül milyen módon oszlanak meg a visszaigazolási módok. Az összsokaság 34,2 %-a csak ismerősöket jelöl be, 16,4 %-a idegeneket is, ha van közös ismerős, 6,8 %-a az ismerőseinek csak egy részét hajlandó visszaigazolni, 1,4-1,4 %-a pedig vagy megbizonyosodik a jelölő személyazonosságáról, vagy fenntartások nélkül még ismeretlent is megjelöl. Ezen csoportok alkotják a 60,3 %-os halmazt, melyben a felhasználók nem adnak meg személyes adatot – vagy legalábbis nem tudnak róla.



5. ábra. A közösségi oldalak részvételi aránya, a személyes adatokat nem megadó személyek további bontásával

Amennyiben valaki a személyes adatait úgy adja meg egy közösségi oldalon, hogy csak az ismerősei láthassák, viszont nem kellő gonddal választja meg, hogy kit fogad el ismerősének, gyakorlatilag bárki számára hozzáférhetővé teszi a bizalmasnak vélt adatait. Sokan azonban nincsenek tisztában a személyes adat fogalmával sem, így nem is sejtik, hogy egyszerű regisztrációs kérdések válaszolásával milyen visszaéléseknek teszik ki magukat.

Érdemes még kiemelni a jelszókiadási hajlandóságot. A 6. ábrán a két felmérés adatai láthatók, a kék oszlopok a korosztályok figyelembe vétele nélküli mérés, a piros oszlopok a 16-19 évesek felhasználói szokásaira vonatkozó mérés százalékos megoszlásait mutatja. A két eredmény nem tér el szignifikánsan, aggasztó viszont, hogy életkortól függetlenül a felhasználók kétharmada – 61,2 %-a, az Y generáció tagjainak pedig 69,9 %-a – kiadja a jelszavait mások számára.



6. ábra. Jelszókiadási hajlandóság összehasonlítása az Y generáció és a többi korosztály között

ÖSSZEGZÉS

A két felmérés összehasonlításának eredményeképp megállapítható, hogy bizonyos területeken a fiatalabb generáció kevésbé tart fontosnak adat- és információvédelmi szempontokat. Az idősebb korosztály tagjainál is – ha kisebb mértékben is – tapasztalható volt a biztonságos számítógép-használat hiánya, de véleményem szerint ez a csoport az élet más területein már megtapasztalt negatív hatások és a hozzájuk eljutott tájékoztatások miatt óvatosabb. Ez mutatkozott meg például a tiszta asztal politikára vonatkozó pontnál – ahol az volt a kérdés, hogy az iratokat, dokumentumokat jól látható helyen tartják-e – az idősebbek válaszai jobban közelítettek a biztonságos megoldáshoz.

Számos médiumból tájékozódhatunk a helyes jelszóhasználattal, biztonságos internetezéssel, adat- és információvédelemmel, mégis ezekben a témakörökben nagymértékű ismerethiány tapasztalható. Sajnos, akik tisztában vannak azzal, hogy miként kell eljárni a fentiekben, sokszor hanyagságból nem tartják be az előírásokat, javaslatokat.

Az Internet hatása is érezhető a meggondolatlan adatkezelés kapcsán, mivel a virtuális térben az emberek könnyebben kiadnak személyes adatokat idegeneknek, mint például ha az utcán menne oda valaki hozzájuk. A vizsgálat során azt is felmértem, hogy nyilvános helyen történő telefonbeszélgetés során a megkérdezettek 86,3 %-a odafigyel arra, hogy más ne halhassa a beszélgetésüket, 9,6 %-a általában nem és csak 4,1 %-a nem törődik azzal, hogy ki lesz társalgásának fültanúja. Látható, hogy szignifikáns eltérés tapasztalható a valós és virtuális világban történő kommunikáció védelme között. A személyes kontaktus hiánya csökkenti az óvatosságot, egyszerűbbé és gátlásoktól mentessé teszi a kapcsolatteremtést, ezek kihasználásával információt lehet kicsalni a gyanútlan személyekből.

Meglepőnek találtam, hogy annak ellenére, hogy a vizsgált személyek már gyermekkoruk óta használnak számítógépet, sokuk – az összsokaság 13,7 %-a – nincs tisztában azzal, hogy jelszavas védelem nélkül zárolt gépéhez bárki illetéktelenül hozzáférhet. Egybevetve a 16,4 %-kal, akik a rövid időre magára hagyott gépet kikapcsolják, a fiatal válaszadók mintegy 30,1 %-a valószínűleg nem tudja, hogy a zárolás funkció hogyan működik, mire használható és mikor érdemes, szükséges alkalmazni. Személyes tapasztalatokkal kiegészítve a fenti megállapításokat az Y generáció tagjai annak ellenére, hogy gyermekkoruk óta használnak informatikai eszközöket, csupán egy nagyon szűk, szórakozásra, időtöltésre alkalmas felhasználási módját ismerik.

További következtetések levonására érdemesnek találom a témakör kvalitatív módszerekkel történő tanulmányozását, amely kérdéseinek összeállításához szintén segítséget nyújthatnak az ismertetett felmérések eredményei.

Felhasznált irodalom

[1] Schüller Attila: Az emberi tényező az információbiztonság területén. Szakdolgozat. BMF, Budapest, 2009.

[2] Kulcsár Zsolt: Az integratív e-learning felé. E-book, 2008. http://www.crescendo.hu/konyvek/integrativ-e-learning Letöltés ideje: 2011. június 7.

[3] Dr. Kovács László (szerkesztő): Számítógép-hálózati hadviselés: Veszélyek és a védelem lehetséges megoldásai magyarországon. Tanulmány. ZMNE, Budapest, 2010.

[4] Tari Annamária: Y generáció. Jaffa Kiadó, Budapest, 2010.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Török Szilárd
torok.szilard@gmail.com

SOME ASPECTS OF CYBER ATTACKS IN 2011

Absztrakt

Az elmúlt évek publikus informatikai biztonsági incidensei alapján a támadások mértéke, technológiai háttere jelentős átalakuláson esett át. A célzott, precízen előkészített támadások kerültek előtérbe, az okozott kár vagy a lehetséges veszteség mértéke többszörösére emelkedett. Jelen publikáció célja, hogy bemutassa a 2011 első félévében történt jelentősebb információbiztonsági eseményeken keresztül a biztonsági fenyegetések technológiai változását, ismertesse a támadások jellegét és hátterét, rávilágítson a célzott hacker és a hacktivista támadások közötti különbségre, majd ezekből kiindulva szakmai tanulságok levonásával összegezze a lehetséges, jövőben alkalmazható biztonsági megoldásokat.

Based on the public IT security incidents of the past few years the extents of the attacks and the technological background have gone through an immense change. The targeted, precisely prepared attacks gained ground, and the extent of the caused damage and possible loss has multiplied. The goal of this publication is to present and demonstrate the technological changes of IT security, the background and characteristics of attacks, and to highlight the differences between targeted hacking and hacktivist attacks through the significant IT security events taken place in the first term of 2011. These events will serve as a tool to summarize professional conclusions concerning possible future security solutions.

Kulcsszavak: *token hitelesítés, APT, böngésző tanúsítvány, hacktivista, social engineering, korai észlelés, nulladik nap kihasználása ~ token authentication, APT, browser certificate, hacktivist, social engineering, early detection, zero day exploit*

INTRODUCTION

In the first term of 2011 the world encountered such cyber-attacks that have never taken place before. In an organizational and technological sense such a background could be observed which unambiguously demonstrated that organized crime, or the support of certain states supposedly provide a solid background through the media to the people and groups called hackers.

Previously isolated attacks could be observed, through which the method of the attacks could be detected more easily, and the extent of caused damages was significantly lower.

On the contrary, the tendencies of the past 1-2 years demonstrate that throughout the selection of the targets the hacker obviously intended to acquire great volume of financial or informational value. Their tools include self-developed codes to which the IT security systems of organizations do not provide sufficient protection.

Throughout the setup of the attack the human and application level factors are used contrary to the previously typical network and operational system level errors. The goal of this study is to present those IT security abuses which had the greatest impacts, the attack methods used throughout these abuses, to analyze the steps taken for protection and its deficiencies, and draw conclusions.

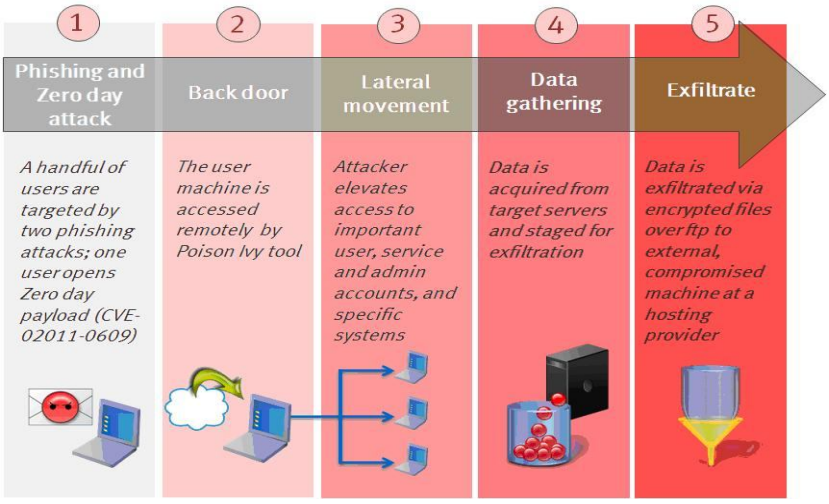
REVIEW OF ATTACKS

EMC/RSA token

The first significant attack took place against the RSA division of EMC. One of the most important products of this company is the synch and a-synch token which supports two-factor authentication. This product is used worldwide with maximum confidence. The goal of token usage is to eliminate weaknesses of passwords.

Supposedly the intruder intended to acquire the so-called "seeds" used on the tokens. In case of acquiring these seeds the secrets used throughout the token authentications become decipherable. [1] The success of the attack was acknowledged by the company at the end of March 2011 and communicated toward its clients „this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." [2]

The essence of the methodological process of the attack is demonstrated in the following graphic:



1. figure. (Source: blogs.rsa.com)

EMC as a security company pays significant attention to its protection solutions, inspite of this it became a victim of a targeted attack. This called the attention of the IT field to the fact that expectedly aligned IT attacks can take place on significant targets.

Comodo authentication provider

Simultaneously the abuse on the system of an authentication provider called Comodo transpired. It turned out that such signature certificates can be generated in the system without authority which are accepted as authentic by significant operation systems and browsers. [3]

The real danger in this is that even a mischievous code can be sent to the user's computer and neither of the protection functions of the operation system alarms to it, since it considers it authentic. [4]

These acquired sets of information made it possible for the authentication process to be compromised throughout the target attack.

APT Attacks

The RSA referred to the fact in its announcement that it became a victim of a so-called Advanced Persistent Threat – APT. Throughout an APT a group potentially backed by state support launches a targeted attack against a significant target which generally has proper IT protection. The goal of the attack is to acquire information that represents directly or indirectly significant value to the group or to the organization behind them. The APT attacks include a wide range of extremely developed and precisely prepared IT penetration techniques and technologies, telephone and satellite surveillance methods. [5]

The acquired information was presumably used throughout internet espionage as the security incidents that can be related to some armaments industry firms in the USA and the affected IT systems of Lockheed Martin, L-3 and Northrop Grumman suggest. [6]

There is no exact information on the leaked data, just as well the method of the attacks is unknown, however according to some press and media organizations it can be linked to the attacks made on the systems of RSA and Comodo.

Sony PlayStationsystems

In this period the press also dealt a lot with the security incidents related to Sony networks which were made public continuously from April until June 2011, and it affected different types of systems. [7]

The series of attacks was directly prevented by the legal measures against George Hotz (geohot) who broke into the security system of Playstation 3 produced by Sony. This hack made it possible – after long years of useless efforts – that anybody after updating the special firmware of the system, copied game DVD-s could be used on the console. The series of attacks cannot be directly linked to this man, but the Anonymous group supported him during the trial, and later explicitly took responsibility for certain cyber-attacks against Sony. [8]

These apparently do not belong to the category of APT attacks. This can be based on the fact that the attacks were based on the weak IT security system of the firm, no special professional APT typical preparation was required, and based on the announcements and publications of the past few months the acquired information was not used, furthermore this information is not suitable for APT usage. Moreover apparently this could be a hacker activity.

Carbon-dioxide quota systems

In the first half of 2011 a series of abuses regarding carbon-dioxide quota trading in the EU were revealed. It was typical of the attacks that the quota trading systems were hit by targeted and organized attacks.

[10] Most of the abuses took place in 2010 and Austria, Denmark, Poland and Estonia were affected. 38 million dollars worth of carbon-dioxide quota was stolen from the Checz dealer. Throughout the attacks with the help of a keylogger that was sent to the operator administrator's computer, took over control of the trading system, and approximately during a 4 hour bomb alarm the illegal transactions were carried out. In December 2010 Denmark got wind warded by couple of billion dollars with a similar APT attack.

THE METHOD OF APT ATTACKS

An APT attack typically has 3 main phases

- *social engineering, spear phishing:* The main difference is in the well-organized social engineering type attack during the first phase compared to the hacker attacks used previously. A targeted, confidential person is chosen as a victim, whom they send a targeted mischievous code in a personal e-mail, which exploits the earlier unknown deficiency of a widely used boxed product. It is almost impossible to set up a protection against such an attack. This method is called spear phishing, targeted data exploration. [11]
- *zero day exploit:* The second phase is that through the running of the embedded - typically zero day – exploit, taking over control of the target's computer. Zero day exploit in many cases is based on the exploitation of a weeks or months long default, however the exploited default is not published, possibly the solution itself is not publicly available. In this case the exploit as a matter of fact is a backdoor program which enables remote access and control for the hacker through legally used firewall ports.
    - *staging attack–advancing to other systems within network:* The third phase of the attack is riskier for the hacker, since he has to occupy and attack other computers (possibly servers) through the occupied computer and within the internal network. However, based on the well prepared first phase (social engineering) the hacker might have the necessary information, thus knows the accessibilities, designations of the final, real target systems, since the acquisition of these through the used backdoor program is not necessarily a complicated hacking process.

      In case the hacker does not have sufficient information in order to advance within the internal network, and does not get busted within a short time for example by log analysing, DLP or other security systems, then he can deal with the third phase for a long time. It is typical of the internal security settings of the IT systems that they are more open to the internal usage and entrance, thus a well-chosentarget person's computer can be a guarantee for success. [12]

SUMMARY

Based on the attacks, abuses presented in the first chapter two attack types can be distinguished:

- APT hacker attacks
- hacktivism

The prevention of APT attacks is currently almost impossible due to the fact that it targets internal confidential people and due to the exploits which are specifically made for these attacks. The current preventive security systems are typically not suitable for beating off such attacks quickly and efficiently. Instead early detection needs to be emphasized, this can result in real solution.

The security of application development, the security elements of the applied development method, IT security courses in higher education can be the guarantee elements in decreasing the risks of such attacks.

The development of security awareness of IT operators, developers and users has to be the basic element of defence against social engineering and spear phishing, moreover the internet self-examination of companies, meaning what is available about them on the internet, what can be found by a simpler search on social websites about their IT systems and employees.

REFERENCES

[1] Art Coviello: Open Letter to RSA Customers, In: RSA website, (22 Mar.2011); http://www.rsa.com/node.aspx?id=3872

[2] Comodohacker: A message from Comodo Hacker, In: Pastebin, (26 Mar.2011), http://pastebin.com/74KXCaEZ

[3] DeclanMcCullagh: Comodo hack may reshape browser security, CNET, (04 Apr 2011), http://news.cnet.com/8301-31921_3-20050255-281.html

[4] Advanced Persistent Threat (13 May 2011), In: Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Advanced_Persistent_Threat (http://en.wikipedia.org/w/index.php?title=Advanced_Persistent_Threat&oldid=428898501)

[5] Kevin Poulsen: Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks(31 May 2011), In: Wired, http://www.wired.com/threatlevel/2011/05/l-3/

[6] PlayStation Network outage, In: Wikipedia, The Free Encyclopedia, downloaded: 20 Jun 2011, http://en.wikipedia.org/wiki/PlayStation_Network_outage (http://en.wikipedia.org/w/index.php?title=PlayStation_Network_outage&oldid=434632625)

[7] George Hotz Bibliographic in Wikipedia, The Free Encyclopedia, downloaded:20 Jun 2011, http://en.wikipedia.org/wiki/George_Hotz http://en.wikipedia.org/w/index.php?title=George_Hotz&oldid=437166342

[8] Anonymous Operation Sony in Wikipedia, The Free Encyclopedia, downloaded: 21 Jun 2011
http://www.youtube.com/watch?v=IpfK7ADqL1Q (21 Apr 2011)
http://en.wikipedia.org/wiki/Anonymous_%28group%29#Operation_Sony
(http://en.wikipedia.org/w/index.php?title=Anonymous_(group)&oldid=438148872)

[9] James Kanter: Emission Permits Theft Estimated at $37.7 Million (20 Jan 2011),In: The New York Times, downloaded: 20 Jun 2011
http://www.nytimes.com/2011/01/21/business/global/21carbon.html

[10] Uri Rivner: Anatomy of an Attack (01 Apr 211), In: Speaking and Security: The RSA blog and podcast, downloaded: 20 Jun 2011,
http://blogs.rsa.com/rivner/anatomy-of-an-attack/

[11] Microsoft: “What is spear phishing?”, In: Microsoft, downloaded: 20 Jun 2011
http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx

[12] PánczélZoltán and Buherátor: “Betörés megrendelésre” – Ordered Hacking, Silent Signal Ltd., Ethical Hacking Conference (12 May 2011)
http://tv.computerworld.hu/video/ethical-hacking-20114-betores-megrendelesre-8211-buherator-es-panczel-zoltan

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Prekup Zsolt
prekupz@szabolcs.police.hu

A RENDŐRSÉG SZOLGÁLATI MAROKLŐFEGYVEREINEK RENDSZERESÍTÉSI ELJÁRÁSÁNAK FELÜLVIZSGÁLATÁRÓL

Absztrakt

A rendőri tevékenység szolgáltató jellegének erősítése és az EU célkitűzései érdekében kiemelten szükséges foglalkozni a rendőri munka minőségének fejlesztésével, valamint az állampolgári és társadalmi igényeknek való megfeleléssel. Ez nemcsak a szakmai tudás gyarapítását jelentheti, hanem a Magyar Köztársaság Rendőrségéről szóló 1994. évi XXXIV. törvényben meghatározott kényszerítő eszközök minőségi javulását is. Az elmúlt időszak eseményei időszerűvé teszik, a Rendőrségnél meglévő szolgálati maroklőfegyverek és az esetlegesen újonnan rendszerbe kerülő lőfegyverek rendszeresítési eljárásának felülvizsgálatát is.

To intensify the supplier character of police work, and because of the aims of the Europian Union, it is very important to deal with innovating the quality of police work. We have to deal with matching the claims of citizens and society. If quality gets better, it means, that not only proffessional knowlege gets better, but also the quality of compeeling instruments, which are determined in the 1994/24 Act about Police of Hungarian Republic. The events of last periods show that it is very important to supervise the ordering method of existing and future manual guns of duty.

Kulcsszavak: *rendőrség, szolgálati lőfegyver, összehasonlítás ~ police, guns of duty, comparison,*

VÁLTOZÁSOK

Minden fegyveres erő, fegyveres testület életében mérföldkőnek számít, ha egy új eszköz rendszeresítésre kerül. Különösen így van ez, ha ez az eszköz, egy új szolgálati lőfegyver. A szolgálati lőfegyverek kiemelt szerepet kapnak, hiszen ezen eszközön mások, vagy éppen használójának saját élete is múlhat. Éppen ezért a rendszerbe állítást igen szigorú követelményeket támasztó vizsgálatok, eljárási módok előzték, előzik meg. Az elmúlt több mint egy évtizedben azonban több olyan változás következett be, amely alapján időszerű lenne a rendszeresítési eljárások felülvizsgálata.

1999. március 12-én NATO tagország, 2004. május 01.-tól hazánk az Európai Unió tagja. Ezen két tagsággal együtt, álláspontom szerint, olyan jogosultságokat is szereztünk, amely az esetlegesen lefolytatandó rendszeresítési eljárásoknál is előnyt jelenthet.

A NATO tagsággal lehetőségünk nyílt a STANAG előírások átvételére és alkalmazására, amelynek során természetesen figyelemmel kell lennünk lehetőségeinkre. A fegyverzet technika területén ilyen például a STANAG 4172 az 5,56x45 NATO lőszer vagy a STANAG 4090, amely a 9mm Parabellum lőszer egységesítéséről szól.

Az Európai Unió tagjainak lehetősége van átvenni más országok szabványait és ez igaz a lőfegyverek szabványaira is. Több ország, köszönhetően jobb anyagi lehetőségeinek már a lőfegyverek, lőszerek szabványosításának területén is előttünk járnak. A legjobb példa erre vonatkozólag Németország. A német példa honosítása nem ismeretlen Magyarországon, hiszen a lőfegyverek megszerzéséről és tartásáról szóló jogszabályok (2004. évi XXIV. törvény, 253/2004 Kormányrendelet, 49/2004 BM rendelet, 50/2004 BM rendelet) is a fenti ország jogszabályain alapul.

Németországban a 9x19 Parabellum kaliberű rendőrségi szolgálati lőfegyverekre a Polizeitechnisches Institut (PTI) dolgozta ki, amely a Deutsche Hochschule der Polizei (D*hPOL – Rendőrtiszti Főiskola német megfelelője*) műszaki intézete.[1] A PTI támogatja és tanácsokkal látja el a szövetségi és tartományi rendőrségeket, professzionális szinten tesz technikai észrevételeket és alakítja ki véleményét, mind a technikai és taktikai követelmények területén. PTI jelenleg a világ 27 országában működik együtt hasonló szervezetekkel. A jelenleg érvényben lévő rendőrségi szolgálati lőfegyverekre vonatkozó követelményrendszere 2008 januárjában készült el és 2008. február 06-án közölték. Az elvárási rendszer minőségére jellemző, hogy több ország is elfogadja tanúsítványát vagy saját rendszerük kidolgozásának alapját képzi.

RENDŐRSÉGI RENDSZERESÍTÉS KÖVETELMÉNYEI ÉS SZABÁLYAI

A jelenleg érvényben lévő jogszabályok[2], illetve belső normák pontosan[3] meghatározzák a szolgálati lőfegyverek rendszeresítésének eljárási menetét, annak megindításától kezdve, a határozat meghozataláig bezárólag.

A Rendőrség által alkalmazott kényszerítő eszközök rendszeresítésének szakmai követelményeit és eljárási szabályait a 384/2007. (XII. 23.)[4] Kormányrendelet határozza meg. Az említett jogi norma **3**. §-a meghatározza, hogy a rendőrség rendszerébe kényszerítő eszköz - így a szolgálati lőfegyver - rendszeresítési eljárás lefolytatását követően kerülhet.

Az 5. § (1) szerint a rendszeresítendő lőfegyvernek meg kell felelnie a használatával összefüggő általános és speciális jogszabályi előírásoknak, továbbá a korábban rendszeresített

[1] Vass Gábor : Achtung ! Polizei ! c. cikk Kaliber Magazin 2011 márciusi szám – 2011 március 12 állapot
[2] 2003. évi CXXIX. Tv. a közbeszerzésekről
[3] 18/2002 BM Utasítás BM Technikai Szabályzatáról
[4] 384/2007. (XII. 23.) Kormányrendelet a Rendőrség által alkalmazott kényszerítőeszközökről

kényszerítő eszközökkel, valamint a hozzájuk szükséges egyéb felszerelésekkel való együtthasználhatósági, valamint az alkalmazhatósági követelményeknek.

A szabályozás értelmezéséből kiderül, hogy szervezeti egységének vezetője[5] – a Rendőrség esetében az országos rendőrfőkapitány – kezdeményezi a rendszerbevételt, miután jelezték annak igényét.

Az országos rendőrfőkapitány, a még nem rendszeresített kényszerítő eszköz beszerzésének szükségességéről - a beszerzési eljárás megindítását megelőzően - írásban tájékoztatja a minisztert, valamint értesítést küldhet a társszervek (TEK, NVSZ) részére.

Amennyiben rendszeresítendő szolgálati lőfegyver beszerzése válik szükségessé, a rendszeresítési eljárás megindítását követően, annak lefolytatásával párhuzamosan a beszerzési eljárás lefolytatását is meg kell kezdeni. Ez a fajta szabályozás álláspontom szerint nem felel meg a költséghatékonyság alapelvének, hiszen a rendszeresítési eljárás lezártával és nem annak megindulását követően, annak végeredményétől függően kellene a beszerzési eljárást lefolytatni. Ezen beszerzési eljárás alapján megkötött szerződés hatályának beállta a szolgálati lőfegyver rendszeresítésétől vagy alkalmazásba vételétől függ és e feltételt a beszerzési eljárást megindító felhívásban is már közölni kell. Ugyanitt célszerű közölni azt is, hogy az eljárások során, nyomatékkal veszik figyelembe a következőket:

- egységesítés lehetőségét
- rendszerben tartott azonos rendeltetésű és funkciójú kényszerítő eszközök típusválasztékának csökkentésére
- rendőri szervek ugyanazon szakmai feladatokat végrehajtó állománya azonos típusú és fajtájú kényszerítő eszközzel kerüljenek ellátásra.

Az engedélyezési eljárások megállapításait, valamint a beszerzési eljárás során elvégzett vizsgálatokat, a rendszeresítési eljárás során figyelembe kell venni. A rendszeresítési eljárás megindítását követően az eljárás során szükséges szakértői feladatok ellátására, az ORFK vezetője szakértői bizottságot hoz létre. A szolgálati lőfegyver csak rendszeresítési határozattal kerülhet a Rendőrség alkalmazásába, de az meg kell előznie egy próbahasználatnak.

PRÓBAHASZNÁLAT

A próbahasználat tapasztalatairól jegyzőkönyvet kell készíteni. A próbahasználaton részvevő szolgálati lőfegyverek mennyiségét az országos rendőrfőkapitány határozza meg és szükségessége esetén a próbahasználatot végző személyi állományt annak használatára ki kell képezni.

A próbahasználat során meg kell győződni a következőkről:

- a korábban rendszeresített, illetve beszerzett felszerelésekkel való együtthasználhatóságáról *(interoperabilitás elve),*
- a gazdaságos üzemeltetésére, technikai kiszolgálására, javítására, tárolására, szállíthatóságára, kezelhetőségére vonatkozó feltételrendszer megteremtésének lehetőségeiről.
- A próbahasználatot végrehajtó rendőri szerv a kényszerítő eszköz próbahasználatát követően, az arról készült jegyzőkönyvben - indoklással együtt - az alábbi megállapításokat teheti:
  - rendőrségi alkalmazásra megfelel,
  - rendőrségi alkalmazásra a megfelelő módosítások elvégzését követően megfelel,
  - rendőrségi alkalmazásra nem felel meg.

[5] ORFK Oktatási és Kiképző központ : Rendőri szolgálati technikai ismeret

A próbahasználat mellett a minősítő, az összehasonlító és az ellenőrző vizsgálatokat el kell végezni, kivéve, ha a rendszeresíteni kívánt szolgálati lőfegyver már rendelkezik olyan tanúsítvánnyal, amelyik olyan, e tevékenység elvégzésére akkreditált, független hazai vagy más EGT-államban működő szervtől származik.

A rendszeresítés részletes szakmai protokollját a 19/2010. ORFK Utasítás írja le. Ezen utasítás megfogalmazza többek közt a szakmai bizottság összetételét, feladatait, működésének szabályait, de még azt is, hogy a rendszeresítést kezdeményező átiratnak milyen tartalmi követelményei vannak.

A fentiekből látható, hogy a rendszeresítési eljárás bonyolult és nem utolsó sorban költséges is.

PTI

Ezen eljárási rend kiváltható lenne - a próbahasználat kivételével - ha például elfogadnánk a már említett PTI által kiállított Technische Richtlinie (TR – Technikai (Műszaki) Szabályzat) elnevezésű tanúsítványát.

A TR[6] szigorára és magas követelmény szintjére néhány példa szolgálati maroklőfegyverek területéről:

- szolgálati lőfegyver élettartama legalább 10000 lövés, biztonságot vagy kezelhetőséget negatívan befolyásoló változás bekövetkezése nélkül
- 25 méter távolságból 10 lövést leadva 16 cm átmérőjű körben kell lennie
- Az elcsettenések, akadályok száma a 2 ezreléket nem haladhatja meg
- Mind a fegyvert, mind a tárat úgy kell kialakítani, hogy ne lehessen hibásan összeszerelni és balesetveszélyesen működtetni
- A következő lövés leadásához az elsütőbillentyűt legalább 4 mm-rel vissza kell engedni (a stressz alatti vétlen lövés megakadályozása céljából)

A teljesség igénye nélkül az alábbi gyártmányú lőfegyverek kapták meg a tanúsítványt:

- Sig Sauer P226;
- , Sig Sauer P228;
- , HK P30 V2 és V6;
- , Glock 17, Glock 26.

AHOGYAN MI CSINÁLJUK

Kétségen kívüli az a tény, hogy a Magyar Köztársaság Rendőrségénél rendszeresített maroklőfegyverek (*vagy ahogyan a 2004. évi XXIV. Tv. a lőfegyverekről és lőszerekről szóló jogszabály ezt a kategóriát elnevezi" rövid lőfegyver"*) [7] több mint 90 % -a elavult. Néhány kiemelt egység vagy szerv kapott korszerűnek mondható lőfegyvereket (HK USP, HK USP Compact), de ezeknek száma nem éri el az ötszáz darabot sem. A rendőrség megítélését nemcsak a szakmai tudás, hanem a látszat is determinálja és valljuk be, nem segíti a pozitív összkép kialakulását az egyenruhás rendőr oldalán rossz minőségű szolgálati tokban logó, 1980-ban gyártott PA-63 típusú szolgálati lőfegyver.

Az új maroklőfegyverek rendszeresítésének hiánya azonban nemcsak a pénztelenség hibája. Tekintve a lőfegyvergyártók éles versenyét és figyelembe véve azt a tényt, hogy

[6] Erprobungsrichtlinien zur Technischen Richtlinie „Pistolen"
www.dhpol.de/de/hochschule/organisation/pti
7 2004. évi XXIV. Tv. a lőfegyverekről és lőszerekről

mekkora reklámértékkel bír az, hogy egy ország rendfenntartó szerve, szervei az általuk gyártott maroklőfegyvert használja álláspontom szerint megoldható lett volna az anyagi források (*ellentételezés, hazai gyártás*) előteremtése[8].

A nehézséget legfőképpen a rendszeresítési eljárás túlzott bonyolultsága okozza, amelyre példaként lehetne említeni a 9x19 mm Parabellum kaliberű 96 M P9RC típusú szolgálati maroklőfegyver rendszeresítését.

A FÉG gyártmányú P9 *(FP9 / P9M / P9R / P9 RK/ P9RZ*) típus család volt a kiinduló alap a 96 M P9RC lőfegyver tervezésénél. A P9 típusú lőfegyvert Kameniczky József tervezte 1971-ben, majd bővítette a típus családot 1978-ban a P9R-rel. A köztudomással ellentétben, a P9R alapját nem a Browning High Power M-1935 típusú klasszikus adta, hanem az 1954-1980 között gyártott Smith & Wesson M59 kismértékben átalakított másolata.[9] A 96 M P9RC típus pedig az 1979-től gyártott FÉG P9R elhanyagolható mértékű továbbfejlesztése, vagyis alapjaiban egy majdnem 60 éves konstrukció.

A kiindulási alapként szolgáló P9 kaliberre *(9x19 Parabellum vagy más elnevezéssel 9mm Luger/ 9mm NATO/ 9mm sk ptr / 9mm Pistolenpatrone 08 / 9mmx19/ DWM C-D 487 C stb.)* megfelelt a NATO előírásoknak. Jól érzékelték a döntéshozók, hogy az akkoriban rendszerben lévő 9x18 mm Makarov lőszert tüzelő PA-63 már nem felel meg a kor követelményeinek.[10] Sem a PA-63 műszaki jellemzői és az általa használt Makarov lőszer célban kifejtett ballisztikai hatása és teljesítménye nem teljesítette az elvárásokat, szolgálati célra történő továbbfejlesztése nem vezetett volna eredményre.

A P9 típus továbbfejlesztését álláspontom szerint csak egy elfogadható ok támasztotta alá, még pedig, hogy hazai tervezésű lőfegyvert, hazai gyártással adunk a fegyveres erőknek, fegyveres testületeknek. Ne feledjük a cseréről született döntés 1991 év vége, 1992 elején született meg, de a tényleges ellenőrző vizsgálatok már a P9 típusnál gyakran előfordult csőszakáll törés kijavítása után 1996 májusában indult el. Az igen szakszerűen és precízen lefolytatott és dokumentált próbákat az akkori BM felkérésére a Haditechnikai Intézet végezte el és hivatalosan 1997. február 28-án lett vége. *Ne feledjük, a HTI ebben az esetben azt a fegyvert véleményezte, amelyet a rendelkezésére bocsátottak és nem egy adott pályázaton induló több fegyvertípusból kellett kiválasztania az általa legjobbnak tartottat*. Érdekesség, hogy 1996 őszétől folyamatosan történt a Magyar Honvédség ellátása, de hivatalosan az akkori honvédelmi miniszter a 90/14/2003/VKI (HK 20/2003) sz. határozatával rendszeresítette a Magyar Honvédség eszköztárában a 96M P9RC pisztolyt.

A cikk elkészítése érdekében végzett felkészülésemkor meglepődve tapasztaltam, hogy bár a rendszeresítési eljárást a HTI végezte, de a Rendőrség, a Magyar Honvédségtől korábban, 73-101/2/1999 nyilvántartási számon rendszeresítette[11]. A rendszeresítés okaként a „PA-63 típusú pisztolyok kiváltása nagyobb hatékonyságú fegyverrel" (sic!) lett, megjelölve. A fentiekből világosan látható, hogy a döntés meghozatalától (1992) a rendőrségi rendszeresítésig (1999) hosszú idő telt el.

A folyamat végén a Rendőrség birtokában került egy olyan fegyver, amely már a rendszeresítési eljárás megindításakor is elavult volt.

Ne feledjük, 1979-ben rendszeresítették a Sig-Sauer P225 típust, a közismert Glock 17 műanyag tokos lőfegyver 1982-től készül sorozatgyártásban és 1983-ban rendszeresítették a NATO-ban *(NATO rendszeresítési ügyszám: 1005/25/133/6775)*, 1984-ben állt rendszerbe a Sig-Sauer P 226, 1993-ban debütált a HK USP család.

8 228/2004 Kormányrendelet a védelem terén alapvető biztonsági…
9 www. hu.wikipedia.org
10 19/2010. ORFK Utasítás kényszerítő eszközök rendszeresítései
11 23/1997 ORFK Utasítás Magyar Köztársaság Rendőrsége Lövészeti és Lőkiképzési Utasítás

JAVASLAT

Álláspontom szerint jelentős költség megtakarítással járna, ha a rendszeresítési eljárás csak a próbahasználatból (Magyar Honvédség elnevezése csapatpróba) állna olyan szolgálati lőfegyver esetében, amely már rendelkezik egy ilyen tanúsítvánnyal (például PTI által kiadottal).

A PTI által tesztelt és a tanúsítványt megkapó lőfegyverek listája igen imponáló. Egyetlen egy fegyverről nem lehet azt elmondani, hogy rosszabb paraméterekkel bírnának mint a jelenleg rendszerben lévő lőfegyvereink. Megfigyelhető, hogy a 2003 után tesztelt fegyver még a mai napig világszínvonalat képviselnek a képességeikkel *(cserélhető markolatpanel, picatinny-szereléksín, egyszerű szétszedés stb)*.

A próbahasználat elhagyása nem lenne célszerű, annak megtartásához néhány ok :

- Kompatibilis- e a már rendszeresített derékszíjjal a fegyverhez járó szolgálati tok (célszerű, de főleg olcsóbb a már kipróbált és nemzetközi szinten folyamatosan tesztelt gyári vagy gyár által javasolt hordtok)
- A fegyver és tok kialakítása miatt be lehet-e kapcsolni a szolgálati autóban biztonsági övet
- Nem akadályozza-e a fegyver gyors elővételét a már rendszeresített egyenruha
- Lehetséges-e a lőfegyver belsőtokban való hordása (polgári ruhás állomány vagy civil ruhában végrehajtott akciók miatt)
- stb

Egy ilyen megoldással elkerülhető lenne az, ami a 96M P9 RC típusú szolgálati lőfegyver rendszeresítésénél történt. Hazánk a jelenlegi gazdasági helyzetben nem engedheti meg magának a rendszeresítési eljárás során végzendő vizsgálatokkal járó költségeket.

A cikkem végére még egy érdekesség a PTI-ről. Az intézet nem csak lőfegyvereket tesztel és készíti el azokkal szemben lévő követelményrendszert, hanem tesztelnek még például lövedékálló mellényeket, rendőrbotokat, tömegoszlató pajzsokat…

Úgy gondolom, hogy ezen tanulmány a döntéshozók számára nyújthat egy olyan alternatívát a költségcsökkentés szempontjait is figyelembe véve, amely számukra és a végrehajtói állományra nézve is csak pozitív változásokat hozhat.

Felhasznált irodalom:

[1] Vass Gábor : Achtung ! Polizei ! c. cikk Kaliber Magazin 2011 március

[2] ORFK Oktatási és Kiképző központ : Rendőri szolgálati technikai ismeret

[3] 2004. évi XXIV. Tv. a lőfegyverekről és lőszerekről

[4] 2003. évi CXXIX. Tv. a közbeszerzésekről

[5] 384/2007. (XII. 23.) Kormányrendelet a Rendőrség által alkalmazott …

[6] 228/2004 Kormányrendelet a védelem terén alapvető biztonsági…

[7] www. dhpol.de (Erprobungsrichtlinien zur Technischen Richtlinie „Pistolen”)

[8] 18/2002 BM Utasítás BM Technikai Szabályzatáról

[9] 19/2010. ORFK Utasítás kényszerítő eszközök rendszeresítései…

[10] 23/1997 ORFK Utasítás Magyar Köztársaság Rendőrsége Lövészeti …

[11] www. hu.wikipedia.org

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Rohr Linda
linda.rohr@ymail.com

KAMERAOLDALI ÉS SZERVEROLDALI VCA[1] KÖZÖTTI VÁLASZTÁS TERVEZŐI KÉRDÉSEI

Absztrakt

A videotartalom-elemzés alapvető célja, hogy az operátorok munkáját megkönnyítse, mintegy automatikusan felismerve a biztonsági aspektusból veszélyes helyzeteket, személyeket. Fejlesztői szándék, hogy ezt minél kevesebb téves riasztással, minél pontosabban tegye, lehetőség szerint az emberi beavatkozás szükségességét minimálisra szorítva, illetve a holtidőben való visszakereséseket optimalizálva. Tervezői szándék, hogy a rendszer a környezeti, helyzeti specifikációit figyelembe véve a technológia előnyeivel és hátrányaival tudatosan számolva jöhessen létre a maximális biztonság. A tanulmány célja, hogy a zártláncú megfigyelő rendszerek alapelemévé és egyben folyamatosan fejlődő alapfunkciójává vált VCA két típusának - kameraoldali és szerveroldali feldolgozás - tervezéskor mérlegre tehető lehetőségeire és buktatóira rámutasson.

The aim of Video Content Analysis is to make the operators' job much easier with automatically recognizing the unsafe situations or dangerously acting people. For this reason the developers continuously work to minimize the possibility of false alarms and human mistakes, to optimize the dead time spent onto replaying and searching. The main target for security engineers is to design the system with the feasible maximum safety. Reaching this goal they have to be aware of the circumstances of the system as well as the advantages and disadvantages of the technology solutions. This paper tries to show the strong and weak points of the camera side and server side VCA those should be born in mind at the first steps of choosing the right solution.

Kulcsszavak: *IP kamera, CCTV, VCA, Szerveroldali video-képanalízis, Kameraoldali videoképanalízis ~ IP cameras, CCTV, VCA, Server side, Camera side*

[1] Video Content Analysis – Videó-képtartalom elemzés

BEVEZETÉS

A 2000-es években két nagy lökést kapott a VCA fejlődése. Az egyik a számítástechnika, és azon keresztül az IP világának térhódítása, amely jelen állapot szerint egészen a multi-megapixel, Full HD felbontású kamerákig, a H.264 tömörítésig, az NVR-ek és szoftver menedzsment programok megjelenéséig vezetett el. A másik a 2001. szeptember 11-i események hatása, amelyek következtében alaposan megnövekedett a hatékony védelmi megoldások iránti igény. Mivel a 9/11-es esetben a repülők nagy szerepet játszottak, a repülőtér-specifikus alkalmazások fejlesztése vált prioritássá. Ezek közé sorolható az otthagyott/elveszett tárgy detektálása, a virtuális határ átlépése, a mozgásirány azonosítása és végül a komplexebb viselkedési mintákat elemző megoldások olyan szolgáltatásokkal, mint a „lődörgés" vagy feltartott kéz érzékelése.

A technológia fejlődését legjobban talán az arcfelismerés céljából végzett fejlesztések demonstrálják. Az FRVT[2] szerint a 2009-es arcfelismerési megoldások több mint tízszer pontosabbak, mint 2002-ben és százszor hatékonyabbak, gyorsabbak, mint a 90-es évek közepén.

A videotartalmat a kamera vagy a szerver elemezze-e, melyiknek milyen előnye és hátránya van, a perem-mag témakörben folyó viták okait és az ezek által megszületett tervezői szempontrendszert fogom a következőkben részletesen kifejteni. [1]

1. KAMERAOLDALI VIDEO-KÉPANALÍZIS

Kameraoldali videokép-elemzés esetében a kamerába integrált szoftver és processzor együttesen végzi el az analizálási feladatokat, majd az eredmények alapján eldönti, hogy mely képeket küldi tovább a központi szerver felé: ezt nevezik eseményvezérelt, vagy triggerelt rögzítésnek. Ennek a megoldásnak legfőbb előnye, hogy csak azok a videofolyamok terhelik a hálózatot és végül a tárhelyet, amelyek releváns információt tartalmaznak. A továbbítási metódusnak kétféle változata létezik. Abban az esetben, amikor a hálózat áteresztő képessége szűkkeresztmetszetet jelent, a kamera ténylegesen csak akkor ad képet, amikor történik valami az aktív területen, azonban ez hiányos lehet. Gondolok itt olyan incidensre, amikor a gyanús cselekmény előtti állapot is fontos lehet vagy kétséges, hogy minden ténylegesen detektálásra került, esetleg a berendezés hibázott. A másik, többször alkalmazott lehetőség, amikor a kamera mindig továbbítja az eseményeket, azonban a nyugalmi állapotról készült felvételt alacsonyabb minőségben és sebességben, például CIF felbontásban 5 fps[3]-el továbbítja, majd érdekes esemény bekövetkeztekor megapixel vagy HD felbontásban 25 fps-el rögzíti és továbbítja a videostreamet.

Kameraoldali videokép analizálás esetében a kamera az úgynevezett nyersképeken hajtja végre a VCA algoritmusokat, amelyek teljes tömörítetlen állapotban állnak rendelkezésre, továbbá maga indukálja a riasztást, így azonnali reagálásra képes. Ez korlátlan számú alkalmazási lehetőséget jelenti egyrészről, másrészről azonban egyenként korlátozott erőforrásokat. A kamerák „egyedülállósága" lehetővé teszi a kamera belső paramétereinek pontos ismeretét, például a zajok csak az adott kamerára vonatkoztatott precízebb szűrését, mivel a szenzor közvetlenül, a végpont egyéni zaj karakterisztikája alapján dolgozik.

Különböző, kameraoldali analízist támogató IP kamerákat gyártó cégek honlapja alapján a következő szoftverszolgáltatások valósíthatók meg a peremen (2010):

[2] Face Recognition Vendor Test – Arcfelismerő rendszereket fejlesztő szervezetek tesztje

[3] Frame per Secundum – a képtovábbítási sebesség mértékegysége a szakirodalomban ips-ként Image per Secundumként is előfordul

ESEMÉNY	REAKCIÓ LEÍRÁS	FUNKCIÓ
Eltakarás/kiforgatás, Szabotázs	Riasztást küld, ha a kamerát elforgatják, kitakarják vagy bármilyen módon működésképtelenné teszik	Védi a rendszer integritását
Elhagyott tárgy	Riasztást küld, ha egy tárgyat magára hagynak (p.l.: bőröndöt a repülőtéren)	Védi az emberéletet és az értékeket
Ellopott tárgy	Riasztást küld, ha egy megjelölt tárgyat elmozdítanak.	Védi az értékeket
Forgalom irány megszegés	Riasztást küld, ha egy jármű vagy személy a megjelölt forgalmi iránnyal szemben halad	Nagyobb közúti biztonság, védi az emberéletet
Rendszámtábla felismerés	Felismeri és azonosítja a gépjárműveket	Védi az értékeket
Tömeg kialakulása	Riasztást küld, ha egy területen nagy tömeg gyűlik össze	Védi az értékeket és az emberéletet
Futó ember	Riasztást küld, ha egy személy a szokásosnál jelentősen gyorsabban halad	Védi az értékeket és az emberéletet
Parkolási szabály megszegés	Riasztást küld, ha egy gépjármű tilos helyen parkol	Védi az értékeket és az emberéletet
Gyorshajtás/ forgalomszámlálás	Felismeri a gyorsan haladó gépjárműveket, kategóriánként számolja a forgalmat	Védi az értékeket és az emberéletet
Virtuális kerítés	Virtuálisan kijelölt vonalon áthaladó/ átmászó/áttörő személyeket, járműveket detektálja és riasztást küld	Védi az értékeket és az emberéletet
Jelenlét nélküli terek	Általában emberi jelenlét nélkül működő terek (pl.: generátor termek) figyelése. A beállított időintervallumon kívül történő behatolást jelzi és rögzíti.	Védi az értékeket

1. táblázat: Kameraoldali VCA általi szolgáltatások [2]

Az eddig leírtak alapján úgy tűnhet, hogy a kameraoldali analízis könnyedén működhet, azonban komplexebb, nagy kameraszámú rendszerek esetében több probléma is felmerül. Először is a videó menedzsment szoftver szemszögéből elengedhetetlen az integráció lehetősége. Ez alatt azt értem, hogy a tervezéskor és kiépítéskor figyelni kell arra, hogy az összes rendszerelem ugyanazt a szabványt, ONVIF-et vagy PSIA-t támogassa vagy a gyártókat, típusukat figyelembe véve fel kell készíteni a szoftvert a használatukra. A videó menedzsment szoftver számára azonban standard interfészen keresztül sem lehet egyedüli megoldás a kameragyártók saját analízis szoftvere, mivel nem lehet egységes, azonos minőségű szolgáltatást definiálni.

Másodszor, több kamerát használó megoldások esetében (tracking over many cameras, 3D tracking) a hatékony adattömörítés nehézkesen, vagy sehogy sem oldható meg, mert több kamera összehangolt tömörítését kéne megvalósítani. Harmadszor egy szerintem nem túl távoli jövőben megoldódó problémát emelnék ki, a webes beállítási és frissítési gondokat. Az IP kamera önállóan képes működni a webkamerákkal ellentétben, ez azonban azt is jelenti, hogy saját intelligenciával, számítógépes háttérrel rendelkezik, amelyet ugyanúgy frissíteni kell a megfelelő, hibamentes működéshez, mint a PC-ken futó programokat, operációs rendszereket, majd a beállításokat elvégezni. Száz darab kamera esetében jelen állás szerint ez száz darab eszköz frissítését jelenti, amely feladat megoldható ugyan egyszerre egy külön szoftver segítségével, de a kamerák beállítását külön-külön újra el kell végezni.

Kérdéses még a már meglévő analóg rendszerekkel való összehangolt működése a kameraoldali VCA-nak, amennyiben azt ki szeretnék egészíteni és egy hibrid digitális rögzítőn kezelni.

Végül pedig, ugyan a kameragyártók szívesen hívják fel a figyelmet a tárhely és sávszélesség tehermentesítése miatti pénzbeli megtakarításra, ez a kitétel csak abban az esetben igaz, ha egy szuper intelligens kamera pontosan annyiba kerül mínusz a szervert érő terhelés járulékos költsége, mint egy egyszerűbb kivitelű darab, amelyben viszont nincs szükség annyi elektronikára, mert a szerver végzi az analízist. [2] [3]

2. SZERVEROLDALI VIDEO-KÉPANALÍZIS

A hagyományosnak tekinthető VCA futtatási hely a központi egység, hiszen az analóg rendszereknél elemzett digitális jelekké konvertálás és DVR-eken történő tárolás lehetővé tette a digitális jelek analizálását az akkori szervereken is. Kiemelkedő előnye a processzor kapacitás, illetve ennek rugalmas felhasználhatósága, valamint hogy egyéb kiszolgáló erőforrásokkal egyszerűbben és nagyobb mértékben bővíthető a peremeszközökhöz képest.

Szerveroldali video-tartalomanalízis esetében a kamerák tömörítve küldik el a képeket egy központi szervernek, vagy több szerver esetén a saját csomóponti szerverüknek, majd a videofolyam ott kerül kitömörítésre, képekre bontásra és analizálásra. Ez a típusú analízis korlátlan erőforrásra tud építeni, így bonyolult algoritmusok is lefuttathatók, valamint nagy rendszerekhez kellő rugalmasságot biztosít. Az egész videostream analizálására kiterjedő kondíciókat ad, ugyanis nemcsak a tárolás kérdését oldja meg, hanem processzorigényes, összetett számítások is elvégezhetőek. Erőforrás igényes gépi látás eszközök alkalmazhatósága (háttérmodell, integrál hisztogram, kimerítő keresések, sztochasztikus követési algoritmusok – kiterjesztett Kalman szűrő) is megoldott.

A szerveroldali VCA során nincs szükség metaadat[4] átvitelre, amely a kameraoldali tartalomelemzés esetében szükséges ahhoz, hogy az azonos osztályozású képeket egy helyen tárolják megérkezésük után.

Ezzel a változattal könnyebb több különböző videostream-et használó megoldások alkalmazása és a kamerák minden típusával képes összehangolt működésre, amely megkönnyíti a videó menedzsment szoftvergyártók feladatait.

A szerver programjainak, operációs rendszereinek frissítése hatékonyan történhet akkor is, amikor több szervert alkalmaznak egyszerre. Ez vonatkozik a beállítási (setup) eljárás periódusára is.

A rendszer konfigurációja egyszerű abban az esetben is, ha különböző gyártók, vagy ugyanazon gyártó jelentősen eltérő termékeinek egy rendszerbe való integrálása a feladat. Nem szükséges bajlódni az eltérő menürendszerek és beállítási paraméterek okozta nehézségekkel.

[4] A metaadat adat az adatról. A metaadattal összekötött tartalmat *tartalomcsomag*nak nevezik.

Ha a meglévő rendszerbe nem integrálható VCA, akkor a szerveroldali képanalízis költséghatékonyabb, hiszen nem kell hozzá lecserélni a már működő eszközöket, inkább csak kiegészíteni azt megapixel vagy HD felbontású kamerákkal az indokolt pontokon.

Általában a teljes installáció kameráinak csak egy kisebb része végez videó analízist, adott esetben a videó menedzsment rendszer szervere még gond nélkül ellátja a feladatot ahelyett, hogy az intelligens kamerák plusz kiadást jelentenének. Ez a helyzet persze a jövőben megfordulhat a videó analitika elterjedésével.

A szerveroldali analízis rugalmassága miatt folyamatos küzdelmet is jelent a fejlesztő cégek számára a „gyors, megengedhető" algoritmusokért (IPP-Intel Integrated Performance Primitives, openCV-Open Computer Vision library, JNI-Java NAtive Interface, GPGPUGeneral Prupose GPU Programming). [4]

3. ÖSSZEVETÉS

Ebben az alfejezetben kerül sor a két videokép-analízis terület összehasonlítására. Az összehasonlítást olyan szempontok alapján végzem, amelyek egyrészt befolyásolják a tervezési döntéseket, másrészt kihatással lehetnek a fejlesztési irányokra, harmadrészt, amelyekben összemérhető a két módszer.

3.1. CPU igény

Általánosan kijelenthető, hogy a memóriakapacitás bővítése egyszerűbb és olcsóbb feladat, mint a processzoré, ezért az alapul választott, rendelkezésre álló CPU teljesítménye kulcskérdés, ahogy esetleges cseréjének következményei is. Kamerákon belül cserélni, bővíteni nehézkes vagy veszteségek nélkül nem megoldható, márpedig a végfelhasználók a kamerákkal 5-10, sőt, bizonyos esetekben 15 évre előre szeretnének tervezni, míg szerverek vagy számítógépek esetében a cserét akár 2-3 évente is hajlandóak végrehajtani.

Az 1.1. táblázatban bemutatott kameraoldali VCA szolgáltatások mindegyike csak a cselekmény történésének detektálására irányul, mivel a cselekmények mikéntjének és hogyanjának eldöntése processzorigényes feladat. Például elhagyott, vagy ottfelejtett tárgy esetében a kamera képes a statikusság megállapítására, de már nem rendelkezik elég erőforrással ahhoz, hogy megállapítsa, mi is az a tárgy. Erre csak egy bonyolultabb algoritmus képes, amelyhez a szerveroldal nyújtotta processzor és memória szükséges. Ugyanez a helyzet a személyszámláló algoritmusok esetében. Kisebb forgalmú helyre betérő és kisétáló személyek számlálására a kamera is alkalmas, azonban egy bevásárlóközpont napi, akár tízezres nagyságrendű személyforgalmát képtelen lenne követni. A szerveroldali VCA fejlesztők is most szembesülnek ennek a feladatnak a megbízhatóbbá tételével, de itt már olyan „apró" célok elérése a tét, mint a babakocsi, bevásárlókocsi, háziállatok megkülönböztetése, az embercsoportok egymástól való szétválasztása, a környezet nehezítő körülményeinek kivédése (pl.: árnyékok), a lengőajtók, kapuk kimaszkolása akkor is, ha a beállításkor elfelejtik azt kiiktatni. Tehát összegezve: a worst case-re való programtervezés és megvalósítás. [4]

3.2. Sávszélesség igény

Mint ahogy erről már szó esett, a sávszélesség igény kérdése a hálózati megfigyelés gyenge pontja, szűkkeresztmetszete. A peremoldali tartalomelemzés nagy előnye, hogy a sávszélesség igényt lecsökkenti, nem veszi folyamatosan igénybe a hálózati infrastruktúrát, mivel csak az érdekes képeket továbbítja. Itt viszont ismét utalnék a kamerák adta funkciók táblázatára (1.1. táblázat), amelyben tizenegy szolgáltatás került felsorolásra az alapvető mozgásérzékelésen túl. Ha olyan szélsőséges eset állna fenn, hogy az összes funkció egyszerre való alkalmazása lenne

szükséges, akkor ebben az esetben is állandósulna a képátvitel. Természetesen a kamerákat a különböző alkalmazási igények szerint kalibrálják telepítéskor, így nem fogja az összes funkciót egyszerre használni, hanem például múzeumi felhasználás esetében a műtárgyakra állított kamerák tárgykövetés funkciója fog esetleg kiegészülni az ottfelejtett tárgy funkcióval. Az alkalmazott funkciók számának növelésével a használt sávszélesség (és tárhely) a különböző események bekövetkezésének arányában fog nőni.

Szerveroldali VCA esetén ahhoz, hogy optimálisan használt sávszélességről lehessen beszélni, egyrészről az újabb tömörítési eljárásokra lehet alapozni. Másrészről a fejlesztő cégek olyan technológiai fejlesztéseken dolgoznak, mint az ABS ™[5]. Ez a technológia többnyire H.264 streamek felett működik, MPEG-4-en és MJPEG-en túl. Az elgondolás lényege, hogy az aktívan figyelt tér úgynevezett „I" (az összehasonlításon és predikción alapuló tömörítések alapképei) képeit teljes JPEG[6]-ként viszi át, azon belül pedig az eseményeket, elmozduló objektumokat nagyobb felbontásban, élesen, majd a továbbiakban beérkező, a változások történésének ellenőrzésére szolgáló képek (P és B képek) információtartalma alapján feljavítja a kezdetben még pixeles hátteret. [4]

3.3. Berendezés biztonság

A berendezéseink biztonságának kérdése elhanyagolt terület a fejlesztő, gyártó cégek részéről, ám a biztonságtechnikai tervezésnél alapvető szempont. A kamerákat érdemes például olyan magasságba telepíteni, ahol kézzel nem elérhetők, ám karbantartásuk, tisztántartásuk nem ütközik nehézségbe. Sajnos gondolni kell arra is, hogy miként előzhető meg a biztonsági berendezés vagy annak információtartalmának lopása.

A hálózati megfigyelés képeit kódolják, illetve tűzfalakkal, vírusölőkkel, VPN[7] kialakításával igyekeznek magát a hálózatot biztonságossá tenni, ennek ellenére is Damoklész kardja örökké az IP rendszerek feje felett lebeg. Vannak törekvések a kódolási algoritmusok megfejtésére, a kulcsok feltörésére, a digitálisadat visszafejtésére. „A gyengébb titkosítási eljárások már ma sem jelentenek akadályt, a jobbak feltöréséhez a matematikai-hardveres apparátus még nem elég egy darabig. Másik oldalról pedig a legtöbb algoritmust nem kell megfejteni, mert minden normálisabb nyílt és megismerhető, csak a gyengeségeit kellene kihasználni." - Sereg Tibor (Aspectis Kft. 2010.06.03.)

Azonban az egyértelmű előny, hogy többé nem elég a koaxális hálózatra csatlakozni az információ megszerzéséhez vagy álképek betöltéséhez. Ebből az aspektusból vizsgálva a vírusokkal való megfertőzés, az illetéktelen hozzáférés egy szerverre koncentráltan könnyebb lehet, mint több végpontra szétosztottan. Habár a vírusok a legritkább esetben jönnek képbe, ha képi adatok biztonságáról van szó, szerintem. Inkább a lehallgatás, az illetéktelen hozzáférés, esetleg a kompromittálódás a fő veszély.

A hardver rész biztonsági kérdéseinél azonban egy vagy több szerverszoba védelme egyszerűbben megoldható megfelelő beléptetőrendszer alkalmazásával, mint minden egyes végpont még egy kamerával való megfigyelésével. A kamerák gyors eltulajdonítására a szabotázsvédelem nem ad elégséges megoldást, márpedig a szuper intelligens kamerák értékes berendezések bármely rendszer elemeiként és önmagukban is.

[5] Adaptive Balanced Streaming Technology
[6] Joint Photographic Experts Group
[7] Virtual Private Network

3.4. Stabilitás, robusztusság

Jelenleg - a fentebb taglaltak alapján - a szerveroldalon működő VCA algoritmusok stabilabban működnek a rugalmas CPU támogatottság miatt, így kevesebb téves riasztást generálnak. A programok és fejlesztési irányok rugalmasabb környezetre találnak a szerverekben, több lehetőséget nyújtanak az újdonságoknak, a részletesebb kidolgozottságnak. Az idő múlásával fény derül arra, hogy melyik specifikáció, funkció elég robusztus ahhoz, hogy a jövőben is fennmaradjon, mintegy a szoftverszolgáltatások evolúciójában. Amelyek fennmaradnak és megbízhatóan, „egyszerűen" működnek, azok kamerákba integrálhatóvá válnak. Tehát ugyan a szerveroldali fejlesztések mindig egy vagy két lépéssel a kameraoldali fejlesztések előtt fognak járni, de a kamerákba már csak a „bejáratott", stabil működést biztosító megoldások kerülnek át. [4]

3.5. Reakcióidő

Reakcióidő alatt értem azt az időtartamot, amely eltelik a gyanús esemény bekövetkezése és a riasztás létrejötte közt. Ebben a tekintetben a kameraoldali analízis és az általa kiküldött riasztási jel jelzési ideje minden kétséget kizárólag megelőzi a szerveroldali VCA reakcióidejét. Ezt a különbséget az a továbbítási és feldolgozási idő adja, amely eltelik a kép leképezése, tömörítése, továbbítása, a tömörítés helyreállítása, majd az analízis végrehajtása után végül megjelenő jelig. Ez az idő nem több néhány másodpercnél, egyszerűbb algoritmusok esetében a másodperc tört részénél. Azonban a sokszor elhangzó szólás miszerint csak „másodperceken múlt" valaki élete, értéke, ebben az esetben erősen befolyásolja az adott ügy végkimenetelét. Ezen tulajdonság is igényt támaszt a kétféle videotartalomelemzés szimbiózisára.

3.6. Karbantartás

A szoftver karbantartásáról, folyamatos frissítésének szükségességéről már esett szó. A kameránkénti külön-külön végzendő upgrade a csak szervereken végzendő frissítésekkel szemben több befektetett munkát igényel, körülményesebb, különösen nagy rendszerek esetében, de akár már 8-16 kameraszámú rendszer esetén is. A kamerák karbantartása a tisztántartás mellett azt is jelenti, hogy a hatékony bűnmegelőzésre folyamatosan figyelni kell, a megjelenő bűnözési trendeket összevetve a rendszer szolgáltatásaival. Természetesen a tisztántartás, a megfelelő működés ellenőrzése szerveroldali videokép analízis esetén is esszenciális, bár ezen túlmenően a szervereken belüli esetleges memóriabővítés, vagy a processzorkapacitás növelése egyszerűbben megoldható.

3.7. Üzleti szemszög

Ezt a nézőpontot azért említem meg, mert az analóg rendszereknél kialakult CCTV piac az IP kamerák megjelenésével felborult. A hagyományos, nagy tapasztalatú kameragyártók úgy vélekednek, hogy a biztonságtechnikai piacra belépő számos, alapvetően informatikai cég a hálózati megfigyelésre úgy tekint, mint isten adta ajándékra, amely csak rájuk vár a kamerák, az NVR-ek, a szoftverek fejlesztésével. (A világ piacvezető IP kamerája gyártója az Axis Communications is informatikai cégként indult, majd állandóan élen járó minőségi fejlesztéseivel felbolygatta ezt a piaci szegmenst.) Az analóg világ gyártói így csak piackövető szerepet tudnak betölteni az internetalapú megfigyelésben, habár ők is látják, hogy a jövő egyértelműen az IP irányába és az analóg kamerák megszűnése felé vezet. A

reakciójuk, miszerint a nyersképeket nem szívesen adják ki kezükből, hanem azokon még ők szeretnék az analízist elvégezni, így emelve a kamerák értékét, egyértelmű következménye a közelmúltbeli piaci változásoknak. A 2010-es előrejelzések szerint ezek a kameragyártók erős üzleti és marketinglépéseket fognak tenni annak érdekében, hogy a kameraoldali VCA kerüljön előtérbe.

3.8. Piacelemzést segítő extra funkciók

Internetes reklámok, hirdetések folyamatosan cikkeznek arról, hogy egy IP kamerának köszönhetően különböző gazdasági célú statisztikákat lehet összeállítani, ezzel könnyítve meg az áruházak számára a vásárlói szokások és igények felmérését. A fejlesztési irányok ezen vonala nem biztonsági célzattal jött létre, hanem annak a felfogásnak következményeként, hogy minél több lehetőséget aknázzanak ki a már meglévő erőforrásokra építve. Az erőforrások alatt nemcsak a hardver és szoftver igényeket értem, hanem továbbmenve a kutatás-fejlesztésbe invesztált energiákat is.

Olyan szolgáltatásokat építenek ezért be a kamerákba, mint az áruházon, bolton belüli útvonalak forgalom szerinti sorrendezése, így mutatva meg, hogy melyik árut hova érdemes tenni, attól függően, hogy népszerűségét növelni akarják-e. A kamerák intelligens megoldásai a boltban eltöltött átlagos időt is mérni tudják ahhoz, hogy a vásárlói elégedettségre, a bolton belüli komfortérzetre nézve vonjanak le következtetéseket. Elemezhető az is, hogy egyes termékcsoportok előtt mekkora érdeklődés figyelhető meg, például hogy a mosóporok polcai előtt mekkora a látogatottság. Nem utolsó sorban az alkalmazottak munkája is ellenőrizhetőbbé válik.

A jövőbe mutató fejlesztések azt próbálják megvalósítani, hogy egyrészről olyan statisztikákat is képes legyen a hálózati megfigyelő rendszer létre hozni, amelyek alapja az alapérzelmek felismerése egyes termékekre vagy termékcsoportokra vetítve, másrészről az alkalmazottak színre lépése után, közben hogyan változik vagy torzul el a látogató arca.

Ezek a feladatok már bonyolult algoritmusokat igényelnek, így nagy a CPU igényük, biztonsági szempontból ráadásul hátráltató lehet a végpontokon tárolni, onnan továbbítani a feldolgozott adatokat, illetve a statisztikai és biztonsági funkciók összeakadhatnak, amikor ugyanazt az erőforrást ugyanakkor akarják igénybe venni. Így ennél az alkalmazási területnél a szerveroldali video-tartalomelemzés kerül előtérbe.

ÖSSZEFOGLALÁS

A 2005. július 7-én a londoni metróban történt terrortámadást példának véve, 120 ezer órányi anyag állt a biztonsági szakemberek rendelkezésére ahhoz, hogy megkeressék a lehetséges gyanúsítottakat a videostreamekben. Ez VCA nélkül 10 fős csoportoknak napi 24 órában folyamatosan 500 napnyi munkát jelentett volna, feltételezve a lankadatlan figyelmet.

A pontosabb video-tartalomelemzést lehetővé tevő megapixel kamerák megreformálják a videós megfigyelő rendszerek tervezését, mivel látószögük nagyobb területet képes lefedni, vagy részletgazdagabb kinagyított képet tudnak leképezni. Ezek az analóg rendszereknél nem tapasztalt sajátságok, tulajdonságok további számításokat és precíz helyszíni bejárást igényelnek a tervezési fázisban. A kamerák elhelyezésekor a videokép analízis előre definiált célja meghatározó kell, hogy legyen.

A kétféle video-tartalomelemzés típust az alapján különböztetik meg, hogy hol kerül sor az analízisre, hogy a rendszer peremén vagy magjában lévő berendezés végzi azt. Mind a kameraoldali, mind a szerveroldali analízisnek megvannak a maga előnyei és hátrányai. Annak megállapítása, hogy melyikre van szükség, a kifejtett szempontok alapján történhet.

További részletek pontos meghatározását mindig az adott rendszer és körülményeinek alapos átgondolása, majd a választott módszer szerinti tesztelése alapján lehetséges megadni.

Véleményem szerint a jövőben a kétféle video-tartalomelemzés összehangolt működése adhat egy olyan komplex megoldást, amely az előnyöket erősítve, a hátrányokat kiküszöbölve teremt szimbiózist. A kölcsönös együttműködéshez szükséges a közös szabványokon nyugvó hálózati megfigyelés, amelyben a rendszerelemek gyártótól, típustól függetlenül kompatibilisen integrálhatók rendszerbe. Az általános, mindenre kiterjedő szabványosítás megvalósulása azonban várat magára.

HIVATKOZÁSOK

[1] SM (Security Management): MBT szakfolyóirat különszáma 2009., 29.-42. old. Ollári Viktor, „Blöff vagy a jövő technológiája”

[2] http://intellio.eu/technologia_beepitettintelligencia.php - letöltés ideje: 2010.05.20.

[3] http://www.videoiq.com/solutions.html - letöltés ideje: 2010.05.20.

[4] Ez a rész a szerzőnek Dezsényi Lászlóval történt konzultáció alapján készült a Netavis Kft. telephelyén. – 2010. 05.03. és 2010.05.11.

HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Horváth Tamás
tamhorvath@mvm.hu

IP ALAPÚ CCTV RENDSZERT?

Absztrakt

Szinte naponta kerül szóba videó megfigyelő rendszerek telepítését megelőző nem könnyű döntés: vajon van-e értelme IP alapú CCTV rendszert telepíteni, vagy a klasszikus analóg rendszer biztosítja a legjobb elvárt eredményt? A válasz természetesen nem egyszerű még akkor sem az, amikor a tervezési, illetve telepítési lehetőségek gazdasági szempontból nem elsődlegesek, azaz nem a rendszer bekerülési ára a meghatározó, hanem a végeredmény. Most is, mint minden hasonló esetben, a válasz összetett.

Almost every day, before install video surveillance systems, we get the question not easy decide: it is any reason to install IP based CCTV system or we should implement the classic analogue one? What is the system which provides the best expected result? The answer of course is not easy even if the design and the implementation are not basically restricted by financial things. Now the answer is complex, as usual.

Kulcsszavak: *IP alapú, nagyfelbontású képek, LAN, PoE ~ IP-based, high-resolution images, LAN, PoE*

AZ IP ALAPÚ RENDSZEREK ÉRTÉKEI

A műszaki különbségek az analóg, és az IP alapú CCTV rendszerelemek között természetesen meghatározók, de lehetnek meggyőzőek az analóg rendszerek által biztosított, főként a nehéz műszaki körülmények között készült képek, de az IP technológiából adódó lehetőségek rendkívüli módon rugalmassá, felhasználó baráttá, időtállóvá, és nem utolsó sorban nagyméretű rendszerek esetén olcsóbbá tehetik az IP alapú rendszereket.

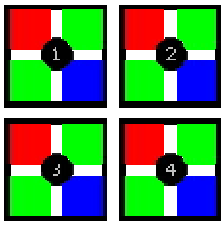
Nagyfelbontású videó képek

Digitális kamerák fejlesztése egyik alapvető célja a nagyfelbontású képek előállítása, továbbítása, és archiválási lehetősége biztosítása, ennek megfelelően a kamerák felbontása az egyik legmeghatározóbb tulajdonsága. Nem nehéz belátni, hogy az analóg technológiában gyakori felbontású video képek (D1: 720x576 – PAL), optimális esetben kiváló eredményt produkálnak, de nem lehet vita, hogy ezen felbontás napjainkban már nem konkurencia az IP alapú kamerák esetében. Egy-egy telepítés esetén ma már nem ritkák a 2-3, akár 4 Megapixel felbontású IP alapú kamerákkal felépített megfigyelő rendszerek azok előnyeivel, és hátrányaival együtt.

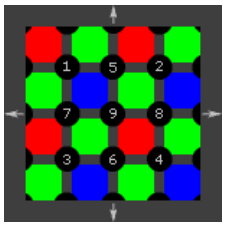
Mit jelent a 4 Megapixel?

Az analóg technológiából ismert felbontás az IP alapú rendszereknél már nem használható, de a színes képek előállítási módja a teljesen digitális rendszerekben sem más, az alapelvek jól használhatóak ebben az esetben is.

Az analóg technikából közismert Bayer szűrő[1] (Bayer Pattern) könnyen érthetővé teszi a szineskép alkotás módját:



1. kép: Bayer szűrő



2. kép: Interpoláció

A korábban már említett 4 Megapixeles képalkotó elem esetében (érzékelő méret: 1/2.5” CMOS; effektív pixel szám: 2288 (H) x 1712 (V) 4:3 képarány esetén, azaz a 3,9 MP) egyetlen képpont, amellyel a szükséges színű képelem előállítható 4 elemi pixelt tartalmaz. Annak érdekében, hogy a 4-es pixelcsoportok közötti szigetelő funkciójú terület ne legyen látható a képen, matematikai módszerrel (interpolációval) egymást 50%-ban átfedő képelem csoportokat képeznek, amely jó hatással van a képalkotó elem által biztosított kép felbontására is.

Egy másik igen fontos fizikai jellemző, hogy az emberi szem a zöld fény mennyiségére a legérzékenyebb, azaz a legkisebb változás drasztikusan módosítja a kép valósághűségét. Ennek megfelelően a Bayer szűrő 2-szeres mennyiségű zöld pixellel került kialakításra, ezzel biztosítva a szükséges zöld szín mennyiségét.

A fentiekből könnyen belátható, hogy egy 4 Megapixeles képalkotó elem esetében a valóságos képfelbontás a látható pixelcsoportok, képpont egységek tekintetében 2 Megapixel, a számításoknál ezeket a megfontolásokat érdemes figyelembe venni.

Helyi hálózat megléte

Az épületek nagy része már rendelkezik helyi számítástechnikai hálózattal. A hálózati végpontok az épületek szinte valamennyi helyiségéhez elérnek. A kamerák a LAN[4] végpontjaira csatlakoztathatóak [2], így nem szükséges önálló hálózati táplálás kialakítása, mert a hálózati kábelen keresztül (megfelelő hálózati aktív eszközök megléte esetén) ún. PoE-val[5] megoldható. Analóg kamerák integrálására is lehetőség nyílik a különböző csatornakódolók[6], illetve video szerverek segítségével.

Ez az előny, talán a legkevésbé használható érv a szakember számára. Természetesen az elméleti lehetőség valóban megvan az épületek ügyviteli hálózatai felhasználásra, de egy biztonságtechnika megfigyelő rendszert ilyen módon – a meglévő informatikai hálózat felhasználásával - TILOS megépíteni. Ezt a határozott tiltást arra alapozom, hogy a teljes biztonságtechnikai célú informatikai hálózat, annak valamennyi eleme üzemletetése a védett létesítmény biztonsági szintjével azonos kategóriába kell, hogy essen.

Nem kifejtve a biztonsági kockázatokat, az összes szakmai indokot nem elhanyagolható az a tény sem, hogy a rendszerrel dolgozó, az azt üzemeltető munkatársak előzetes szűrése, kiválasztása a biztonsági igényeknek megfelelőnek kell lenni. Ennek megfelelően a szokásos „Erkölcsi Bizonyítvány” nem elegendő.

Természetesen nem azt állítom, hogy néhány kamerát, a létesítmény méretétől függően, nem kapcsolhatunk rá az ügyviteli hálózatra, ha az aktív eszközök támogatják a VLAN[7] struktúrát, a kamerák által továbbított kép megfelelő konfiguráció mellett nem terhelheti a hálózatot, a szóban forgó informatikai hálózat csak az alacsony biztonsági kockázatú objektumban lehet, illetve kamerák száma ne haladja meg az 5-öt.

Kábel nélküli eszközök használata

A különböző rendszer-elemek kábel nélküli (Wireless) eszközökkel csatlakoztathatóak a hálózathoz, így egyes kamera pozíciók gond nélkül módosíthatóak. Ez igen nagy flexibilitást ad a rendszernek.[2] Akár két, vagy több IP alapú CCTV rendszer, rendszerenként sok-sok kamerával (megfelelő sávszélesség igény számítása mellett), összekapcsolható egy nagy rendszerré, mely üzemeltetése, felügyelete akár egyetlen helyszínről is lehetséges.

Biztonsági szempontokat szem előtt tartva meg kell jegyezni, hogy a kábelnélküli rendszereknél annak feltörése a viszonylagosan könnyű hozzáférhetőség miatt, lényegesen könnyebb, mint a biztonságtechnikai szabványoknak, elveknek megfelelően telepített kábelhálózaté.

Természetesen az informatikai hálózatok esetében használatos titkosítások a kábelnélküli rendszereknél is használhatóak, de azzal számolni kell, hogy a titkosítás megléte növeli a szükséges sávszélességet.

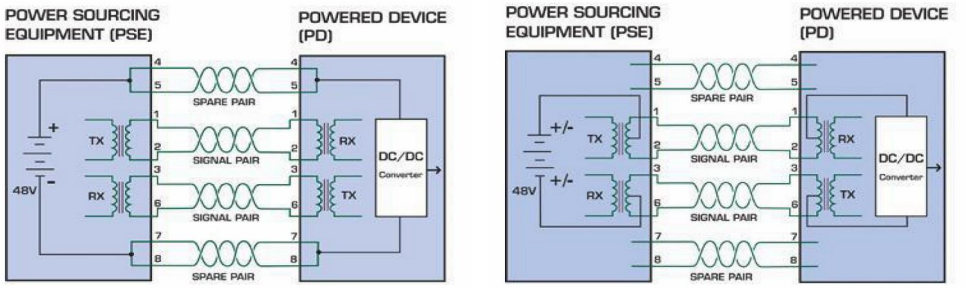
[4] LAN – Local Area Network – helyi számítástechnikai hálózat
[5] PoE- Power Over Ethernet – a helyi hálózati kábelezésen keresztül eljuttatott tápfeszültség az adott eszköz működtetéséhez.
[6] Olyan eszköz, mellyel az analóg kamerajeleket konvertálni tudjuk IP alapú rendszerekbe történő integráláshoz.
[7] VLAN: Virtuális Lokális Hálózat

PoE tápellátás

Az egyes kamerák hálózati tápellátására kézenfekvő megoldás lehet a meglévő hálózati kábelen történő tápellátás biztosítás. Az IP kamerák képátviteléhez (Ethernet felületű kommunikációhoz) elegendő két érpár, így lehetőség nyílik a fennmaradó kábel erek felhasználásával tápfeszültség bekötésére, természetesen számítással ellenőrizni kell az egyes PoE tápfeladók[3] terhelhetősége határait.

Napjainkban nem ritka az 1,5 KVA terhelhetőségű hálózati kapcsoló, amely az igen alacsony terhelést (2,5 W teljesítmény igény/kamera) adó IP alapú kamerák esetében rendkívül kedvező.

Lehetőség nyílik központi szünetmentes tápegység felhasználásra, amely a biztonságtechnikai CCTV rendszer biztonsági szintjét jelentősen megemelheti.



1. ábra: PoE megvalósítása[8]

Távoli elérés lehetősége

Meglévő hálózati hozzáférés lehetőséget teremt az IP alapú biztonságtechnikai CCTV rendszerek távoli elérésére az Interneten keresztül. Ezzel a módszerrel egymástól igen nagy távolságban lévő vállalatok (leányvállalatok, távfelügyelt épületek, objektumok, stb.) CCTV rendszerei egy hálózatba köthetőek, együtt menedzselhetők. Nem elhanyagolható az a lehetőség sem, amennyiben azt a telepítés, illetve a hálózati eszközök konfigurációjánál azt lehetővé tesszük, hogy az egyedi kamerák táveléréssel ellenőrizhetőek, az egyedi beállítások módosíthatóak, a karbantartás ilyen módon történő támogatása az üzemeltetést kifejezetten javíthatja.

Az egyes kamerák távelérése valóban jelentős előny lehet, de nem javasolt biztonságtechnikai megfigyelőrendszerek esetén, mivel az egyes kameraképek védelme nehezebben kivitelezhető.

A gyakorlatban, figyelemmel a biztonsági kockázatokra, nem ezt a megoldást szokás választani. Az egyes kamerák egy teljesen másik alrendszerben kell, hogy legyenek a rögzítőhöz képest, így a kamerák kizárólag a szerveren (rögzítőn) keresztül elérhetőek, így a biztonsági kockázat jelentősen csökkenthető, az esetleges behatolási kísérlet felfedezhető, nyomon követhető.

[8] Letöltve: Connect Power over Ethernet http://www.lantronix.com/support/

Alacsonyabb költségek [2]

Amióta az archiválás merevlemezekre történik az analóg rögzítést biztosító videomagnók üzemeltetési költségei, mint a rendszeres karbantartás, a kazetta hegyek megszűnése jelentősen csökkentek. A szakmai támogatást biztosító karbantartó társaság távoli hozzáféréssel is képes a műszaki problémák egy részének megoldására, amely további utazási, és karbantartási költségek csökkentését jelenti.

ÖSSZEGZÉS

Az IP alapú videó megfigyelő rendszerek előnyei egyértelműek az analóg rendszerekhez képest, de nem feledjük, hogy a jó minőségű videó képhez nem csak jó kamerát kell telepíteni, hanem a szükséges megapixeles optikai mellett a megvilágítási körülményeknek is közel optimálisnak kell lennie, ha szeretnénk a nagyfelbontású képek előnyeit élvezni.

A gyakorlatban a legjobb, leghatékonyabb megoldást a hibrid rendszerek biztosítják, melyek esetében a nehéz műszaki körülmények között, például gyenge megvilágítás, napjainkban az analóg, valódi Day/Night[9] kamerák rendkívül gyenge megvilágítási körülmények között is jól értékelhető képet biztosítanak. Az optimálishoz közeli megvilágítás megléte esetén a nagyfelbontású IP kamerák telepítése már nem okoz problémát. A fejlődés megállíthatatlan, az IP kamerák előretörése teljes körűvé válik a közeljövőben.

IRODALMI HIVATKOZÁS

[1] Tóth Levente: CCTV magyarul (Kiadó: BM Nyomda Kft., 2004)

[2] Herman Kruegle: CCTV Surveillance Video Practice and Technology Second Edition (Kiadó: Elsevier Butterwoth-Heinemann, 2007)

[3] Andrew S. Tanenbaum: Számítógép hálózatok

[9] Valós Day/Night: a kamerában beépített képérzékelő szenzor előtt egy mechanikusan mozgatható infra szűrő van, amely gyenge megvilágítás esetében elmozdul a szenzor előtt, így biztosítva a többlet fénymennyiséget és a megfelelő fókuszálást.