BOLYAI SZEMLE

2018/1. SZÁM

A NEMZETI KÖZSZOLGÁLATI EGYTEM KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA

XXVII. évfolyam, 2018/1. szám

BOLYAI SZEMLE

A NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI TUDOMÁNYÁGI FOLYÓIRATA

A borítón Prof. dr. Berek Lajos ezredes, CSc, Mednyánszky László-díjas szobrászművész *Bolyai János, a hadmérnök* című szobra látható.

A lapban megjelenő írásokat lektoráltatjuk. A közlésre szánt tanulmányokat a bolyaiszemle@uni-nke.hu címre kérjük megküldeni magyar és angol címmel, valamint magyar és angol összefoglalóval ellátva.

Kiadó: Nordex Nonprofit Kft. – Dialóg Campus Kiadó
Olvasószerkesztő: Tóth Orsolya
Korrektor: Balla Nóra
Elérhetőség: 1083 Budapest, Ludovika tér 2. – www.dialogcampus.hu
A kiadásért felel: Petró Ildikó ügyvezető
Tördelés és grafika: Nordex Nonprofit Kft.
ISSN 1416-1443

Tartalom

Természettudomány

Horváth István: A Gamma-spektrumok inverz problémája 11

Fatalin Dóra – Fatalin László: Szabályos ellenállásrácsok egyszerűsített számításaihoz 21

Biztonságtechnika

Tóth Levente: A komplex objektumvédelem kihívásai napjainkban 35

Tóth Attila: A biztonságtechnikai tervezők helyzete 45

Védelmi elektronika, informatika és kommunikáció

Munk Sándor: Kiberbiztonsági szervezetek közötti interoperábilis információcsere-megoldások (sérülékenységek kezelése) 54

Katonai logisztika

Estók Sándor: A modern logisztikatudomány fejlődésének kapuja kitárva 78

Réger Béla: Logisztika 4.0 hatása az okoseszköz-applikációk lehetőségei a multinacionális oktatási programokban 90

Lakatos Péter: A Közszolgálati Lenyomat Ludovika Kutatócsoport 2017-es tevékenysége és kutatási eredményei: a rendőrség 2016-os karbonlábnyoma és a reverz logisztika aspektusai 101

Katasztrófavédelem

Antal Örs: Zöld infrastruktúrák alkalmazásának lehetőségei az árvízmentesítés terén – innovatív fejlesztési lehetőségek 124

Balog Fatime: Az egységes digitális távközlő rendszer (EDR) szerepe a katasztrófakezelésben 146

E számunk szerzői

ANTAL ÖRS PhD-hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola. ORCID: 0000-0002-3656-0750

BALOG FATIME PhD-hallgató, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola. ORCID: 0000-0001-8773-1655

ESTÓK SÁNDOR dr., PhD, szakközgazdász, logisztikai magiszter. ORCID: 0000-0002-2422-5293

FATALIN DÓRA energetikai mérnök, a NKM Földgázszolgáltató Zrt. energetikai projekt mérnöke. ORCID: 0000-0002-0436-6611

FATALIN LÁSZLÓ matematikus, villamosmérnök, az NKE Természettudományi Tanszék egyetemi docense. ORCID: 0000-0002-7117-8573

HORVÁTH ISTVÁN Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Logisztikai Intézet Természettudományi Tanszék, tanszékvezető egyetemi tanár. ORCID: 0000-0002-1343-1761

LAKATOS PÉTER dr., PhD, egyetemi docens, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Logisztikai Intézet Hadtáp és Katonai Közlekedés Tanszék. ORCID: 0000-0003-1658-308X

MUNK SÁNDOR dr., DSc, ny. ezredes, egyetemi tanár, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Üzemeltető Intézet, Informatikai Tanszék, egyetemi tanár. ORCID: 0000-0001-8576-308X

RÉGER BÉLA dr., habil, PhD, főiskolai tanár, Edutus Főiskola. ORCID: 0000-0001-7296-0308

TÓTH ATTILA fejlesztési üzletág-igazgató, TVT Vagyonvédelmi Zrt. ORCID: 0000-0002-2530-1649

TÓTH LEVENTE szakmai igazgató, TVT Vagyonvédelmi Zrt. ORCID: 0000-0003-2979-5911

Our authors

ÖRS ANTAL, PhD student, National University of Public Service, Doctoral School of Military Engineering, research field: disaster management. ORCID: 0000-0002-3656-0750

FATIME BALOG, PhD student, National University of Public Service, Doctoral School of Military Engineering. ORCID: 0000-0001-8773-1655

SÁNDOR ESTÓK, PhD, Specialized Economist, Master of Logistics. ORCID: 0000-0002-2422-5293

DÓRA FATALIN, energy engineer, working as an energy project engineer at NKM Zrt. ORCID: 0000-0002-0436-6611

LÁSZLÓ FATALIN, mathematician and electrical engineer, Associate Professor at the National University of Public Service, Department of Natural Sciences. ORCID: 0000-0002-7117-8573

ISTVÁN HORVÁTH, Head and Professor at the National University of Public Service, Faculty of Military Science and Officer Training, Natural Sciences Department. ORCID: 0000-0002-1343-1761

PÉTER LAKATOS, PhD, Associate Professor at the National University of Public Service, Department of Supply and Military Transport, Military Logistic Institute. ORCID: 0000-0003-1658-308X

SÁNDOR MUNK, DSc, Col. (ret.), Professor at the National University of Public Service, Department of IT, Institute of Military Maintenance, Faculty of Military Science and Officer Training. ORCID: 0000-0001-8576-308X

BÉLA RÉGER, PhD, College Professor with Habilitation, Edutus College. ORCID: 0000-0001-7296-0308

ATTILA TÓTH, TVT Vagyonvédelmi Zrt., Development Director. ORCID: 0000-0002-2530-1649

LEVENTE TÓTH, TVT Vagyonvédelmi Zrt., Operational Director. ORCID: 0000-0003-2979-5911

Horváth István

A Gamma-spektrumok inverz problémája

Az utófények 1997-es felfedezéséig a gamma-kitöréseket csak a gamma-tartományban tudták megfigyelni. A kibocsátás távolsága nem volt ismert, a kitörés maximum néhány percig tartott, ezért a vizsgálatok csak az időbeli lefolyásra, illetve az észlelt fotonok energiaeloszlására (spektrumára) korlátozódhattak. Cikkemben ezen gamma-tartományban végzett spektrális vizsgálatokat tekintem át.

Kulcsszavak: asztrofizika; gamma-csillagászat; gamma-kitörések; kutató műholdak

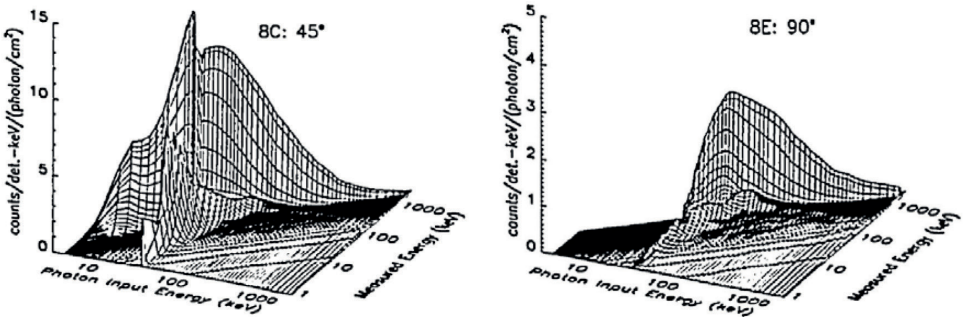
Közismert a gamma-spektrumok előállításának, az úgynevezett gamma inverz problémának a kérdése. [1] Minthogy a mért spektrum nem egyezik meg a megfigyelt spektrummal, hanem annak és a detektorban lezajló folyamatoknak az együttes hatása. A mért adatokból a megfigyelt valódi spektrum kiszámítására több dekonvolúciós eljárás létezik. [1] A mért spektrum nem egy folytonos függvény, hanem egy adatsor. Ezt jellemezhetjük egy $\underline{a}$ vektorral, ami a mért adatok energia szerint rendezett sora. Ebből kell meghatározni a bejövő spektrumot, amelyet egy $\underline{s}$ vektorral jellemezhetünk. A detektorra jellemző tulajdonságokat egy mátrixszal szokás leírni. Sajnos azonban a probléma megoldását jelentő A mátrix nem ismert, csak az inverze. A megoldást ugyanis a következő összefüggés szolgáltatná:

$$\underline{s} = A\,\underline{a} \tag{1}$$

Ugyan az A mátrix alakját nem ismerjük, ismerjük viszont az A mátrix R inverzét. Ekkor ugyanis

$$\underline{a} = R\,\underline{s} \tag{2}$$

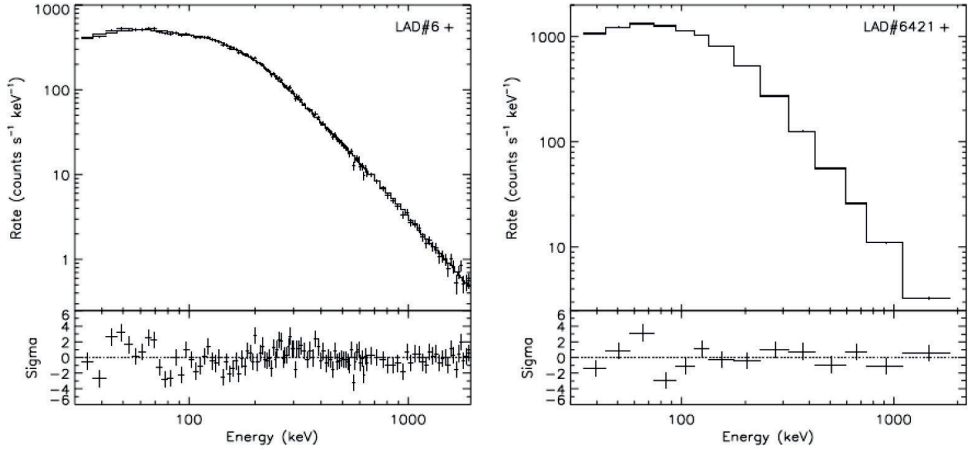
Ez az egyenlet azt fejezi ki, hogy egy adott spektrummal besugározva a detektort, milyen $\underline{a}$ eredményt kapunk. Az R mátrixot hívjuk a *detektor válaszmátrixának,* amely laboratóriumban mérhető. Az R mátrix függ a műhold felépítésétől is, hiszen a különböző műholdelemeken a fotonok és a részecskék szóródhatnak. A problémát tetézi, hogy az R mátrix leggyakrabban nem invertálható, tehát a spektrumot előállító A mátrix nem meghatározható. Ez az úgynevezett gamma inverz probléma. A detektor R válaszmátrixát laboratóriumban tudjuk mérni. A CGRO BATSE detektorának válaszmátrixát mutatja az 1. ábra. [2]



1. ábra – A CGRO BATSE detektorának válaszmátrixa a beérkezési szögtől függően ([2] alapján saját szerkesztés)

Megjegyzés: Vízszintesen a bemenő és az észlelt energia, függőlegesen pedig a megfigyelt beütésszám a feltüntetett egységekben

A CGRO BATSE detektorok válaszmátrixait a BATSE-csoport 1995-ben publikálta. [2] A gamma inverz problémát részletesen kifejti Bouchet tanulmánya. [1] Több különböző megoldással kísérleteztek az irodalomban: szinguláris értékekre való felbontás, [3] [4] Backus Gilbert-módszer, [5] [6] Phillips–Twomey-módszer [7] [8] stb., azonban egyik sem állítja elő az általános megoldást. A különböző módszerek különböző esetekben szolgáltatnak közelítőleg helyes megoldásokat. [1] [9]



2. ábra – Spektrumok a CGRO BATSE spektrális katalógusból [10]

Vizsgáljuk meg a spektrumok illesztését. Egy tipikus spektrum látható a 2. ábrán, amely Kaneko és társai BATSE spektrális katalógusában [10] jelent meg. A detektor válaszmátrix inverzének meghatározására nincs általános módszer. A detektor válaszmátrix ismeretében viszont megtehető, hogy modellspektrumokat transzformálunk a mért R mátrixszal

és a kapott számítási eredményt hasonlítjuk össze a mérési eredményekkel. Ezt a módszert alkalmazták a CGRO BATSE munkatársai a spektrális katalógusukban, [11] illetve a már említett 2006-os második katalógusukban. [10] A leggyakrabban használt illesztett függvény a David Bandról elnevezett úgynevezett *Band-függvény,* [12] amely a következő alakú:

$$f(E) = A\left(\frac{E}{100keV}\right)^{\alpha} \exp\left(-\frac{E(2+\alpha)}{E_{peak}}\right) \tag{3}$$

ha $E<E_{break}$,

$$f\ (E) = A\left((\alpha-\beta)\frac{E}{100keV(2+\alpha)}\right)^{\alpha-\beta}\left(\frac{E}{100keV}\right)^{\beta} \exp(\beta-\alpha) \tag{4}$$

ha $E\geq E_{break}$,

itt $E_{break} = (\alpha-\beta)\frac{E_{peak}}{2+\alpha}$, A az amplitúdó (mértékegysége fotonszám/cm^2/s/energia), α az alacsony energiás spektrális index, β a nagyenergiás spektrális index, E_{peak} egy illesztett energiaérték. Egy ilyen Band-függvény illesztése látszik az 2. ábra bal oldalán.

Ezen kívül használatos még a *tört hatványfüggvény:*

$$f(E) = A\left(\frac{E}{E_{támp}}\right)^{\lambda_1} \tag{5}$$

ha $E<E_{break}$

$$f(E) = A\left(\frac{E}{E_{támp}}\right)^{\lambda_1}\left(\frac{E}{E_{break}}\right)^{\lambda_2} \tag{6}$$

ha $E<E_{break}$

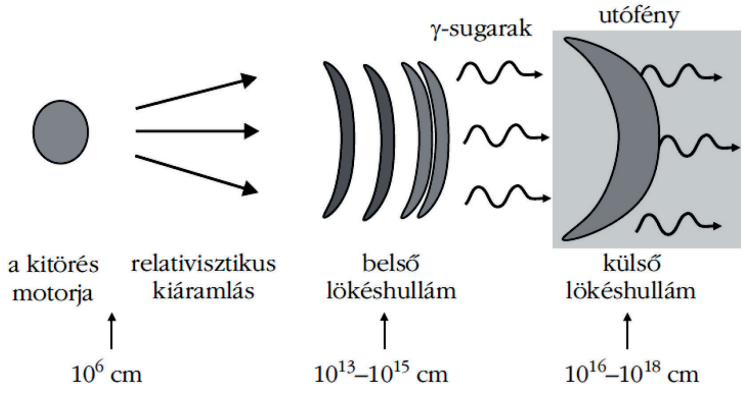
ahol λ_1 és λ_2 jelöli az alacsony és magas energiás indexeket, $E_{támp}$ pedig egy tetszőleges energia, amit arra választunk, hogy hol tekintjük a normálási amplitúdót. Ebben a spektrumban egy éles törés van, ellentétben a Band-függvénnyel, amelynek a deriváltja mindenütt létezik és véges.

Amikor a nagyenergiás spektrális index, β abszolútértéke lényegesen nagyobb kettőnél, akkor a Band-függvényben nem illesztenek nagyenergiás spektrális indexet. Ez a comptonizált modell, ezért neve a *Comp-modell.* A spektrumot leíró függvény ez esetben a következő alakú:

$$f(E) = A\left(\frac{E}{E_{piv}}\right)^{\lambda} \exp\left(-\frac{E(2+\lambda)}{E_{peak}}\right) \tag{7}$$

λ és E_{piv} itt is illesztendő paraméterek a spektrumban. [10]

Az egyik elfogadott nézet szerint a kitöréseket úgynevezett belső lökéshullámok ütközéseivel lehet magyarázni. Egy belső központi motor produkálja az extrém relativisztikus héjakat (3. ábra), amelyek egymás közti ütközését nevezik belső lökéshullámnak. A relativisztikus ütközések produkálhatják az azonnali gamma-sugárzást, amelyet a Földön gamma-kitörésként észlelünk.



3. ábra – A gamma-kitörések belső lökéshullám modellje ([13] alapján saját szerkesztés)

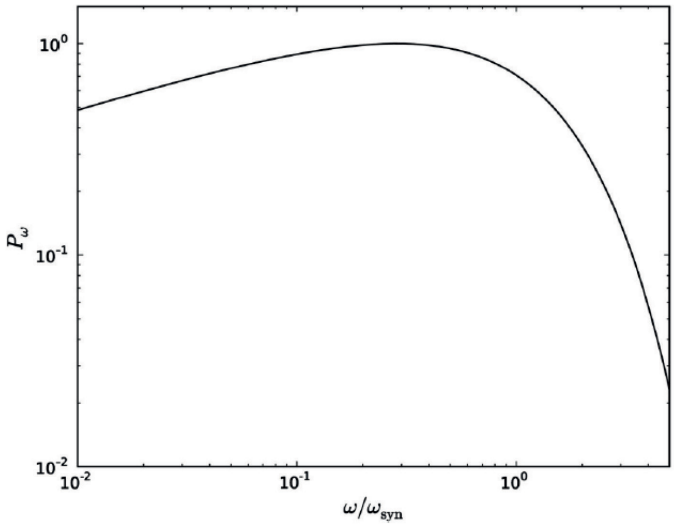
A relativisztikusan mozgó anyagcsomókban különböző folyamatok zajlanak le, aminek eredményeképpen gamma-sugárzás keletkezik. Jelentős mágneses tér esetén a relativisztikus elektronok

$$P_{szink} = \frac{2q^4 B^2 \Gamma^2}{3c^3 m_e^2} \tag{8}$$

teljesítménnyel sugároznak (szinkrotronsugárzás), itt q az elektron töltése, m_e a tömege, B a mágneses fluxussűrűség. Ennek a karakterisztikus körfrekvenciája

$$\omega_{szin} \approx \frac{qB\Gamma^2}{cm_e} \tag{9}.$$

Az ezzel kapcsolatos további részletek megtalálhatók Kumar és Zhang átfogó cikkében. [14] A 4. ábrán egy elektron szinkrotronspektruma látható. [15] Kis frekvencián a kitevő nagyjából egyharmad, míg nagy frekvencián egy erős exponenciális levágás van.

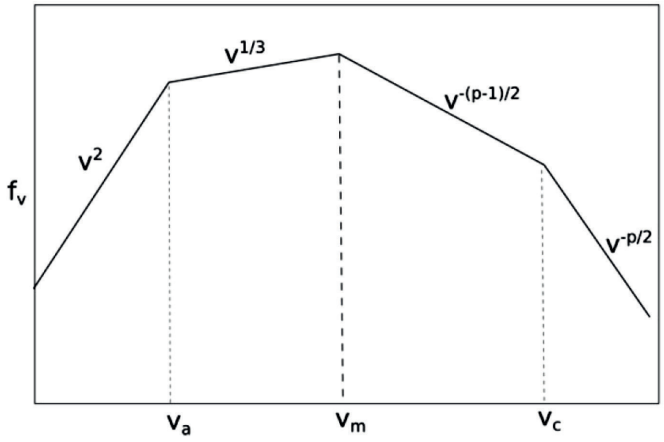


4. ábra – Az elektron szinkrotronspektruma [15]

A megfigyelhető gamma-spektrumokról Sari és társaitól olvashatunk jó összefoglalást. [16] Az ott levezetett szinkrotron hűlési frekvencia

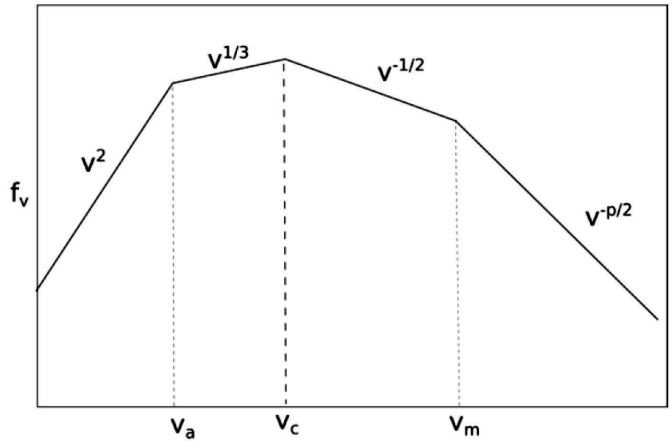
$$\nu_c = \frac{3qB\Gamma^2}{4\pi c m_e} \tag{10}$$

Itt Γ az elektronok termális Lorentz-faktora. Egy másik határfrekvencia (ν_a) amikor a fotonokra az inverz szinkrotronfolyamatból adódó elnyelés válik dominánssá. Amikor a minimális energiájú elektronokhoz tartozó frekvencia (ν_m) a fenti két frekvencia közötti érték, akkor a megfigyelt spektrum az 5. ábra szerinti. A $\nu_a < \nu_c < \nu_m$ esetben a gamma-spektrum a 6. ábra szerinti. [14]



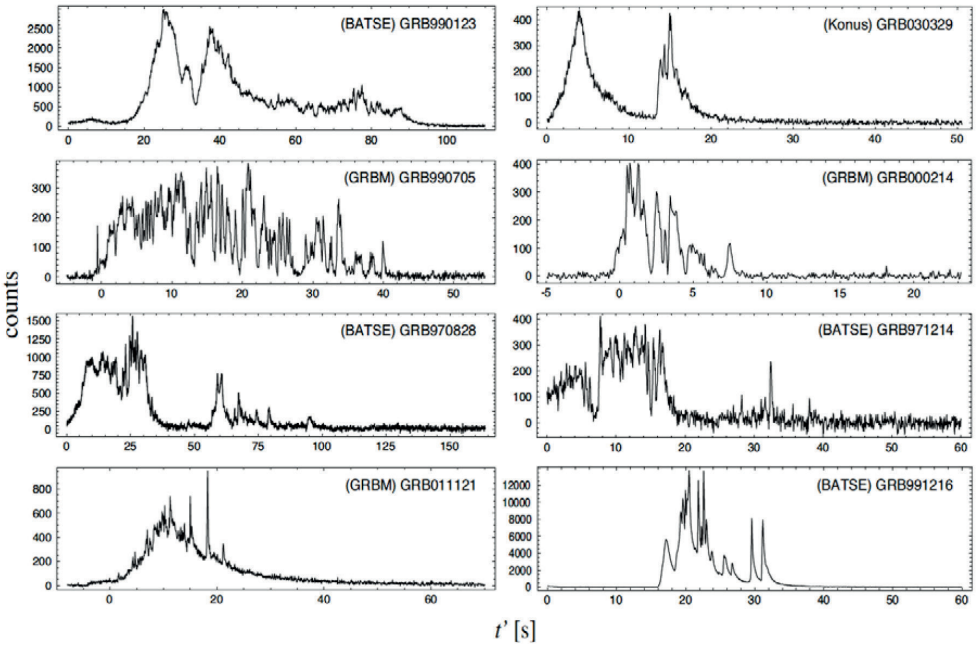
5. ábra – A gamma-spektrum $\nu_a < \nu_m < \nu_c$ esetén ([13] alapján saját szerkesztés)

Eredetileg azt gondolták, hogy egyedül a szinkrotronsugárzás segítségével is meg lehet magyarázni a gamma-kitörések spektrumát. A későbbi megfigyelések szerint az alacsony energiás spektrális indexek eloszlása nem egyezik meg a szinkrotronmodell jóslataival. Az ellentmondást úgy tudták feloldani, hogy feltételezték, hogy az alacsony energiájú fotonok inverz Compton-szórással növelik meg energiájukat. [17] [18] [19]



6. ábra – A gamma-spektrum $\nu_a < \nu_c < \nu_m$ esetén ([14] alapján saját szerkesztés)

A gamma-kitörések azonnali gamma-tartományban történő felfénylését csökkenő fluxussal csökkenő energiájú sugárzás követi. A 7. ábra mutat néhány gamma-tartománybeli fénygörbét.

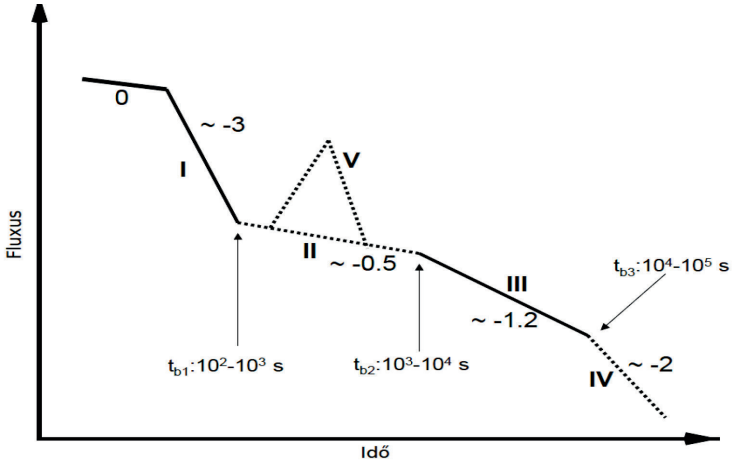


7. ábra – Gamma-kitörés fénygörbék [20]

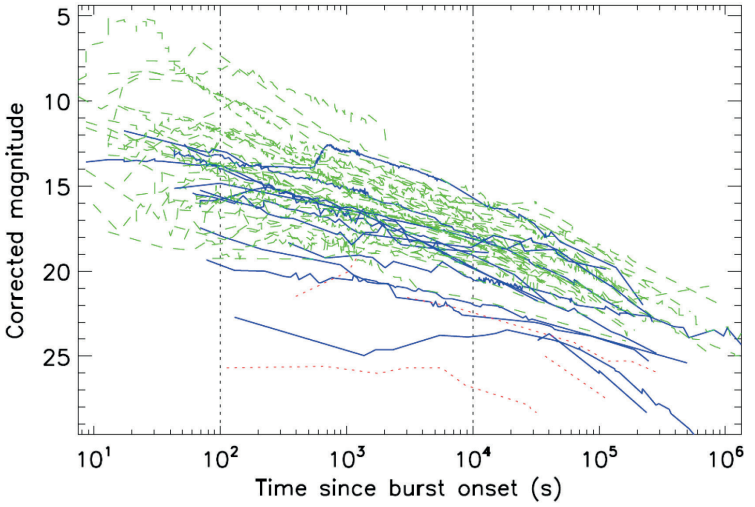
Megjegyzés: Vízszintesen az idő, függőlegesen a beütésszám van feltüntetve

A pár perces gamma-emissziót követi a röntgentartománybeli kisugárzás. Ennek kanonikus alakját mutatja a 8. ábra. Az azonnali gamma-felfénylés után az I. fázisban meredeken esik a fluxus (például a GRB 050126 és GRB 050219A esetében). Néhány esetben a röntgenfluxus esése megtörik, és egy kevésbé gyors plató (II. szakasz) következik (például GRB 050128, GRB 050315, GRB 050319 és GRB 050401). E két szakaszt a Swift műhold mérései alapján azonosították. Ezt követi a már régebben felfedezett III. szakasz, amelyet körülbelül –1,2 kitevőjű hatványfüggvény szerinti csökkenés jellemez. Ritkán a röntgenutófény végén egy gyorsabb elhalványulás (IV. szakasz) figyelhető meg (például GRB 050315). [21] Ez megfelel a később tárgyalandó jettörésnek. [22] A II. szakasz alatt megfigyelhető esetleges kitöréseket röntgenflereknek nevezzük (V. szakasz).

A röntgensugárzásban az itt tárgyalt egyes szakaszok ki is maradhatnak, illetve akár többszöri felfénylések is jelentkezhetnek. Ilyen röntgenflereket figyeltek meg például a következő kitörések esetében GRB 050406, GRB 050202B, GRB 050724, GRB 050502B, GRB 050724, GRB 050406, GRB 050202B, GRB 011121. [23] [24]



8. ábra – A gamma-kitörések röntgensugárzásának alakja Zhang és társai sematikus ábrája alapján [23]



9. ábra – A gamma-kitörések utófényei a látható tartományban, ha mind z = 1 távolságra lenne [25]

Megjegyzés: A piros szín a 2 másodpercnél, a kék szín a 10 másodpercnél rövidebb, a zöld szín pedig a 10 másodpercnél hosszabb kitöréseket jelöli

A néhány órás röntgenkibocsájtást több napig tartó ultraibolyában, látható fényben és rádiótartományban észlelhető utófénylés követi. Több tucat, látható fényben megfigyelt utófény fényességlefolyását láthatjuk az 9. ábrán de Ugarte Postigo és társai cikke alapján. [25]

A jetbreak utáni hatványkitevő a hűlésnek megfelelő halványodás szerinti. A törés előtti görbe kevésbé meredek, hiszen egyre több és több sugárzó, bár gyorsan hűlő anyag sugárzását figyeljük meg. [26] A fent leírt folyamat nem függ a sugárzás energiájától, azaz színétől, így a különböző hullámhosszakon felvett fénygörbék azonos időpontban, egyidejűleg szenvedik el a törést. A megfigyelések ezt több esetben igazolták.

Felhasznált irodalom

[1] Bouchet, L.: A comparative study of deconvolution methods for gamma-ray spectra. *Astronomy and Astrophysics Supplement,* Volume 113, 1995, 167–183.

[2] Pendleton, G. N. – Paciesas, W. S. – Mallozzi, R. S. – Koshut, T. M. – Fishman, G. J. – Meegan, C. A. – Wilson, R. B. – Horack, J. M. – Lestrade, J. P.: The detector response matrices of the burst and transient source experiment (BATSE) on the Compton Gamma Ray Observatory. *Nuclear Instruments and Methods in Physics Research A,* Volume 364, 1995, 567–577.

[3] Kahn, S. M. – Blissett, R. J.: The direct deconvolution of X-ray spectra. *Astrophysical Journal, Part 1,* Volume 238, 1980, 417–431.

[4] Hanka L.: A Gamma-spektrumok kiértékelésének matematikai módszerei: Regularizációs módszerek. *Bolyai Szemle,* 17. évf. 3. szám, 2008, 33–54.

[5] Backus, G. E. – Gilbert, J. F.: Uniqueness in the Inversion of Inaccurate Gross Earth Data. *Royal Society of London Philosophical Transactions Series A,* Volume 266, 1970, 123–192.

[6] Loredo, T. J. – Epstein, R. I.: Analyzing gamma-ray burst spectral data. *The Astrophysical Journal,* Volume 336, 1989, 896–919.

[7] Phillips, D. L.: A technique for the numerical solution of certain integral equations of the first kind. *Journal of the Association for Computing Machinery,* Volume 9, 1962, 84–97.

[8] Twomey, S.: On the numerical solution of Fredholm integral equations of the first kind by inversion of the linear system produced by quadrature. *Journal of the Association for Computing Machinery,* Volume 10, 1963, 97–101.

[9] Bagoly, Z. et al.: Searching for electromagnetic counterpart of LIGO gravitational waves in the Fermi GBM data with ADWO. *Astronomy and Astrophysics,* Volume 593, 2016, 4.

[10] Kaneko, Y. – Preece, R. D. – Briggs, M. S. – Paciesas, W. S. – Meegan, C. A. – Band, D. L.: The Complete Spectral Catalog of Bright BATSE Gamma-Ray Bursts. *The Astrophysical Journal Supplement Series,* Volume 166, 2006, 298–340.

[11] Preece, R. D. – Briggs, M. S. – Mallozzi, R. S. – Pendleton, G. N. – Paciesas, W. S. – Band, D. L.: The BATSE Gamma-Ray Burst Spectral Catalog. I. High Time Resolution Spectroscopy of Bright Bursts Using High Energy Resolution Data. *The Astrophysical Journal Supplement Series,* Volume 126, 2000, 19–36.

[12] Band, D. – Matteson, J. – Ford, L. – Schaefer, B. – Palmer, D. – Teegarden, B. – Cline, T. – Briggs, M. S. – Paciesas, W. – Pendleton, G. – Fishman, G. J. – Kouveliotou, C. – Meegan, C. – Wilson, R. – Lestrade, P.: BATSE observations of gamma-ray burst spectra. I – Spectral diversity. *Astrophysical Journal,* Volume 413, 1993, 281–292.

[13] Balázs L. G. – Horváth, I. – Kelemen, J.: Gammakitörések. *Fizikai Szemle,* 11, 2011, 371–377.

[14] Kumar, P. – Zhang, B.: The Physics of Gamma-Ray Bursts and Relativistic Jets. *Physics Reports,* Volume 561, 2015, 1–109.

[15] Rybicki, G. B. – Lightman, A. P.: *Radiative Processes in Astrophysics*. Wiley-VCH, 1986.

[16] Sari, R. – Piran, T. – Narayan, R.: Spectra and Light Curves of Gamma-Ray Burst Afterglows. *The Astrophysical Journal,* Volume 497, Issue 1, 1998, L17–L20.

[17] Piran, T.: The physics of gamma-ray bursts. *Reviews of Modern Physics,* Volume 76, Issue 4, 2004, 1143–1210.

[18] Piran, T. – Sari, R. – Mochkovitch, R.: Prompt emission from gamma-ray bursts. In Kouveliotou, C. – Wijers, R. A. M. J. – Woosley, S. szerk.: *Gamma-Ray Bursts.* Cambridge University Press, Cambridge, 2012, 121–149.

[19] Rácz, I. I. et al.: Statistical properties of Fermi GBM GRBs' spectra. *Monthly Notices of the Royal Astronomical Society,* Volume 475, 2018, 306–320.

[20] Borgonovo, L. – Frontera, F. – Guidorzi, C. – Montanari, E. – Vetere, L. – Soffitta, P.: On the temporal variability classes found in long

gamma-ray bursts with known redshift. *Astronomy and Astrophysics,* Volume 465, 2007, 765–775.

[21] Vaughan, S. et al.: Swift Observations of the X-Ray-Bright GRB 050315. *The Astrophysical Journal,* Volume 638, Issue 2, 2006, 920–929.

[22] Mészáros, P. – Wijers, R. A. M. J.: Basic gamma-ray burst afterglows. In Kouveliotou, C. – Wijers, R. A. M. J. – Woosley, S. szerk.: *Gamma-Ray Bursts.* Cambridge University Press, Cambridge, 2012, 151–167.

[23] Zhang, B. – Fan, Y. Z. – Dyks, J. – Kobayashi, S. – Mészáros, P. – Burrows, D. N. – Nousek, J. A. – Gehrels, N.: Physical Processes Shaping Gamma-Ray Burst X-Ray Afterglow Light Curves: Theoretical Implications from the Swift X-Ray Telescope Observations. *The Astrophysical Journal,* Volume 642, Issue 1, 2006, 354–370.

[24] Burrows, D. N. – Falcone, A. – Chincarini, G. – Morris, D. – Romano, P. – Hill, J. E. – Godet, O. – Moretti, A. – Krimm, H. – Osborne, J. P. – Racusin, J. – Mangano, V. – Page, K. – Perri, M. – Stroh, M. – Swift XRT Team: X-ray flares in early GRB afterglows. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* Volume 365, Issue 1854, 2007, 1213–1226.

[25] de Ugarte Postigo, A. – Horváth, I. – Veres, P. – Bagoly, Z. – Kann, D. A. – Thöne, C. C. – Balázs, L. G. – D'Avanzo, P. – Aloy, M. A. – Foley, S. – Campana, S. – Mao, J. – Jakobsson, P. – Covino, S. – Fynbo, J. P. U. – Gorosabel, J. – Castro-Tirado, A. J. – Amati, L. – Nardini, M.: Searching for differences in Swift's intermediate GRBs. *Astronomy and Astrophysics,* Volume 525, id. A109, 2011.

[26 Perez-Ramirez, D. et al.: Detection of the ultra-high z short GRB 080913 and its implications on progenitors and energy extraction mechanisms. *Astronomy and Astrophysics,* Volume 510, Paper A105, 2010.

The Gamma Inverse Spectral Problem

István Horváth

Until the discovery of their afterglow in 1997, the gamma ray bursts were only observed in the gamma band. The bursts' distance were unknown, they lasted only a few minutes, therefore their studies could only be limited to their light curve and the energy distribution (spectrum) of the detected photons. In this paper I review the spectral studies of this gamma range.

Keywords: astrophysics, gamma-ray astronomy, gamma-ray bursts, research satellites

Fatalin Dóra –
Fatalin László

Szabályos ellenállásrácsok egyszerűsített számításaihoz

Az elmúlt évtizedekben több javaslat is született olyan trükkös feladatok bevezetésére a villamosságtani alapképzésbe, amelyek tanulságosak lehetnek az alaptörvények és számítási módszerek mélyebb tartalmi megalapozásában, és egyben problémamegoldó kihívást is jelenthetnek a jobb hallgatók számára. Ez a cikk a passzív hálózatokhoz javasolt szabályos ellenállásrácsokra vonatkozó feladatokat és elemi megoldási módszereiket tekinti át és bővíti ki. E rendszerezés eredményeként logikailag és didaktikailag megalapozottabb következtetések vonhatók le az egyes feladattípusok alkalmazhatóságáról. A tárgyalás során néhány olyan gyakorta elkövetett elvi hibára is fény derül, ami fogalmi káoszt okozhat, miközben az ötlet alkalmazhatósági korlátaira vonatkozó információk elvesznek.

Kulcsszavak: szabályos rácsok, szimmetrikus hálózatok, homogén hálózatok, izotróp hálózatok, létrahálózatok, prizmahálózatok, tóruszrácsok

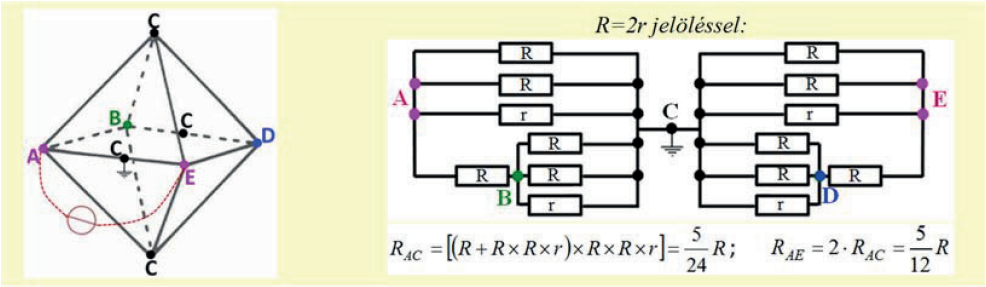
Mindig a részletek a legizgalmasabbak.
Pablo Picasso

A passzív hálózatokra vonatkozó szokványos alapfeladatok (soros, párhuzamos, vegyes ellenálláshálózatok) tárgyalása hagyományosan a csillag–delta átalakítással egészül ki a villamosságtani alapképzésekben. A cikk első része az ezen módszereket meghaladó feladatokat és elemi megoldási módszereiket ismerteti konkrét, didaktikailag felépített feladatsoron keresztül, ami alapot ad az egyes feladattípusok és megoldási módszereik egzaktabb jellemzéséhez.

Szimmetrikus, illetve homogén és izotróp hálózatok

Klasszikus feladat az egyforma ellenállásokból álló szabályos poliéder-élváz két szomszédos csúcsa közti eredő ellenállás számítása, ami többféle megoldás tanulmányozására is alkalmas.

Az egyik módszer a szomszédos *AE* pontokra mint passzív kétpólusra feszültségforrást képzel, és a (tükör)szimmetria alapján meghatározza az ekvipotenciális pontokat, amikkel a hálózat soros/párhuzamos kapcsolásokra egyszerűsíthető. (Többnyire a szimmetrikus felbontás elve is használható.) Az 1. ábra e megoldás menetét mutatja az oktaéder példáján keresztül.[1]



1. ábra – Oktaéder szomszédos csúcsai közti ellenállás meghatározása szimmetriaelvvel

Egy másik megoldás a hálózat homogén izotróp tulajdonságára épít, és a szuperpozíció elvét alkalmazza eredeti módon. Jelölje a csúcsok számát *n,* az egy csúcsból induló élek számát pedig *k*. A szomszédos *A* és *B* csúcsok közti ellenállás számítható a 2. ábrán látható módon:

a) Először vezessünk be az *A* pontba *(n–1)* × *I* nagyságú *áramot, a többi (n–1)* csúcsból pedig ki *I* nagyságú *áramot*.[2] Az izotrópia miatt az *A* csúcsból minden szomszédos csúcs felé *(n–1)I/k áram folyik, így az A* csúcs és a szomszédos csúcsok *közti* feszültség *(n–1)IR/k*.

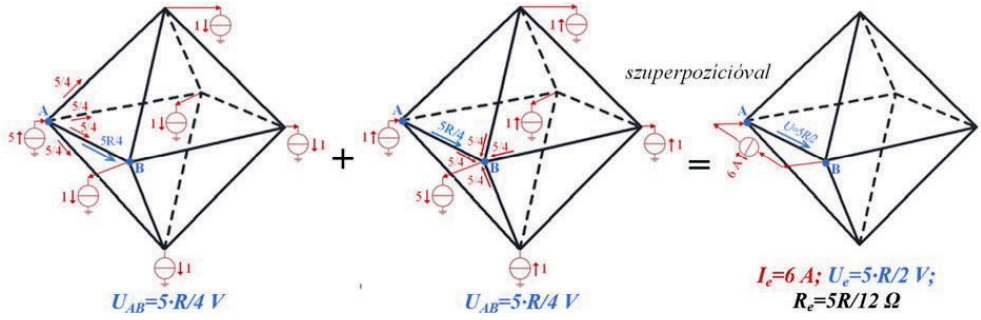
b) Másodszor vezessünk ki a *B* csúcsból *(n–1)* × *I áramot, a többi (n–1)* csúcsba pedig be *I* áramot. (Ez is realizálható!) Az izotrópia okán a *B* csúcsba minden szomszédos csúcstól *(n–1)I/k áram folyik, így egy szomszédos csúcs és a B* csúcs közti feszültség *(n–1)IR/k*.

c) A szuperpozíció elvét alkalmazva az *A* csúcsba $I_e = n \times I$ eredő *áram folyik be, ami a B* csúcsból folyik ki, a többi csúcsba pedig nem folyik sem be, sem ki áram, míg az *AB* pontok közti eredő feszültség $U_e = 2(n–1)IR/k$, *így* az eredő ellenállás:

$$R_e = \frac{U_e}{I_e} = \frac{2(n-1)}{n \cdot k} R$$

[1] A szimmetriaelvű megoldások elsősorban a csomópont fogalmi tartalmának mélyebb megalapozását segítik elő, valamint a szimmetrikus felbontási módszer megismerését készítheti elő. [1]

[2] A csomóponti törvény betartása szükséges az áramkör realizálhatóságához!



2. ábra – Véges homogén és izotróp ellenállás-hálózat szomszédos csúcsai közti eredő ellenállás meghatározása az oktaéder példáján keresztül

A második megoldás használható minden *n* pontból álló homogén és *k* irányba izotróp ellenállásrács szomszédos csúcsai közti eredő ellenállásának számítására lineáris rendszer esetén.[3]

Érdemes meggondolni, hogy milyen *n* és *k* értékek mellett létezik homogén rács. Ennek szükséges feltétele: $2 \le k \le n-1$, ugyanis egy csúcsból legfeljebb az összes többi $(n-1)$ csúcshoz futhat él, a $k = 2$ határesetet pedig megvalósítja a síkbeli szabályos *n*-szög gráfja. Ekkor az ellenállások száma *n* és $R_e = (n-1)R/n$.[4] A $k = n-1$ határesetet realizálja a teljes gráf, amelynél egy-egy ellenállás *köt össze* minden csúcsot minden csúccsal, azaz az élek száma $n \times (n-1) / 2$. Az utóbbi észrevétel felhívja a figyelmet arra, hogy egy $(n;k)$ értékpár mellett az összes él, azaz a felhasznált ellenállások száma $n \times k / 2$, így a rács realizálhatóságának szükséges feltétele, hogy az $n \times k$ szorzat páros legyen.[5] Az eddigi homogén rácsok közül a szabályos poliéderek és sokszögek rendelkeznek izotróp tulajdonsággal is. E feladatok sajátos általánosításai az úgynevezett végtelen(ített) $(n \to \infty)$ homogén izotróp rácsok, amelyekről a későbbiekben lesz szó.

[3] E feltétel biztosítja a szuperpozíció elvének használhatóságát. [2] A továbbiakban csak lineáris rendszerről és összefüggő (rezisztív, illetve reaktáns elemekre) épülő rácsokról lesz szó.

[4] Az elemi levezetés szerint itt az *A* és *B* csúcsok közti *R* ellenállással párhuzamosan kapcsolódik sorosan kötött $(n-1)$ darab *R* ellenállás, így az eredő ellenállás számolható replusszal: $R_{AB} = R \times [(n-1)R] = \frac{(n-1)}{n}R$. (A $k = 1$ esetben összefüggő gráfként csak egy szimpla kétpólus jöhet szóba, ami érdektelen, bár a képlet igaz.)

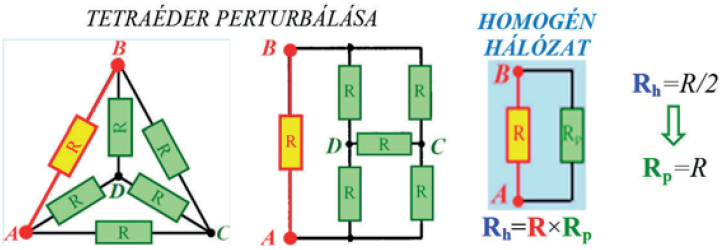
[5] Páratlan *n*-re nem valósulhat meg a $k = n-2$ eset, míg a $k = n-3$ esetet mindig realizálja a szabályos *n*-szög átlóinak gráfja. Nem nehéz belátni, hogy az $n \times k$ szorzat párossága a homogén rács realizálhatóságának elégséges feltétele, de egy homogén rács nem szükségszerűen izotróp tulajdonságú!

Homogén hálózatok variálásai

Az előző feladatok egy módosításaként az *AB* pontok közti *R* ellenállás törlődik a többi rész változatlanul hagyása mellett.[6] (3. ábra) A rács homogenitása és izotrópiája ettől megszűnik, de ez a perturbált eset elemi úton megoldható a következő (fordított) okoskodással:

A perturbált esetből (R_p) úgy kapható meg az eredeti homogén eset (R_h), hogy az AB pontok közé párhuzamosan bekötünk egy R ellenállást, így $R_h = R \times R_p$, amiből

$$R_p = \frac{R \cdot R_h}{R - R_h} = \frac{2(n-1)}{n \cdot (k-2) + 2} R.$$

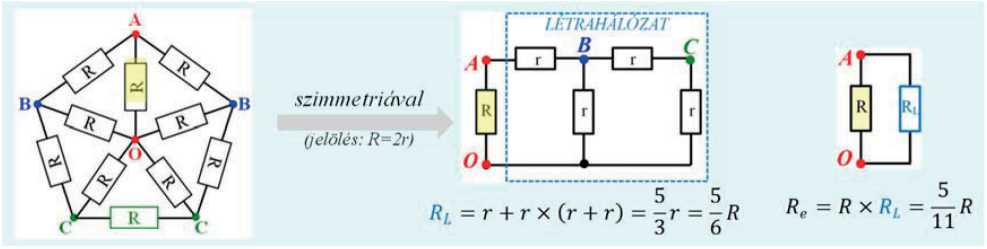


3. ábra – A perturbált eset számítása a tetraéder példáján keresztül

Egy szabályos sokszögrácshoz kapcsolható egy újabb *O* pont úgy, hogy e pontot egy-egy *R* ellenállás köti össze minden eredeti rácsponttal. (4. ábra) E rács is szimmetrikus, de homogenitása *n* > *3* esetén a kitüntetett *O* pont miatt megszűnik. Az *O* pont és egy eredeti *A rácspont közti eredő ellenállás* visszavezethető az úgynevezett *létrahálózatok eredő ellenállásának meghatározására* a következő meggondolással:

A rács szimmetriája alapján az ekvipotenciális pontok miatt a hálózat ekvivalens egy AO pont közti létrahálózattal (R_L) párhuzamosan kapcsolódó (az A és O pontot közvetlenül összekötő) R ellenállás eredőjével, így $R_e = R \times R_L$. (4. ábra)

[6] A levezetés érvényességéhez szükséges, hogy e szakadás után is összefüggő maradjon a gráf! A 4. ábrán látható, hogy a tetraédernél e szakadás utáni eredmény éppen a hídkapcsolás.



4. ábra – Egy szimmetria elvű számítás az eredő ellenállás meghatározására

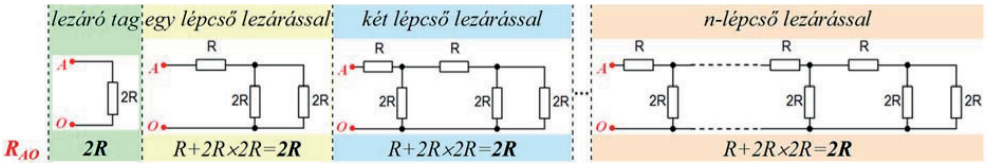
A létrahálózatok sajátos kezelési módszerei tanulságosak, ezért érdemes külön foglalkozni ötletes számítási módszereivel.

Létrahálózatok

A létrahálózatok közül részben meglepő eredménye, részben széles körű alkalmazása okán közkedvelt az 5. ábra úgynevezett lezárásos létrahálózata.[7] Rekurzív módszerrel könnyű belátni, hogy egy ilyen *n*-lépcsős létrahálózathoz $(R_{L,n} = 2R)$ egy újabb lépcsőt kapcsolva az eredő ellenállás:

$$R_{L,n+1} = R + (2R) \times R_{L,n} = R + (2R) \times (2R) = 2R,$$

azaz az eredő ellenállás értékét *nem befolyásolja* a lépcsők száma.

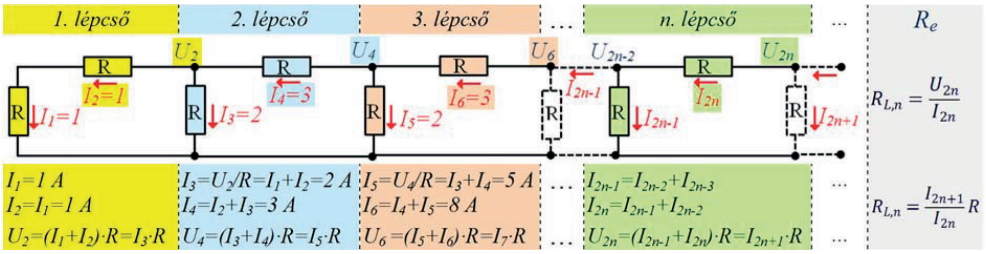


5. ábra – Lezárásos létrahálózat eredő ellenállása

A 4. ábra létrahálózatára az eredő ellenállás egyszerűen felírható: $r_L = r + r \times (r + r)$, de hosszabb létrahálózat esetén az $r_{L,n} = r + r \times r_{L,n-1}$ rekurzív képlet alkalmazása már gondot jelent, ugyanis egy (nemlineáris) rekurzióval adott sorozat *n*-ik tagjának explicit felírása nem része a matematika alapkurzusoknak. A rekurzív eljárást egyszerűbb fiktív áram-, illetve feszültségértékekkel végezni, mert így a rekurziós formulák lineárisak, sőt

[7] Különösen kedvelt megoldás a D/A átalakítókban. [3]

a kezdőérték is szabadon választható. A 6. ábra mutatja be e számolás menetét a vizsgált létrahálózatra $I_1 = 1\ A$ mellett. *(A valós feszültség- és árameloszlás jól számolható egy* $U_{tény}/U_{fiktív}$ *faktorral történő szorzással!)*



6. ábra – Létrahálózat belső áramainak és csomóponti feszültségeinek számítási módszere[8]

Ha az n-edik R ellenállás áramát I_n*, a (két ellenállásonként fellépő) csomópontokat pedig* U_{2n} *jelöli, akkor a rekurziós képlet:* $I_n = I_{n-1} + I_{n-2}$ *és* $U_{2n} = I_{2n+1} \times R = (I_{2n-1} + I_{2n}) \times R$*, míg az n-edik lépcsőn a feszültség* $U_{2n} = I_{2n+1} \times R$*, a befolyó áram* I_{2n}*, azaz az eredő ellenállás:*

$$R_{L,n} = \frac{I_{2n+1}}{I_{2n}} R$$

Szimmetrikus és homogén létrahálózatok

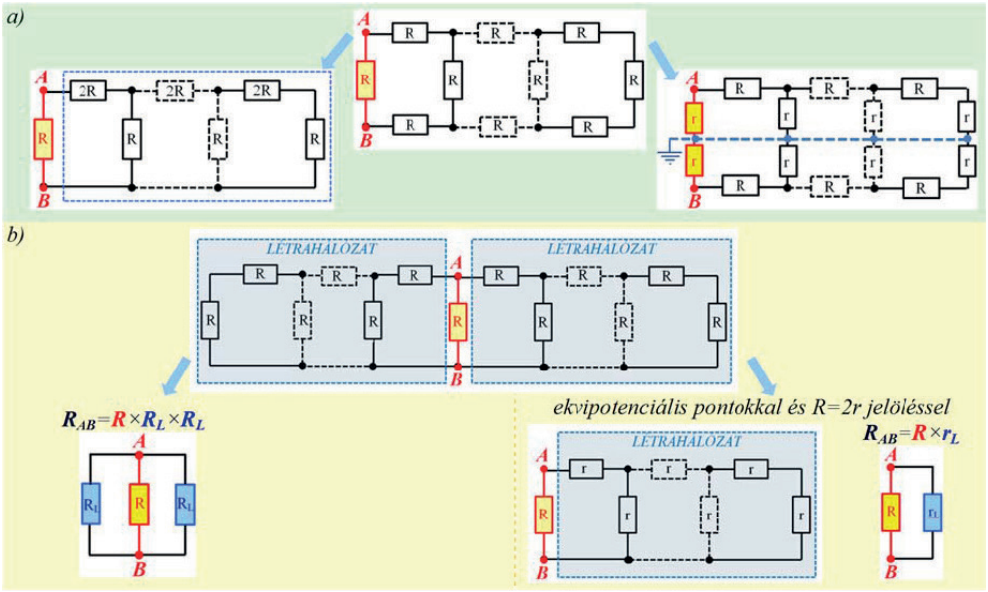
Az eddigi létrahálózatok nem rendelkeztek sem szimmetria-, sem homogén, sem izotróp tulajdonsággal, de variálásukkal különböző szimmetrikus hálózatok állíthatók elő. A 7/a. ábra hálózata például az *AB* szakaszfelező-merőlegesre szimmetrikus, ezért kétféle ekvivalens átalakítással is egyszerűsíthető.[9]

[8] Itt az I_n éppen a jólismert Fibonacci-sorozat, ami az úgynevezett Binet-formulával zárt alakba is felírható:

$$I_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{\sqrt{5}\cdot 2^n}, \quad \text{azaz} \quad R_{L,n} = \frac{I_{2n+1}}{I_{2n}} = 2\cdot\frac{(1+\sqrt{5})^{2n+1} - (1-\sqrt{5})^{2n+1}}{(1+\sqrt{5})^{2n} - (1-\sqrt{5})^{2n}}\cdot R,$$

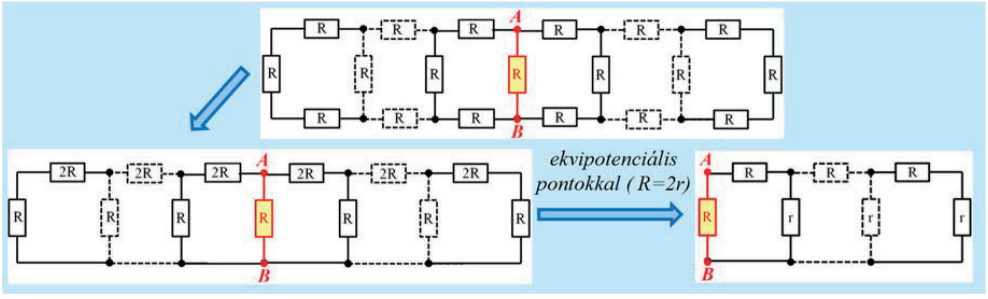
de nem előnyös e képlet használata, mert a kerekítési hibák halmozódása miatt hamis eredményre vezethet.

[9] Fontos, hogy az első megoldás ekvivalens hálózatában a *B* pont mindvégig jelenlevő közös földponttá válik!



7. ábra – Egy szimmetrikus létrahálózat és ekvivalens átalakításai

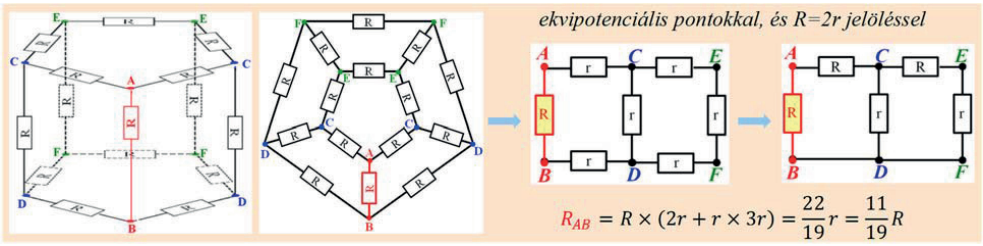
A 7/b. ábra létrahálózata az *AB* tengelyre szimmetrikus, így e passzív hálózat az (*AB* pontokat közvetlenül összekötő) *R* ellenállással két párhuzamosan kapcsolódó létrahálózatból (R_L) áll, *így* az eredő ellenállás: $R_{AB} = R \times R_L \times R_L$. (Az ábrán látható, hogy az eredő ekvipotenciális pontok segítségével is számítható.) A 8. ábra szabályos rácsa mindkét szimmetriával rendelkezik, így azok átalakítási módszereivel az ábrán látható ekvivalens hálózat adódik eredményül.



8. ábra – Szimmetrikus létrahálózatok és ekvivalens átalakításaik

Az előző szimmetrikus hálózatok a határpontjaik miatt biztosan nem homogének, de e határpontok eltüntethetők például a 7/a. ábra szimmetrikus létrahálózat két-két

végpontjának rövidre zárásával, azonosításával, ami már véges homogén rácsot eredményez.[10] (Az ötszög prizma szimmetria elvű számítása látható a 9. ábrán.)



9. ábra – Az ötszög prizma és síkbeli változata mint véges homogén hálózat ekvivalens átalakításai

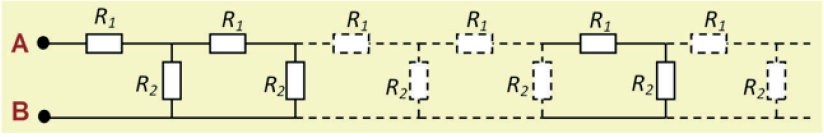
Végtelen(ített) passzív hálózatok

A létrahálózatok végtelenítése a határpontok eltűnését jelenti, ami lehetőséget ad újabb homogén rácsok konstruálására. A végtelenítés formailag az $R_{L,n}$ sorozat $(n\to\infty)$ határértékének a megállapítását jelenti. Az 5. ábra lezárásos létrahálózatának az eredő ellenállása a lépcsők számától függetlenül $2R$, így ennek a határértéke is nyilván $2R$.

A 10. ábra általánosabb létrahálózatának végtelenítésekor egyszerűen felírható az $R_{L,n}$ sorozatot leíró rekurziós képlet, ami a sorozat explicit alakjának előállítása nélkül is lehetőséget nyújt a határérték egyszerű kiszámítására az alábbi meggondolással:

Egy végtelen lánc R_e eredő ellenállása nem változik meg, ha a bemenetére még egy lépcső kapcsolódik. Ekkor *az R_e eredő ellenállású lánc egy R_2 ellenállással van párhuzamosan kötve, és az egészhez sorosan kapcsolódik még egy R_1 ellenállás is:*

$$R_e = R_1 + R_2 \times R_e = R_1 + \frac{R_2 \cdot R_e}{R_2 + R_e}.$$



10. ábra – Egy végtelen létrahálózat

[10] E konstrukció realizálható például a létrahálózat hengerre, esetleg Möbius-szalagra történő felvitelével. (A pontok azonosítása síkban is elvégezhető, amit mutat a 9. ábra.) Fontos észrevétel, hogy az így kapott rács többnyire továbbra sem lesz izotróp! (A többnyire jelző csak a kocka miatt szükséges!)

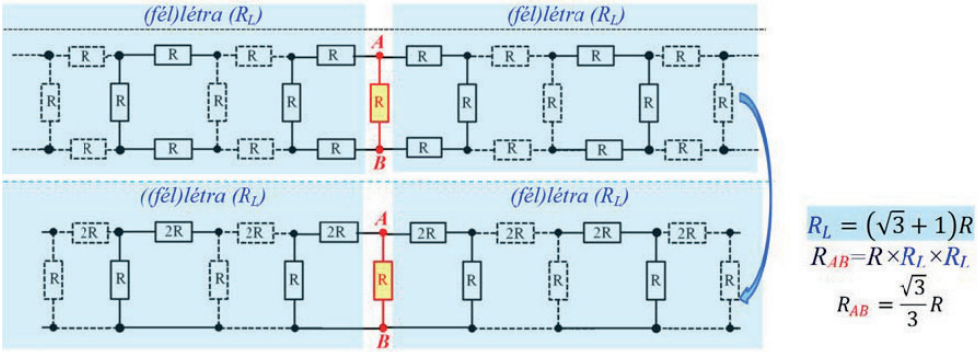
E másodfokúra vezető egyenletből az R_e eredő ellenállás kifejezhető, amelyből itt csak a pozitív gyöknek van fizikai értelme:

$$R_e = \frac{R_1 + \sqrt{R_1^2 + 4R_1R_2}}{2}.$$

Ez a képlet a 6. ábra $R_1 = R_2$ létrahálózatára éppen a Fibonacci-sorozat határértékét adja:

$$R_e = \frac{1+\sqrt{5}}{2}R.$$

A 8. ábra szimmetrikus rácsának végtelenítése homogén hálózatot eredményez.[11] Az AB pontok közti R ellenállással párhuzamosan kapcsolódó két (fél)rács eredője az $R_{AB} = R \times R_L \times R_L$ képlettel számítható, ahol a 11. ábrán látható ekvivalens átalakítással a végtelenített (fél) létra ellenállása $R_L = (\sqrt{3}+1)\,R$, ezért e homogén rács eredő ellenállása: $R_{AB} = \frac{\sqrt{3}}{3}R$.



11. ábra – 1-dimenzió szerint végtelen(ített) homogén rács

A végtelen homogén (k-irányba) izotróp rácsokra formailag alkalmazva a határértékképzést kimondható a következő megállapítás:

$$R_e = lim\,\frac{2(n-1)}{}R = \frac{2}{}R.$$

E formailag elegáns levezetés szerint az elemi úton megoldható feladatokhoz besorolhatóak a 12. ábra végtelen homogén izotróp rácsai is.

[11] A végeredmény is mutatja, hogy ez a homogén hálózat sem izotróp, hiszen akkor az eredmény $\frac{2}{3}R$ lenne!

rácstípus	hatszögrács	négyzetrács	háromszögrács	kockarács
izotrópia–szám (k)	3	4	6	6
szomszédos pontok közti eredő ellenállás	2R/3	R/2	R/3	R/3

12. ábra – Többdimenziós végtelen homogén rácsok

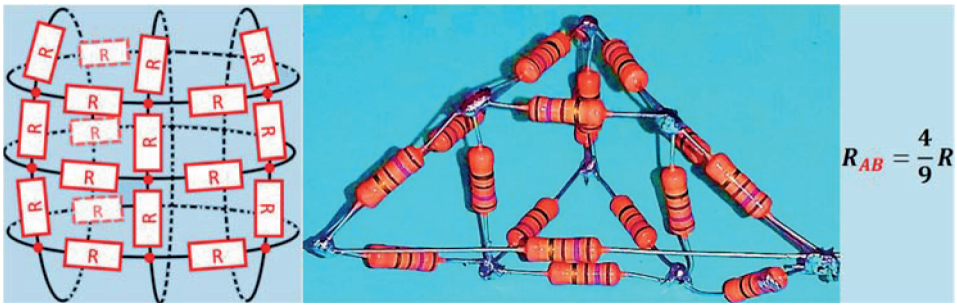
Többdimenziós végtelen ellenállásrácsok és a határértékképzés

Bár a 12. ábrán szereplő eredmények helytállóak, ám meggyőzően elegáns levezetésük némileg hiányos, ugyanis a szabályos ellenállásrácsok végtelenítése során a formálisan alkalmazott határértékképzésről elmondható, hogy a $k > 2$ esetekre[12] véges homogén izotróp hálózatként csak az öt platóni test közismert, így az $n \to \infty$ határérték-képzési folyamat *ismeretlen, netán nem létező* hálózatokon keresztül történik, ami erősen megkérdőjelezi a határértékképzés alkalmazhatóságát![13] A fenti érveléshez illene még valószínűsíteni, hogy bármilyen nagy n-re is létezik n-nél több rácspontból álló véges homogén izotróp hálózat. Ez egy nem túl egyszerű gráfelméleti kérdés. Egy $n \times n$-es négyzetrács tóruszra történő felvitelével persze konstruktív módon valószínűsíthető,[14] hogy kellően nagy véges szabályos rácsok is léteznek, valamint három- és hatszögráccsal is meggondolható e konstrukció, de a formulát még ekkor is ki kell egészíteni a $k \to \{2;3;4;6\}$ megszorítással! (13. ábra)

[12] A $k = 2$ esetet minden n-re realizálja a szabályos n-szög gráfja, ami 2-irányú izotrópiával rendelkező homogén hálózat, így a határértékképzés elvégezhető, és a triviálisan érdektelen ($R_{AB} = R$) eredményt adja.

[13] Az extenzióját tekintve üres fogalmakkal logikailag bármi (így az ellentéte is) igazolható, mert a semmire vonatkozó állítás ellenpéldával cáfolhatatlan. Az üres fogalmak nem kaphatnak szerepet a tudományos vizsgálatokban! [4]

[14] A tórusz topológiailag két körvonal Descartes-szorzataként származtatható. Az itt alkalmazott konstrukció pedig az $n \times n$-es négyzetrács két-két szemben fekvő oldalpárjának azonosításával az $(n-1) \times (n-1)$-es tóruszrácsot építi fel, aminél az ellenállás-élek száma $2(n-1)^2$, és így az eredő ellenállása: $R_e = \frac{n(n-2)}{2(n-1)^2} R$.



13. ábra – Egy homogén izotróp 3 × 3-as tóruszrács

Többen a véges esetnél követett levezetést alkalmazzák a végtelen négyzetrácsra, ám logikailag ezek is hibásak/hiányosak. E levezetések két tipikus példája a következő:

- Az egyik megoldás felvesz *„egy n × n-es négyzetrácsot periodikus határfeltétellel”,* [5] és ennek *A* pontjába vezet be *I,* és minden pontjából ki I/n^2 áramot, majd a *B* pontjából ki *I,* és minden pontjába be I / n^2 áramot, majd szuperponálja a két esetet. Ez minden *n*-re realizálható, így képezhető az $n\to\infty$ *határérték*. E meggondolás alaphibája, hogy az egyes véges esetekben *az A és B pont nem lehet egyidejűleg izotróp, így a levezetés is csak közelítő jelleggel bírhat. (Zavaró a tisztázatlan „periodikus határfeltétel” kifejezés szerepeltetése is, ami csak az általános egzakt matematikai megoldás ismeretében érthető. E problémák kikerüléseként a levezetés az előzőekben leírt tóruszra feltekert négyzethálóra végezhető.)*
- Egy másik megoldás [6] egy-egy olyan $+I$ illetve $-I$ áramgenerátorral táplálja meg a végtelen rács *A*, majd *B* pontját, amelyek egy fiktív ⏚ földponthoz kapcsolódnak. E fiktív földpont realizálásaként a szerzők egy a (végtelenben levő) nullapotenciálú határvonalat jelölnek meg. A szuperpozíció elvével ezután a szokásos eredmény adódik, miközben a fiktív földpont is eliminálható.[15] Meg kell jegyezni, hogy ráadásként ezek *az áramgenerátorok végtelen feszültségűek,* mivel négyzetrácsnál $R_{A\downarrow} = \infty$.[16]

[15] A ⏚ fiktív földpont formailag ugyan megoldja a problémát, ám létezésével gondok vannak, azaz ebben a kontextusban ez is egy üres fogalmon keresztüli bizonyítás!

[16] Az $R_{A\downarrow}$ úgy becsülhető, hogy az *A* pont körüli koncentrikus négyzetek pontjait közel ekvipotenciálisnak tekintve az egyes szinteket rendre *4; 12; 20;…; (8n-1);…* ellenállás–ág köti össze, így az eredő ellenállás:

$$R_{A\downarrow} \approx \frac{R}{4} + \frac{R}{12} + \frac{R}{20} + \cdots \frac{R}{8n-4} + \cdots = \frac{R}{4}\left(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1} + \cdots\right) = \infty.$$

Következtetések

A szimmetrikus hálózatok, a perturbáció, a létra- és prizmahálózatok rekurziós formulái, valamint ezek (1-dimenziós) végtelenítése széles kört biztosít olyan feladatok konstruálására, amelyek megoldási módszerei hasznosak lehetnek például a csomópont fogalmának elmélyítésében, a szimmetrikus felbontási elv megismerésében, míg a véges homogén izotróp hálózatok (például tóruszrácsok) eredeti számolása szép példát nyújt a szuperpozíció és a Kirchhoff-törvények sajátos alkalmazására. Az utóbbi elegáns megoldások indoklásai sajnos többnyire pontatlanul a SZIMMETRIA fogalmára támaszkodnak annak konkretizálása nélkül, hogy mely típusa, a középpontos, tengelyes, vagy síkra vonatkozó tükrözési, avagy a forgásszimmetria játszik-e éppen szerepet.[17] Ez különösen zavarba ejtő például a szabályos poliéderek és a homogén izotróp tóruszrácsok esetén!

A felhasznált fogalmak tisztázatlansága a megismerés adott fázisában természetes, amit híven tükröz Bohr következő eszmefuttatása:

„Ez a mosogatás is olyan, mint a nyelv. Piszkos a vizünk, piszkos a törlőruhánk, valahogy mégis megtisztítjuk az edényt meg a poharakat. Így állunk a nyelvvel is: tisztázatlan fogalmakkal dolgozunk, és olyan logikát használunk, amelynek nem ismerjük a pontos érvényességi körét; ennek ellenére reménykedünk, hogy mégiscsak tisztaságot teremtünk a természet megértésében." [8]

A szimmetria, a homogén és az izotróp tulajdonság kaotikus egyvelegének szerepeltetése csakúgy megengedhetetlen ma már, mint a véges-végtelen-határtalan fogalomhármas összemosása. A rácsok elegáns levezetései határozottan a rácspontok *irányfüggetlen (izotróp)* és *egymással ekvivalens (homogén)* tulajdonságára építenek. A homogén és izotróp tulajdonság fogalmának elkerülése egy homályos szimmetriafogalom használatával pedig nem pusztán értelemzavaró, hanem egyben ellehetetleníti a módszer korlátainak behatárolását is. Az izotróp–anizotróp és a homogén–inhomogén fogalmak szükségképpen megjelennek a villamosságtani alapok elsajátítása során is, ráadásul a homogén és izotróp tulajdonságok[18] a modern természettudományos világkép alapvető fogalmai, hiszen a kopernikuszi-fordulat nyomán mára primer alapfeltételezés a világegyetem szerkezetére a homogén és izotróp tulajdonság.[19]

A feladatkörök előzőekben tárgyalt bővítései a szokványos feladatmegoldó rutinok gyakorlása mellett már teret engednek a problémamegoldó készségek fejlesztésének is, ami jelentős motivációt jelenthet a jobb hallgatók számára.[20] A végtelen szabályos rácsok besorolása az elemi úton megoldható feladatok körébe azonban meggondolandó,

[17] A *k*-irányba izotróp rács esetén vélhetően a *k*-adrendű forgásszimmetriára gondolnak a szakirodalomban. [5] [6] [7]

[18] E tulajdonságok tudományáganként némileg eltérő tartalommal rendelkeznek, megnevezésüket az etimológia a görög *homo (azonos) + genosz (fajta),* illetve az *iso (egyenlő) + tropos (irány)* összetételre vezeti vissza.

[19] Pontosabban a tér-idő rendszerben csak a térszerű izotrópia érvényesül.

[20] További hasonló feladatvariációk találhatók: [1] [9] [10].

mert a vázolt problémák mellett a homogén (*k*-irányba) izotróp rácsok többdimenziós végtelenítése több rejtett fogalmi problémát is hordoz magában, amit mutat a többváltozós függvények határértékfogalma csakúgy, mint a parciális differenciálegyenleteknél a peremfeltételek szerepe. A többdimenziós végtelen szabályos ellenállásrácsok egzakt tárgyalási módszerei az elmúlt évtizedekben jelentős fejlődésen mentek át, amit a szakirodalma is mutat. A folytonos modellekben a kiindulási alapot a Laplace-egyenlet adja. A Laplace-egyenlet megoldásának relatíve egyszerű megoldási módszere a változók szétválasztásával történik, ami elvezet a Fourier-sorok alkalmazásához, illetve univerzálisan használhatók még a numerikus megoldási módszerek is.[21] Zombory (2008) pontosan vázolja e módszereket kitérve a *Dirichlet-*, illetve *Neumann*-peremfeltételekre is. [11] A folytonos modellt rácsgeometriára cserélve a Laplace-operátor diszkrét verziója jelenik meg, és mindkét előző módszer alkalmazható a megoldásokhoz. Atkinson és Steenwijk (1999) részletesen ismerteti a numerikus módszert négyzet-, kocka-, háromszög- és hatszögrácsra, [12] míg Cserti (2000) a Green-függvények felhasználásával mutatja be e problémakör kezelését. [13] A szakirodalom kitér a félvégtelen-rácsok, [14] és a hengerre, illetve toroidra felvitt szabályos rácsok számításaira is. [15]

A szabályos rácsok analóg problémája a véletlen bolyongások témaköre, amit átfogóan mutat be Lovász (1996), [16] így a szabályos rács vizsgálata sem pusztán különböző matematikai módszerek virtuóz alkalmazása, ugyanis több területen hasznosítható modelltípusról van szó. E témakör jelentősége dacára megfontolandó, hogy a végtelen szabályos rácsok egyszerűsített számításai milyen mértékben hasznosíthatóak az alapképzésben, ahol törekedni kell a tiszta logikai magyarázatok és az intuitív megfontolások, valamint az egzakt levezetések és a plauzibilis érvelések közti megfelelő egyensúlyra.

Irodalomjegyzék

[1] Fatalin L.: Szimmetrikus hálózatok számítási eljárásairól. *Bolyai Szemle,* 26. évf. 2. szám, 2017, 27–36. www.uni-nke.hu/document/uni-nke-hu/Bolyai_Szemle_2017_02_kesz.pdf (a letöltés ideje: 2018. 04. 01.)

[2] Fatalin L.: A lineáris hálózatok számítási eljárásairól. *Bolyai Szemle,* 25. évf. 4. szám, 2016, 58–70. http://uni-nke.hu/uploads/media_items/bolyai-szemle-2016-04.original.pdf (a letöltés ideje: 2018. 04. 01.)

[3] Pap L.: *Elektronika I.* 2013. www.mcl.hu/sites/default/files/Elektronika1_1.pdf (a letöltés ideje: 2018. 04. 01.)

[4] Fatalin L.: *Hierarchikus fogalmi struktúrák vizsgálata gráfokkal.* Debreceni Egyetem, 2008. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/85019/ertekezes_magyar.pdf?sequence=4 (a letöltés ideje: 2018. 04. 01.)

[5] Gáspár M. E.: *Végtelen ellenálláshálózatok számítása.* Eötvös Loránd Tudományegyetem, Budapest, 2002. www.kfki.hu/~merse/pdf/tdk.pdf (a letöltés ideje: 2018. 04. 01.)

[6] Osterberg, P. – Inan, A.: Calculation of the general impedance between adjacent nodes of infinite uniform N-dimensional resistive, inductive, or capacitive lattices. *American Society for Engineering Education Annual Conference and Exposition,* 2009, 17573–17580. www.researchgate.net/publication/253468340_Calculation_of_the_general_impedance_between_adjacent_nodes_

[21] A véges differenciák módszere például a vizsgált (sík)tartományt úgynevezett ekvidisztáns derékszögű rácscsal, azaz négyzetráccsal fedi le, és e rácspontokra adja meg a közelítő potenciált.

of_infinite_uniform_N-dimensional_resistive_inductive_or_capacitive_lattices (a letöltés ideje: 2018. 04. 01.)

[7] Hauer T. – Tóth I.: A KÖMAL 2286. fizika feladat megoldása. 1989/2, 84–86. http://db.komal.hu/KomalHU/showpdf.phtml?tabla=FelHivatkoz&id=39900 (a letöltés ideje: 2018. 04. 01.)

[8] Heisenberg, W.: *Der Teil und das Ganze.* R. Piper & Co. Verlag, München, 1969. (Magyarul: *A rész és az egész.* Gondolat, 1975.)

[9] Rácz L. – Bérces Gy.: *Elektromos ellenálláshálózatok.* 2010. http://users.atw.hu/fizkonf/program/proc/szekcio-poszter/RaczLilla.pdf (a letöltés ideje: 2018. 04. 01.)

[10] Csefkó Z.: *Egyenáramok – feladatok.* Fazekas Fizika, 2016. http://csefi.f.fazekas.hu/11bc-fakt/05-Egyen%C3%A1ramok-%C3%96t%C3%B6s%C3%A9rt.pdf (a letöltés ideje: 2018. 04. 01.)

[11] Zombory L.: *Elektromágneses terek.* Műszaki Kiadó, Budapest, 2008. http://mkkonyvkiado.hu/wp-content/uploads/2015/04/Dr_Zombory_Laszlo_Elektromagneses_terek.pdf (a letöltés ideje: 2018. 04. 01.)

[12] Atkinson, D. – van Steenwijk, F. J.: Infinite resistive lattices. *American Journal of Physics,* Volume 67, 1999, 486–492. www.researchgate.net/publication/2834057_Infinite_Resistive_Lattices (a letöltés ideje: 2018. 04. 01.)

[13] Cserti, J.: Application of the lattice Green's function for calculating the resistance of an infinite network of resistors. *American Journal of Physics,* Volume 68, 2000, 896–906. www.researchgate.net/publication/238984127_Application_of_the_lattice_Green%27s_function_for_calculating_the_resistance_of_an_infinite_network_of_resistors (a letöltés ideje: 2018. 04. 01.)

[14] Széchenyi G.: *Végtelen ellenállás-hálózatok vizsgálata Green-függvény segítségével.* 2009. http://fizweb.elte.hu/download/Fizika-BSc/!BSc-Szakdolgozatok/Szechenyi_Gabor_szakdolgozat.pdf (a letöltés ideje: 2018. 04. 01.)

[15] Jeng, M.: Random walks and effective resistances on toroidal and cylindrical grids. *American Journal of Physics,* Volume 68, 2000, 37–40. http://cds.cern.ch/record/738139/files/0405135.pdf (a letöltés ideje: 2018. 04. 01.)

[16] Lovász, L. (1996): Random Walks on Graphs: A Survey. In *Combinatorics. Paul Erdős is Eighty,* Vol. 2. János Bolyai Mathematical Society, Budapest, 353–398.

For Simplified Calculation Procedures of Isotropic Resistance Lattices

Dóra Fatalin – László Fatalin

Over the past decades more proposals were created for introduction of tricky tasks in the electrotechnical education, which can be instructive in deeper understanding the basic laws and calculation methods and it can be also a challenge for the better students to solve unusual problems. This article systematizes and extends the tasks and basic solution methods for passive networks. As a result of this systematization logically and didactically more grounded conclusions can be deducted from the applicability of each task types. This examination also reveals errors which can cause conceptual chaos, meanwhile the usability limits of the idea is lost.

Keywords: regular and symmetrical networks, homogeneous and isotropic lattices, ladder and prism networks, toroidal grids

Tóth Levente

A komplex objektumvédelem kihívásai napjainkban

A technológiai fejlődésnek köszönhetően egyre szélesebb eszközpark áll rendelkezésre a biztonságtechnikai piacon. A fejlesztések egy része azonban nemcsak biztonságunk növelésére szolgál, hanem ezekkel vagy ezeken keresztül újabb támadásoknak lehetünk kitéve. A megnövekedett eszközválaszték és az egyre intelligensebb rendszerek nagyobb szakismeretet, pontosabb tervezést, precízebb kivitelezést és karbantartást kíván a kivitelező cégek részéről, míg gondosabb és felkészültebb üzemeltetési feladatokat támaszt a felhasználókkal szemben. A rendszerek nagyságával párhuzamosan nő a bonyolultságuk, az összetettségük és a keletkező információk mennyisége. A hatékony üzemeltetés biztosítása érdekében különböző döntéstámogató algoritmusokat és szoftvereket fejlesztenek ki. Ezek egy része olyan kényelmi szolgáltatást is nyújt, amely újabb támadási felületet eredményezhet. Az új technológiák megjelenésével az objektumvédelem komplexitása további aspektusokkal egészül ki.

Kulcsszavak: drón, integrált felügyeleti rendszer, döntés támogató szoftver, M2M, IoT, UAV

Bevezetés

A rendszerváltozást megelőző időszakban a tulajdontárgyak döntő többsége, a termelőeszközök nagy egésze az állam tulajdonában volt. Ebből kifolyólag az állam mint közhatalmi szervezet látta el az állami vagyonvédelem mellett a tulajdonosi vagyonvédelmi feladatokat is. A rendszerváltást követően a tulajdonszerkezet gyökeres változáson ment keresztül. Az állami tulajdon hányada jelentősen csökkent, és a magántulajdon lett a gazdaság meghatározó tényezője. Ebben a helyzetben viszont az állam a magántulajdonosokat – egészen szűk kivételtől eltekintve – már nem kötelezheti vagyonuk védelmére, mert ezzel indokolatlanul beavatkozna a tulajdonos jogaiba. „Nemzetközi tendencia a magánbiztonság térnyerése, expanziója, amelynek hátterében többek között a rendőrségek kapacitásainak jobb eloszlása és a költséghatékonyság áll. Az államok, kormányok rájöttek, hogy a rendészeti monopólium szigorú fenntartása mellett, bizonyos feladatok, külö-

nösen egyes háttértevékenységek privatizálhatók, kiszervezhetőek." [1: 15] A fenti okok alapján hazánkban megváltozott a vagyonvédelem szabályozásának eddigi koncepciója.

A tulajdonosok részére az állam nem ír elő védelmi kötelezettséget, hanem a megalkotott és kihirdetett jogszabályok alapján lehetőséget biztosít a vagyonuk megvédésére. A különböző társadalmi csoportok közötti vagyoni különbségek növekedése, az országhatárok megnyitása, a szervezett külföldi bűnszövetkezetek megjelenése, a hazai bűnszövetkezetek kialakulása és megerősödésének természetes következményeként a mindennapi élet során egyre inkább előtérbe került a közrend, a közbiztonság helyzete, a bűncselekmények során megsokszorozódott vagyon elleni bűncselekményekkel szembeni hatékony védelmi rendszerek kialakításának igénye. Magyarország – a korábbinál sokkal intenzívebb – nemzetközi szerepvállalása, az Észak-atlanti Szerződés Szervezetéhez (NATO), illetve az Európai Unióhoz (EU) való csatlakozása egy új veszélyforrást idézett elő, amely tovább növelte a hazánk ellen irányuló külső fenyegetettséget is, amely elsősorban a modernkori terrorizmusban ölt testet. [2: 9]

A komplex vagyonvédelmi rendszerek

A bevezetőben felsorolt okok és indokok miatt egyre nagyobb igény jelentkezik a teljes körű vagyonvédelem kiépítésére, illetve a meglévő biztonságvédelmi rendszerek folyamatos fejlesztésére, bővítésére. E feladat megvalósításában kiemelkedő szerepet játszanak a komplex vagyonvédelmi rendszerek, azaz a mechanikai védelem, az elektronikai jelzőrendszerek, valamint az élőerős védelem és a különböző szervezeti intézkedések összessége. A felsorolt tényezők egy esetleges kárkövetkezmény enyhítését szolgáló biztosítással együtt optimális biztonságot képesek nyújtani a felhasználóknak. Teljes körű, 100%-os védelem még így sem valósítható meg, ezért számolnunk kell egy maradék kockázattal, amely a magánszemély vagy egy gazdasági szervezet esetén a menedzsment tudatos kockázatvállalását jelenti azzal, hogy az egyes veszélyforrásokra nem, vagy csak részben reagál védelmi megoldással. E kockázat egy káreseményt követően a visszaállítás során az egyénre vagy a gazdasági szervezetre háruló költségeket jelenti. „Kijelenthetjük, hogy a védelemmel szemben megfogalmazott követelmény kettős, egyfelől elvárás, hogy a védelem csökkentse a vagyon elleni szándékos jogellenes cselekmény elkövetésének valószínűségét a minimálisra, másfelől a cselekmény bekövetkezte esetén az elkövető kockázatát pedig növelje a maximálisra." [3: 8]

Az elektronikai jelzőrendszer, mint neve is mutatja, nem sorolható a klasszikus védelmi rendszerek közé. Ez a rendszer „csak" jelzi a behatolás tényét, illetve annak szándékát. Ezeknek a rendszereknek a feladata a különböző biztonságot veszélyeztető cselekmények detektálása, jelzése, az események nyomon követése, rögzítése, az illetéktelen személyek belépésének vagy a gépjárművek behajtásának gátlása, a különböző tárgyak, áruk, cikkek

be- és kivitelének ellenőrzése, valamint különböző – általában – automatikus vezérlések végrehajtása. Így tehát az elektronikai védelem a mechanikai-fizikai védelemmel szemben nem ad valós védelmet, hiszen nem tudja feltartóztatni a behatolót. Csupán jelzi az eseményt az élőerős védelemnek, aminek a feladata a bűncselekmény megakadályozása vagy az épületbe bejutott személy feltartóztatása, elfogása, vagyis a helyszínen való intézkedés. Az intézkedés végrehajtása viszont tervszerűséget, szervezettséget igényel. Ehhez elengedhetetlen az élőerős tevékenységet szabályzó rezsim (szervezeti) intézkedések megléte. [4]

A vagyonvédelem komplexitása, a védelmek közötti összefüggés úgy határozható meg, hogy az elektronikai védelemnek olyan előrejelzést kell biztosítania, hogy a mechanikai védelem képes legyen visszatartani a behatolni szándékozót az élőerős védelem kiérkezéséig. A védelmi rendszer kialakítása a védelem megfelelő ellátását szolgálja. A védelem folyamatos, komplex tevékenység, amelynek célja, hogy biztosítsa a biztonság kívánatos szintjének elérését, illetve fenntartását. [5]

Az objektumok biztonsága olyan állapotot, helyzetet jelent, amelyben az ott-tartózkodók életét, testi épségét, az anyagi javak és adatok létét, sértetlenségét, továbbá az objektum belső rendjét és működését sem külső, sem belső tényező nem sérti vagy veszélyezteti.

A biztonságot veszélyeztető veszélyforrások lehetnek természeti (villámcsapás, vízbetörés stb.) vagy technológiai eredetűek (elektromos kontakthiba, rosszul működő őrlángérzékelő stb.), illetve emberi közreműködéssel végrehajtott cselekmények. Ez utóbbi lehet tudatos (szándékos jogellenes magatartás) vagy gondatlan (többnyire figyelmetlenségből, hanyagságból keletkező veszélyek). A biztonságot veszélyeztető, emberi közreműködéssel szándékosan végrehajtott cselekmények közé sorolhatjuk a betörést, a lopást, a rablást, de tágabb értelmezésben az informatikai rendszerünk ellen elkövetett feltörést és adathalászatot is.

A felsoroltakból is jól látszik, hogy számtalan tényező veszélyezteti a biztonságunkat. Ebből kifolyólag a védelmi rendszerek eszközválasztéka is rendkívül széles skálát képez, így számos megvalósítási lehetőség áll rendelkezésre az objektumok komplex vagyonvédelmének megtervezésére és kialakítására.

Technológiai fejlődés

A technológiai piacon az 1950-es évek végétől, az integrált áramkörök (IC) megjelenésétől látványos és gyors fejlődésnek lehetünk szemtanúi. Az IC-k integráltsági foka 1,5 évente megduplázódik (Moore[1]-törvény). Ez a fejlődés kihatással van a biztonságtechnikai

[1] Gordon E. Moore, az Intel egyik alapítója.

piacra is. Számos, régebben mechanikai érzékelési elven működő berendezést mára már processzoros jelfeldolgozású szenzorok váltották fel (például üvegtörés és rezgésérzékelők). Különböző érzékelési technológiákat dolgoztak ki, amelyek tovább bővítették az objektumvédelem technikai eszköztárát. A megnövekedett eszközválaszték nagyobb szakismeretet, pontosabb tervezést, precízebb kivitelezést és karbantartást kíván a kivitelező cégek részéről, míg gondosabb és felkészültebb üzemeltetési feladatokat támaszt a felhasználókkal szemben. A rendszerek nagyságával nő azok bonyolultsága, összetettsége, ezzel együtt a hibaforrások és a kezelési hibák száma.

A különböző elektronikai jelzőrendszerek már nem csak önmagukban, azaz a rendszer alkotóelemeivel kommunikálnak, hanem képesek más rendszereknek információt továbbítani, vagy onnan fogadni és értelmezni. Megjelentek a piacon az úgynevezett M2M[2]-eszközök, amelyek intelligens módon képesek a keletkező adatokat feldolgozni és továbbítani más gépekhez vagy a felhasználóhoz. Mára már a rendszerek egymásba ágyazása, integrálása is sokkal mélyebben (szoftveres úton) történhet meg, szemben a tíz évvel ezelőtti relés kimenetek és bemenetek (hardveres) összekapcsolásával.

A komplex objektumvédelem kihívásai

A technológiai fejlődésnek azonban vannak árnyoldalai is. Egyrészt az új, korszerű berendezések nem csak a védelem, az elhárítás oldalán jelennek meg, másrészt pedig pont a kifelé zajló kommunikáció teremtett egy rést a kívülről jövő támadhatóságban. Szintén a fejlődésnek tudható be, hogy igen nagy mértékben megnövekedett az informatikai úton előálló adathalmaz, amelyek között lehetnek személyes, minősített vagy éppen ipari kémkedésnek kitett adatok is. Ebből fakad, hogy a védendő materiális értékek, javak egyre inkább kiegészülnek kevésbé kézzel fogható, de egyes esetekben igen nagy értéket képviselő információkkal, adatokkal is. Mindezekből következik, hogy tágabb értelmezésben a komplex objektumvédelem kialakításánál nemcsak a fizikai úton, erőszakos módon történt anyagi javak megszerzése ellen kell védekeznünk, hanem ugyanilyen fontos a kiberbűnözés elleni védekezés is.

A 21. század új, biztonságvédelem szempontú kihívása a pilóta nélküli repülőgép (UAV[3]), vagy más néven drón.[4] Bár katonai repülésre az 1960-as évek elejétől alkalmazzák, polgári elterjedése néhány éve számottevő.

Magyarországon polgári védelem, katasztrófavédelem, közbiztonság, közrendvédelem céljára több mint 10 éve használják. [6: 130] Az eszköz segítséget nyújt(hat) a zöldhatár figyelése során, az árvízi védekezésben, az erdőtüzek felderítésében, a közlekedési

[2] Machine-to-Machine: gépek közötti adatkommunikációs technológia.
[3] Unmanned Aerial Vehicle: pilóta nélküli repülőgép.
[4] Az angol drone szóból, jelentése here (méh).

helyzet ellenőrzésében, az elfogások, rajtaütések tervezésében és ezek távoli megfigyelésében, valamint a tömegrendezvények biztosításában. [7: 71–72]

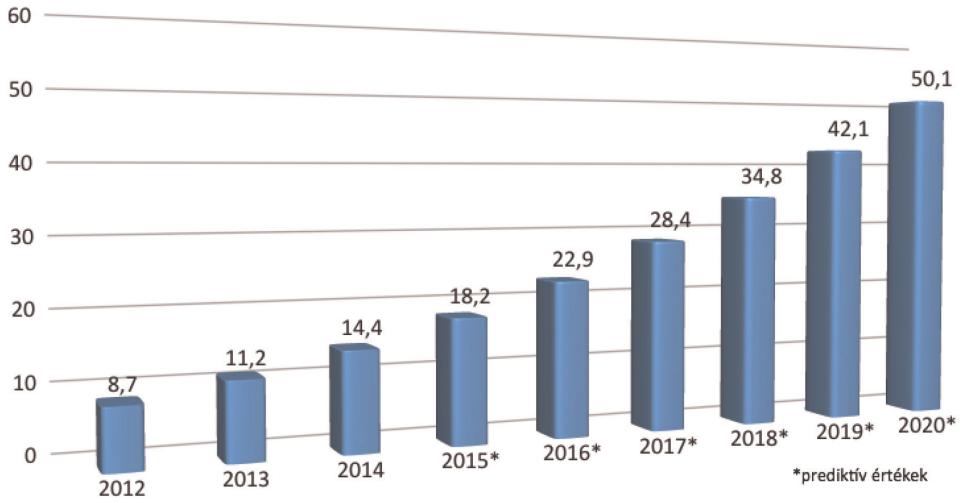
Az eszköz hazai magánbiztonsági felhasználása még nem számottevő, pedig ezen a területen is számos feladatra bevethető. Hatékonyan és jól képes támogatni a nagy kiterjedésű objektumok kerítésvédelmi rendszerét. A rendszer jelzése esetén a célra repülve, gyorsan kiszűrhetjük a téves riasztásokat, illetve rögzíthetjük és nyomon követhetjük az eseményeket. Az őrzési szolgáltatás minőségének javítása érdekében használhatjuk őrjárat ellenőrzésére, vagy éppen ennek kiváltására, azaz kültéri járőrözés végrehajtására.

Fontos kiemelni, hogy a drónok nem csak védelmi berendezésként használhatók. Napjainkban sokkal nagyobb kihívást jelent az ellenük történő védekezés. Jelenleg az Európai Unióban nincs egységes szabályozás a drónok használatáról (ennek tervezett bevezetése: 2018), bár az Európai Repülésbiztonsági Ügynökség (EASA[5]) már kidolgozott egy szabályozási javaslatot. Az átmeneti időszakban a tagállamok egymástól független, nemzeti szabályozásba kezdtek.

Független a törvényalkotás miként jétől, annak megjelenése csak a „jó szándékú" reptetést szabályozza és nem gátja a különböző bűncselekmények végrehajtására bevetett drónoknak. Jelenleg a kereskedelemben kapható drónok sebessége már meghaladja a 110 km/h-át. A jelenlegi megfizethető árú drón észlelési technológiák (radar, termokamera, hang) csak maximum egy-két kilométeres hatótávolságot tesznek lehetővé. Ez azt jelenti, hogy ilyen sebesség mellett kb. 1 perc áll rendelkezésre az észleléstől a megsemmisítésig. Ez még kevesebb is lehet, ha a drón már olyan területre ért, ami felett nem lehet lelőni (például tömegrendezvény).

A technológiai fejlődés másik nagy kockázata biztonság szempontból az egyre nagyobb számban megjelenő IoT,[6] azaz az interneten keresztül elérhető eszközök. A Cisco Internet Business Solutions Group (IBSG) tanulmánya 2020-ra 50 milliárd IoT-eszközt prognosztizál. [8] Ezzel egyetértésben, de ezen is túlmutat az SMA[7] 2014-es kutatása, amely 2035-re 1000 milliárdra prognosztizálja az IoT-eszközök darabszámát. [9]

[5] European Aviation Safety Agency.
[6] Internet of Things: Dolgok Internete, de használatos még az „Internet ott tárgyak" kifejezés is.
[7] Strategy Meets Action.



1. grafikon – IoT-eszközök darabszáma (milliárdban) 2012 és 2020 között [10]

Az eszközök választéka már jelenleg is széles körű. A már szinte hétköznapinak számító okostévén túl találhatunk okoshűtőszekrényt, -mosógépet, -kazánt, de még -kávéfőzőt is. Egyre népszerűbbek az „intelligens ház" (smart home) kialakítások, amelyeknek szerves részét képezik az IoT-eszközök. Egy ilyen rendszernél interneten keresztül mobiltelefon vagy táblagép segítségével vezérelhetjük a különböző otthoni berendezéseinket, vagy felügyelhetjük a fűtést/hűtést, a világítást, a kamerát vagy a behatolást jelző rendszereinket. Ezek a funkciók nagyon kényelmesek, viszont számos veszélyt hordoznak magukban. Mobiltelefonunk ebben a szerepkörben egy teljesen új értelmezést nyert. Ebbe az eszközbe integrálódik a teljes biztonságunk. Ezen egyetlen eszközön keresztül elérhetjük otthoni és céges levelezéseinket, hálózati tárolónkat, fizethetünk vele vagy felügyelhetjük a kameráinkat, ki- és bekapcsolhatjuk a riasztónkat, illetve használhatjuk beléptetőrendszerben kártya helyett, de vezérelhetjük vele a bejárati ajtónk zárját is. Egyes gépkocsiknál már lehetőség van a telefonon keresztüli nyitásra, illetve zárásra. Mindezen funkciókhoz hozzáférhetünk egy kifigyelhető jelkód vagy a születési évünkre beállított jelszó birtokában.

1. ábra – Mobiltelefonos applikációk (a szerző saját szerkesztése)

Ráadásul ez csak az egyik veszélyforrás. A piaci pozíciók stabilizálása érdekében a gyártók felgyorsított fejlesztési, gyártási és tesztelési fázisokat alkalmaznak, amelynek következtében nemcsak a minőség, a tartósság szenved csorbát, hanem kevesebb figyelem jut az eszközök kiberbűnözéssel szembeni védelmére is. Ez utóbbi pedig közvetlenül vagy közvetve is súlyos kockázatot hordoz egy biztonsági rendszer komplexitásában. A gyártó által véletlenül (vagy szándékosan) nyitva hagyott rejtett hozzáférés (backdoor) közvetlen lehetőséget biztosít a teljes kontroll átvételére az adott eszköz felett. Közvetve pedig – e bejáratot kihasználva – megnyílik a lehetőség más, szintén az adott belső hálózatra csatlakozó eszközök elérésére is, amelyről azt gondolnánk, hogy biztonságban van, mivel direkt módon nem csatlakozik az internetre. A cseh Biztonsági Információs Szolgálat (BIS) már a 2014-es évi jelentésében az alábbiakat írta: „Az elmúlt évekhez hasonlóan, a BIS olyan készülékek és technológiák felderítésére összpontosított, mely a biztonságot fenyegető potenciális veszélyt rejt magában. 2014-ben a BIS vizsgálata kiterjedt többek között az IP-kamerákra is (hálózatos kamerákra, webkamerákra). A BIS-hez eljutott információkat megerősítették a saját megállapításaik is, mely szerint egy IP-kamerában olyan firmware-t találtak, amely nem dokumentált rendszergazda fiókot (backdoor) is

tartalmazott. A hálózatra történő csatlakozást követően a kamera kommunikálni próbált egy előre beállított domain szerverrel, ami valószínűleg egy nagyobb felhőtároló része lehetett. Hackerek a böngészőbe beírt lekérdezési karakterlánc segítségével a fent említett backdooron keresztül elérhetik a kamerát." [11]

A fenti észrevétel nem egyedi. Az interneten több olyan esettel is találkozhatunk, ahol – többnyire kínai – gyártókat támadnak azzal, hogy adathalászás vagy kémkedés céljára fenntartott backdoorokat tartalmaz az eszközt működtető firmware-jük. [12] [13]

Amennyiben a szándékosságot kizárjuk, akkor feltételezhetnénk azt is, hogy a biztonságtechnikai eszközgyártók szoftverfejlesztői kevésbé jártasak a szoftverírásban, vagy hanyagság, időhiány miatt nem írják meg megfelelő biztonsági szinten a programot. Bár találhatunk erre is példát (például amikor a hozzáférési jelszót titkosítás nélkül, sima szövegként tárolják, vagy webes hozzáférés esetén egyes aloldalak autentikáció nélkül is elérhetők), mégsem csak erről van szó. 2016 nyarán került napvilágra, hogy a világ 67 országában jelenlévő informatikai nagyvállalat eszközeiben szoftveres biztonsági rést találtak, amely több mint 120 különböző típusú berendezést, köztük biztonságtechnikai eszközöket és kamerákat is érint. [14] A gyártó a honlapján elismerte a hibát, [15] és körülbelül másfél hónap alatt megszüntette a biztonsági rést.[8] Ekkora cégnél, ilyen fejlesztői háttérrel nem beszélhetünk hozzá nem értésről. Ebben az esetben egy beépített kényelmi szolgáltatás (az eszközök távoli elérése a cég szerverén keresztül) okozta az alapproblémát. A túl sok eszközhöz rendelt funkció, a beállítási lehetőségek széles skálája és persze a gyors piaci megjelenés miatt valószínűleg nem történt mindenre kiterjedő, alapos sérülékenységi vizsgálat.

Elgondolkoztató és egyben aggasztó előadást tartott az idei Las Vegasban megrendezett DEF CON hacker konferencián Anthony Rose és Ben Ramsey. [16] A két biztonsági szakember 16 db kereskedelemben kapható, bluetooth-vezérelt „okoszárat" vizsgált meg. Néhány száz dolláros eszközparkkal, különböző módszerekkel a zárak 75%-át (12 db-ot) szoftveresen feltörték. A maradék négyből egyet pedig egy csavarhúzó és fogó segítségével, erőfeszítés nélkül nyitottak ki. [16] Négy különböző zárat találtak, ahol a mobiltelefon és a zár közötti kommunikáció titkosítás nélkül zajlik. Az adatforgalmat egy irányított antennával több száz méter távolságból vették és rögzítették. Egyszerű szöveges üzenetekkel a felhasználó által beállított jelszó felülírható, és ezzel a felhasználó kizárható a hozzáférésből. Alapállapotba visszaállítani a zártestbe szerelt elemek eltávolításával lehet, ami viszont csak a zár nyitott állapotában hajható végre.

A gyártó a honlapon úgy reklámozza a zárat, hogy biztonságosabb, mint a kulcs vagy a kód, mivel ezt nem lehet elveszíteni vagy lemásolni. A gyanútlan felhasználó ezért azt gondolja, hogy bár az eszköz lehet, hogy többszöröse a legjobb minőségű mechanikai

[8] Arra vonatkozóan nincsenek pontos adatok, hogy valójában hányan töltötték le a frissítést és szüntették meg a hibát.

zárnak, de legalább biztonságosabb. Eközben távolról, zajtalanul egy szempillantás alatt nyitható.

Összegzés

A technológiai fejlődés következtében új típusú veszélyforrások jelentek meg a komplex objektumvédelemben. Ezek közül az elkövetkező évek egyik nagy kihívása a drónok elleni védekezés lesz. A hamarosan bevezetendő jogszabályi szigorítás nem fogja megakadályozni az ártó szándékú reptetéseket, ezért a kiemelten fontos objektumoknál szükség lehet észlelő, elfogó/megsemmisítő berendezések telepítésére. Ehhez azonban a jelenlegi technológiákat még fejleszteni, hatótávolságukat növelni kell.

Szintén a technológiai fejlődésnek köszönhető, hogy egyre több önálló intelligenciával és döntési képességgel rendelkező berendezések állnak a vagyonvédelem szolgálatába. Ezek az eszközök egymással vagy egy felügyeleti szoftverrel folyamatosan kommunikálnak. Ez folyamatos (online) jelenlétet igényel, amely egy újabb támadási felületet eredményez. A piaci pozíciók erősítése és stabilizálása érdekében a gyártók felgyorsított fejlesztési, gyártási és tesztelési fázisokat alkalmaznak. Ez utóbbinak köszönhetően megnövekszik az eszközök kibertámadással szembeni sérülékenysége. Megfelelő informatikai tudás birtokában egy külső behatoló akár mesterszintű felhasználói jogosultságokkal – a valós felhasználót kizárva – vezérelheti a komplex védelmi rendszert. Ezért nagyon fontos, hogy a komplex objektumvédelmünk megfelelő szintű informatikai védelemmel is kiegészüljön.

Irodalomjegyzék

[1] Christián L.: *A magánbiztonságelméleti alapjai*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[2] Tóth A. – Tóth L.: *Biztonságtechnika*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[3] Berek L.: *Biztonságtechnika*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[4] Berek T. – Bodrácska Gy.: Az élőerős őrzés az objektumvédelem építőipari ágazatában. *Hadmérnök,* 5. évf. 4. szám, 2010.

[5] Berek L. – Berek T. – Berek L.: *Személy és vagyonbiztonság.* Óbudai Egyetem, Budapest, 2016.

[6] Vránics D. – Üveges A.: Pilóta nélküli légi járművek fejlődése. *Felderítő Szemle,* 14. évf. 2. szám, 2015.

[7] Petrétei D.: A drónok kriminál technikai és rendészeti felhasználása. *Magyar Bűnüldöző,* 6. évf. 1-3. szám, 2015.

[8] The Internet of Things. www.cisco.com/c/dam/ en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (a letöltés ideje: 2016. 12. 27.)

[9] The Internet of Things: Creating a Connected World. https://strategymeetsaction.com/about-sma/ (a letöltés ideje: 2016. 12. 27.)

[10] Internet of Things (IoT): Number of connected devices worldwide from 2012 to 2020 (in billions). www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (a letöltés ideje: 2016. 12. 27.)

[11] Annual report of the Security Information Service for 2014. www.bis.cz/annual-reports/annual-report-of-the-security-information-service-for-2014-9d082374.html (a letöltés ideje: 2016. 12. 27.)

[12] Is the World's Biggest Surveillance Camera Maker Sending Footage to China? www.voanews.com/a/hikvision-surveillance-cameras-us-embassy-kabuk/3605715.html (a letöltés ideje: 2016. 12. 27.)
[13] Dahua DVR Authentication Bypass – CVE-2013-6117. https://depthsecurity.com/blog/dahua-dvr-authentication-bypass-cve-2013-6117 (a letöltés ideje: 2016. 12. 27.)
[14] Serious Vulnerability Affects Over 120 D-Link Products. www.securityweek.com/serious-vulnerability-affects-over-120-d-link-products (a letöltés ideje: 2016. 12. 27.)
[15] Regarding Senr.io Vulnerability Affecting Many D-Link Products. www.dlink.com/uk/en/support/support-news/2016/july/15/senrio-vulnerability (a letöltés ideje: 2016. 12. 27.)
[16] Have a smart lock? Yeah, it can probably be hacked. www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/ (a letöltés ideje: 2016. 12. 27.)

Today's Challenges of Complex Property Protection

Levente Tóth

Due to technological progress, there is an ever wider range of tools available in the security technology market. Besides increasing security, however, a part of these developments may expose us to new attacks. The increased range of tools and the ever more intelligent systems require a higher degree of expertise, more accurate design and more precise implementation and maintenance from the implementing companies, and more careful and skilled operation from the users. The complexity of the systems and the amount of information generated increases in proportion to their size. In order to ensure efficient operation, various decision-supporting algorithms and software are developed. Some of these also provide comfort services that may contain new vulnerabilities. With the appearance of new technologies, the complexity of object protection is extended with new aspects.

Keywords: Drone, Integrated Management System, Decision Support Software, M2M, IoT, UAV

Tóth Attila

A biztonságtechnikai tervezők helyzete

A 2012-ben hatályba léptetett, átalakított vagyonvédelmi törvény nehéz helyzetbe hozta a magánbiztonsági ágazatot. Ennek a változtatásnak estek áldozatul a biztonságtechnikai tervezők is, akiknek a helyzete meglehetősen bizonytalanná vált. A megváltozott jogszabályi környezetben a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara nem tarthatja nyilván a biztonságtechnikai tervezőket, nem felügyelheti szakmai tevékenységüket. A korábban szabályozott szakmagyakorlási jogosultsági rendszer, a jól működő továbbképzési, vizsgáztatási rendszer, a részletes nyilvántartási rendszer (névjegyzék) jelenleg nem működik.

Kulcsszavak: tervezés, magánbiztonság, kamara, biztonságtechnika

Előzmények

Magyarországon a rendszerváltást követő években (az 1990-es évek elején) jelentősen megnövekedett a bűnelkövetések száma. Az országos statisztikák alapján ebben az időszakban megháromszorozódtak a bejelentett vagyon elleni bűncselekmények. A közbiztonsági helyzet romlásával megnövekedett az igény a magánbiztonság területén tevékenykedő vállalkozások szolgáltatásaira. [1: 65]

Az 1990-es évek közepére a magánbiztonság területén piaci szolgáltatást nyújtó vállalkozások tevékenységi területei jelentősen kibővültek. A vagyonőri tevékenységen kívül megjelent egyre több magánnyomozó, személyvédelmi szolgáltatás nyújtó (például testőr), pénz-, és értékszállító, illetve biztonságtechnikairendszer-tervező, -telepítő és -karbantartó vállalkozás. A magánbiztonsági ágazat ugrásszerű növekedése szükségessé tette a személy- és a vagyonvédelmi tevékenység szabályozását. Az ágazati törvény megalkotásáig az 1994. évi XXXIV. törvény (rendőrségi törvény)[1] felhatalmazásával a kormány a 87/1995. (VII. 14.) kormányrendelet megalkotásával átmeneti jelleggel szabályozta a magánbiztonsági szolgáltatást nyújtók tevékenységét. [2: 12] A kormányrendelet

[1] Az 1994. évi XXXIV. tv. 28. § (1) tartalmazta a rendőrhatósági engedélyhez kötött személy- és vagyonvédelmi szolgáltatások körét.

hatálybalépését követően vagyonvédelmi műszaki rendszerek tervezését, telepítését, karbantartását már kizárólag rendőrhatósági engedély birtokában lehetett végezni.[2]

A vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról szóló 1998. évi IV. törvény rendezte első ízben a magánbiztonság területén tevékenykedő vállalkozások helyzetét. Ebben a törvényben definiálták először a vagyonvédelmi biztonságtechnikai tervező, szerelő fogalmát. „Vagyonvédelmi biztonságtechnikai tervező, szerelő: az a természetes személy, aki – tevékenységéből eredően – ismeretekkel rendelkezik a 7. pontban meghatározott vagyonvédelmi biztonságtechnikai rendszer működéséről, s az ilyen rendszer (eszköz, berendezés) tervezését, telepítését, szerelését, üzemeltetését, karbantartását személyesen végzi, azt szakmailag szervezi vagy irányítja."[3] A tervező és a szerelő vesszővel lett elválasztva, sőt több helyen a tervezést, a szerelést, az üzemeltetést és karbantartást is egymás mellett említi a jogalkotó, ezáltal egybemossa ezeket a tevékenységeket, amelyek végzéséhez egyébként eltérő képzettségek, képességek szükségesek.

A jogszabály megalkotása idején már létezett biztonságtechnikaimérnök-képzés. A képzési követelményeket, a tantervet és a képzési tervet a Budapesti Politechnikumba szerveződött öt főiskola[4] képviselői dolgozták ki. Először 1992 szeptemberében indított a Politechnikum négy főiskolája (a Bolyai János Katonai Műszaki Főiskola kivételével) biztonságtechnikai mérnök szakot, nappali képzés keretében. Az induló évfolyamra összesen 130 hallgatót vettek fel a középiskolából hozott pontszámok alapján. 1998-tól a Bolyai János Katonai Műszaki Főiskola levelező rendszerű oktatásban kezdte meg a biztonságtechnikaimérnök-képzést. 2001-től a Budapesti Műszaki Főiskolán is elindult a biztonságtechnikai mérnök szak, levelező képzés keretében. Ezek a képzések főiskolai szintű mérnöki diplomát adtak. [3: 7–8]

2006-ban indult meg a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Karán a biztonságtechnikai mérnökök MSc-szintű képzése. Az első okleveles biztonságtechnikaimérnök-hallgatók 2008-ban végeztek.

[2] 87/1995. (VII. 14.) Korm. rendelet 1. § (2).

[3] 1998. évi IV. törvény a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról 47. § 5. Az idézetben hivatkozott 7. pont a vagyonvédelmi biztonságtechnikai rendszer definícióját tartalmazza.

[4] A Budapesti Politechnikum tagjai a következők voltak: Bánki Donát Műszaki Főiskola, Bolyai János Katonai Műszaki Főiskola, Kandó Kálmán Műszaki Főiskola, Könnyűipari Műszaki Főiskola, Ybl Miklós Műszaki Főiskola.

Az új vagyonvédelmi törvény

A biztonságtechnikai tervezők és szerelők helyzetét a 2005. évi CXXXIII. törvény,[5] valamint a végrehajtásáról szóló 22/2006. (IV.25.) BM rendelet rendezte.

A törvény megkülönböztet vagyonvédelmi biztonságtechnikai tervezőt, vagyonvédelmi biztonságtechnikai szerelőt, mechanikai vagyonvédelmirendszer-tervezőt és mechanikai vagyonvédelmirendszer-szerelőt.[6] [4] A törvény pontosan definiálja ezeket a tevékenységi köröket, például „2. vagyonvédelmi biztonságtechnikai tervező: az a természetes személy, aki – tevékenységéből eredően – ismeretekkel rendelkezik a vagyonvédelmi biztonságtechnikai rendszer működéséről, az ilyen rendszer (eszköz, berendezés) tervezését személyesen végzi, illetve azt – szakmailag – közvetlenül szervezi vagy irányítja". Ezenkívül a 33. § (1) bekezdésében meghatározza, hogy „[m]echanikai vagyonvédelmi, illetve vagyonvédelmi biztonságtechnikai rendszert kizárólag a kamara által kidolgozott szakmai követelményeknek megfelelő, a kamara által kiadott tervezői névjegyzéken szereplő személy tervezhet". A 22/2006 (IV.25.) BM rendeletben pedig leírja, hogy milyen előképzettséget fogadhat el a kamara:[7] 10/A. § „(6) Biztonságtechnikai tervező, szerelő képesítésként kell elfogadni a biztonságtechnikai, a híradástechnikai, a távközlési, az elektrotechnikai, valamint villamosmérnöki képzettséget adó egyetemi vagy főiskolai végzettséget igazoló, illetve a felsőoktatási alap- és mesterképzésben szerzett oklevelet."

A jogalkotók a törvény és végrehajtási rendelete elkészítésekor körültekintően definiálták a tevékenységet végzők feladatát, meghatározták a tervezői jogosultságot kiállító szervezetet (SzVMSzK), illetve meghatározták azoknak az előképzettségeknek a körét, amelyeket a kamara a tervezői jogosultság megállapításához előképzettségként elfogadhat. Ezenkívül a kamara feladatai között[8] említi, hogy a kamara évenként tegye közzé a tervezői névjegyzéket, valamint ellenőrizze az általa kiadott tervezői engedélyekben foglaltak és a szakmai előírások betartását.

A kamara a rá rótt feladatok elvégzéséhez megalkotta a biztonságtechnikai és mechanikai vagyonvédelmi rendszert tervezői jogosultság megújításához előírt továbbképzésre vonatkozó szabályzatot, amelyet a 2007. november 13-i elnökségi ülésen a 124/2007. (11., 13.) számú elnökségi határozattal elfogadtak.

A szabályzatban a szakmagyakorlási jogosultság érvényességét öt évben határozták meg. Az ötéves továbbképzési időszak alatt minden tervező mérnöknek részt kellett venni egy kötelező továbbképzésen, ahol a biztonságtechnikai tervezőket érintő jogi, pénzügyi, szabvány és minőségirányítási ismereteket sajátíthatták el. Ezenkívül szabadon választható szakmai továbbképzésekre kellett járniuk, ahol a legújabb technikai fejlesztéseket

[5] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.

[6] 2005. évi CXXXIII. törvény 74. § 2–5. pont (2005. 11. 30-án hatályos állapot).

[7] Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (SzVMSzK).

[8] 2005. évi CXXXIII. törvény 38. § l.) bekezdés (2005. 11. 30-án hatályos állapot).

ismerhették meg. A szabadon választható továbbképzéseken pontokat gyűjthettek attól függően, hogy milyen hosszú volt a továbbképzés, illetve hogy ott hallgatóként vagy előadóként voltak jelen, de továbbképzési pontot ért a szakmagyakorlási jogosultsághoz kapcsolódó felsőfokú posztgraduális képzés, a publikáció, a különféle szakmai díjak elnyerése is. A tervezői jogosultság meghosszabbításának feltétele volt a továbbképzéseken való részvétel igazolása és a továbbképzési időszakban legalább 20 pont összegyűjtése. [5]

A továbbképzési pontrendszer a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara, a Magyar Mérnöki Kamarával együttműködve dolgozta ki. A Magyar Mérnöki Kamaránál ekkor hasonló továbbképzési rendszer működött. A kettős kamarai tagsággal rendelkező tervezők esetén a továbbképzéseken való részvétel igazolását mindkét kamara kölcsönösen elfogadta.

A vagyonvédelmi törvény módosítása

Az Országgyűlés a 2011. február 28-i ülésnapján elfogadta a 2011. évi XXIV. törvényt, amely az Európai Rendőrségi Hivatallal, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységgel, a lőfegyverrel és a pirotechnikával kapcsolatos törvények jogharmonizációs célú módosításáról szólt.[9]

A jogharmonizációs célú módosítás gyökeresen megváltoztatta a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységről szóló törvényt. A módosítás 2012. január 1-jét követő hatálybalépése után a vagyonvédelmi kamara a továbbiakban már nem tarthatta nyilván az elektronikus, illetve a mechanikus vagyonvédelmi rendszert tervező mérnököket, nem volt jogosult a tervezői engedélyek kiadására és természetesen kreditpontos továbbképzések tartására sem. Eltörölték a kötelező vagyonvédelmi kamarai tagságot is, de nem rendelkeztek a tervezők további sorsáról. A biztonságtechnikai tervező, szerelő igazolványokat továbbra is a lakhely szerint illetékes rendőrkapitányság adta ki, az igazolvány kiadásának feltétele azonban csupán az előképzettség igazolása (az iskolai végzettséget vagy szakképesítést tanúsító oklevél vagy bizonyítvány közjegyző által hitelesített másolata[10]) és a büntetlen előélet volt. Az igazolványt igénylők korábbi referenciáit senki nem vizsgálta. Nem nézték, hogy a tervező tervezett-e korábban bármilyen vagyonvédelmi rendszert, hogy például villamosmérnökként elvégzett-e valamilyen tanfolyamot, részt vett-e bármilyen szakmai továbbképzésen.

A tervezők exlex állapotának megszüntetése érdekében, még a törvénymódosítás hatályba lépését megelőzően a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara akkori biztonságtechnikai alelnöke és a kamara főtitkára egyeztetett a Magyar Mérnöki Kamara (továbbiakban: MMK) főtitkárával, valamint az MMK Elektrotechni-

[9] A törvény a 40. § (4) bekezdése alapján hatályát vesztette 2012. június 30. napjával.
[10] 22/2006. (IV. 25.) BM rendelet 3. § (4) *a).*

kai és Épületvillamossági tagozatának elnökével. Az egyeztetések során megállapodtak az elektronikus vagyonvédelmi rendszereket tervezők betagozódásáról.

Az MMK Elektrotechnikai és Épületvillamossági tagozatán belül 2007 decemberében megalapult az Elektronikus vagyonvédelmi szakosztály (továbbiakban: szakosztály). A szakosztály feladatai voltak többek között a tervezői és szakértői jogosultság elbírálásához, a névjegyzékbe vételhez szükséges szakmai véleményadás az Elektrotechnikai és Épületvillamossági tagozat minősítő bizottságának, a szakmai felsőoktatási intézmények képzési követelményeinek véleményezése, a közreműködés a vagyonvédelmi szakmát érintő szabályozási, szabványosítási, akkreditálási és minőségügyi tevékenységekben stb.[11] Mivel ezeket a feladatokat 2012. január 1-jéig a vagyonvédelmi kamara ellátta, a szakosztályra kevés feladat hárult. Az alapító elnök dr. Utassy Sándor 2010-ben bekövetkezett halálát követően [6: 4] a szakosztály működése leállt. A vagyonvédelmi tervezők mérnöki kamarába tagozódását követően szükségessé vált az elektronikus vagyonvédelmi szakosztály újjáélesztése. A szakosztály 2012. március 20-án taggyűlést tartott az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán, ahol a tagok új elnökséget és Cselovszki Zoltán személyében új elnököt választottak. [7] Ezt követően a szakosztály ismét megkezdte működését.

A biztonságtechnikai mérnökök tervezői jogosultsága

A Magyar Mérnöki Kamara szakmagyakorlási szabályzata [8] tartalmazza a jogosultság megállapításának szabályait és feltételeit.

A szakmagyakorlási jogosultság megállítását és odaítélését első fokon a kérelmező lakóhelye szerinti területi mérnöki kamara titkára, másodfokon a Magyar Mérnöki Kamara főtitkára végzi.[12] A titkár a jogosultág megállapításakor figyelembe veszi az országos kamara által működtetett minősítő testület (OSzMT) szakértői véleményét. Az OSzMT vizsgálja a szakmai gyakorlati időt a 266/2013. (VII.11.) Korm. rendelet[13] 12. § (1)–(2) bekezdései szerint, valamint a kérelmező által benyújtott oklevél szakirányúságát és a szakirányú szakképzettség egyenértékűségét a szakmagyakorlási szabályzat függelékének 1/B mellékletében előírt minimum kreditszámok összege alapján. [9]

A 266/2013. (VII.11.) Korm. rendelet határozza meg az engedélyhez kötött szakmagyakorlási tevékenységek körét.[14] Az elektronikus vagyonvédelmi rendszerek tervezése ez alapján az építményvillamossági tervezési szakterületbe sorolódik. A rendelet nem

[11] Magyar Mérnöki Kamara Elektrotechnikai és Épületvillamossági Szakmai Tagozat Elektronikus Vagyonvédelmi Szakosztálya Ügyrend 2007.

[12] Magyar Mérnöki Kamara szakmagyakorlási szabályzata 5. § (1).

[13] 266/2013. (VII. 11.) Korm. rendelet az építésügyi és az építésüggyel összefüggő szakmagyakorlási tevékenységekről.

[14] 266/2013. (VII. 11.) Korm. rendelet 3. § (3) dd) építményvillamossági tervezési szakterület.

különböztet meg erős és gyengeáramú tervezési tevékenységeket, ezért a biztonságtechnikai rendszereket tervező biztonságtechnikai mérnökökre ugyanazok a követelmények vonatkoznak, mint az erősáramú hálózatokat tervező, villamosmérnök végzettségű épületvillamossági tervezőkre. A biztonságtechnikai mérnök végzettségű szakemberek szakmai előképzettségének igazolásához az OSzMT a szakmagyakorlási szabályzat függeléke 1/B mellékletének[15] az építményvillamossági tervezési szakterületre vonatkozó követelményeit veszi figyelembe.

Ezek a követelmények a következők:[16]

1. táblázat – Az MMK építményvillamossági tervezési szakterületre vonatkozó kredit követelményei (a szerző saját szerkesztése)

	Szükséges kreditek száma	
	BSc	MSc
Természettudományos alapismeretek	45	60
Gazdasági és humán ismeretek	18	25
Szakmai törzsanyag	75	85
Differenciált szakmai ismeretek	62	100
Minimum kreditszám összesen:	200	270

Az Óbudai Egyetemen végzett biztonságtechnikaimérnök-hallgatók az alábbi krediteket szerezték meg:[17]

2. táblázat – Az Óbudai Egyetemen végzett biztonságtechnikaimérnök-hallgatók által gyűjtött kreditek (a szerző saját szerkesztése)

	Kreditek száma	
	BSc	MSc
Természettudományos alapismeretek	46	28 (74)
Gazdasági és humán ismeretek	16	10 (26)
Szakmai törzsanyag	85	30 (115)
Differenciált szakmai ismeretek	63	52 (115)
Minimum kreditszám összesen:	210	120 (330)

A fentiek alapján a mérnöki kamara minősítő testülete a biztonságtechnikai mérnök alapképzésben végzett hallgatók képzettségét nem ítélte egyenértékűnek az építményvillamossági tervezési szakterületre vonatkozó követelményekkel.

[15] A szakmagyakorlási szabályzat függeléke 1/B melléklete: A szakirányú szakképzettség egyenértékűségének vizsgálatához tudományterület szerinti bontás alapján meghatározott minimum kreditszámok összege a besorolásra nem alkalmas szakképzettségek tekintetében.

[16] Az OSzMT a szakmagyakorlási szabályzat függeléke 1/B mellékletének az építményvillamossági tervezési szakterületre vonatkozó követelményei alapján.

[17] Az Óbudai Egyetem biztonságtechnikai mérnök alap- és mesterképzési szak tanterve alapján.

A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 110. § (3) bekezdés *b)* pontjában kapott felhatalmazás alapján az Emberi Erőforrások Minisztériumának minisztere rendeletben szabályozza a felsőoktatási szakképzések, az alap- és mesterképzések képzési és kimeneti követelményeit.[18] A felsőoktatási intézmények e rendelet figyelembevételével alakítják ki képzési programjaikat. A rendelet 3. melléklete tartalmazza az alapképzési szakok, a 4. melléklete pedig a mesterképzési szakok képzési és kimeneti követelményeit.

3. táblázat – A biztonságtechnikai mérnökök számára a 18/2016. (VIII. 5.) EMMI rendelet alapján adható kreditek[19] (a szerző saját szerkesztése)

	Kreditek száma	
	BSc	MSc
Természettudományos alapismeretek	40–50	20–35
Gazdasági és humán ismeretek	14–30	10–20
Szakmai törzsanyag	70–105	15–35
Differenciált szakmai ismeretek	min. 40	40–60
Minimum kreditszám összesen:	210	120

A táblázatból látható, hogy az Óbudai Egyetemen végzett biztonságtechnikai mérnökök végzettsége megfelel a jogszabályokban előírt képzési és kimeneti követelményeknek.

A villamosmérnökökre vonatkozó jogszabályi követelmények tökéletesen megegyeznek a biztonságtechnikai mérnökökre vonatkozókkal. Felmerül a kérdés, hogy miért nem a jogszabályban meghatározott kimeneti követelmények szerepelnek a Magyar Mérnöki Kamara szakmagyakorlási szabályzatában.

Következtetések

A biztonságtechnikai rendszerek tervezése eltér a hagyományos értelemben vett elektromos vagy informatikai hálózatok tervezésétől. Ezeknek a rendszereknek a tervezésénél nem csupán az elektronikai, elektrotechnikai fogalmakkal, illetve a vonatkozó szabványokkal kell tisztában lennie a tervezőnek, hanem jóval szélesebb látókörrel kell rendelkeznie. A biztonságtechnikai tervezőnek ismernie kell a különféle építészeti, gépészeti megoldásokat, ismernie kell a védendő objektum minden részletét, megközelíthetőségét, a környezetének bűnügyi fertőzöttségét, ezek alapján pedig kockázatelemzést kell végeznie. A különféle objektumokra, illetve a biztonságtechnikai megoldásokra más és más

[18] 18/2016. (VIII. 5.) EMMI rendelet a felsőoktatási szakképzések, az alap- és mesterképzések képzési és kimeneti követelményeiről, valamint a tanári felkészítés közös követelményeiről és az egyes tanárszakok képzési és kimeneti követelményeiről szóló 8/2013. (I. 30.) EMMI rendelet módosításáról.

[19] 18/2016. (VIII. 5.) EMMI rendelet 3. melléklete, VII. Műszaki képzési terület, 3. fejezetének 8.1 Szakmai jellemzők című pontja, valamint a 4. melléklet VII. Műszaki képzési terület, 19. fejezetének 9.1 Szakmai jellemzők című pontja alapján.

jogszabályi, adatvédelmi előírások vonatkoznak, amelyeket a rendszerek tervezésénél figyelembe kell vennie. Emiatt nagyon lényeges a biztonságtechnikai tervezők folyamatos képzése, tevékenységük felügyelete.

A bemutatott helyzet a teljes magánbiztonsági ágazat egy nagyon kis szegmensét (a biztonságtechnikai tervezőket) érinti, őket viszont jelentős mértékben. Jelenleg a vagyonvédelmi kamara nem tarthatja nyilván a biztonságtechnikai tervezőket, a mérnöki kamara honlapján pedig nem lehet ilyen jogosultságra keresni, így a tervezésre jogosultakat nem lehet megtalálni.

A helyzetre megoldást jelentene, ha a sokszor ígért vagyonvédelmi törvény módosításával ismét visszakapná a vagyonvédelmi kamara a tervezői névjegyzék kezelését, a jogosultságok megállapítását, valamint a tervezői továbbképzések szervezését. Esetleg további jogkörként megkapná a tervezői tevékenységek ellenőrzését.

Amennyiben a vagyonvédelmi törvény módosítása a fentieket nem fogja tartalmazni, akkor a mérnöki kamara szakmagyakorlási szabályzatának változtatására lenne szükséges, illetve egy önálló szakmai tagozatot kellene létrehozni erre a szakterületre. Erre a tervező- és szakértő mérnökök, valamint építészek szakmai kamaráiról szóló 1996. évi LVIII. törvény 2. § (4) pontja lehetőséget biztosít, mivel a biztonságtechnikai tervezés – a jogszabályban megfogalmazott – jogosultsághoz kötött tervezői mérnöki szakterület.

Irodalomjegyzék

[1] Szécsi Gy.: Bűnmegelőzés, vagy…? *Belügyi Szemle,* 46. évf. 12. szám, 1998, 65–68.

[2] Christián L.: *A magánbiztonság elméleti alapjai.* Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014.

[3] Kiss S.: *A biztonságtechnika alapjai.* Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2003.

[4] http://jogiportal.hu/view/a-szemely–es-vagyonvedelmi-valamint-a-magannyomozoi-tevekenyseg-szabalyairol-szolo-2005-evi-cxxxiii-tv (a letöltés ideje: 2017. 05. 21.)

[5] A Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara (SzVMSzK) biztonságtechnikai és mechanikai vagyonvédelmi rendszert tervezői jogosultság megújításához előírt továbbképzésre vonatkozó szabályzata. Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara, Budapest, 2007.

[6] *Dr. Utassy Sándorra emlékezünk.* Detektor Plusz, Budapest, 17. évf. 7–8. szám, 2010.

[7] Elnökséget választott az MMK Elektronikus Vagyonvédelmi Szakosztálya. www.securinfo.hu/hirek/755-elnokseget-valasztott-az-mmk-elektronikus-vagyonvedelmi-szakosztalya.html (a letöltés ideje: 2017. 05. 31.)

[8] A Magyar Mérnöki Kamara Szakmagyakorlási Szabályzata. http://mmk.hu/tudastar/szabalyzatok/szakmagyakorlasi-szabalyzat.pdf (a letöltés ideje: 2017. 05. 31.)

[9] MMK: *Függelék: A szakmagyakorlási tevékenységek engedélyezésének és bejelentésének eljárási rendje.* http://mmk.hu/tudastar/szabalyzatok/szakmagyakorlasi-fuggelek.pdf (a letöltés ideje: 2017. 06. 08.)

The Situation of Security System Engineers

Attila Tóth

The modified Property Security Act, adopted in 2012 created a difficult situation for the private security sector. Security system engineers fell victim to this change as well, making their situation rather uncertain. In the modified legislative environment, the Chamber of Bodyguards, Property Protection and Private Detectives cannot register security system engineers thus they cannot monitor their professional activity. The well-regulated system monitoring the entitlement to carry out this professional activity, a well-functioning training and certification system and a detailed register that had been functioning earlier is currently unavailable.

Keywords: planning, private security, Chamber of Bodyguards, security technology

Munk Sándor

Kiberbiztonsági szervezetek közötti interoperábilis információcsere-megoldások (sérülékenységek kezelése)

A kibertér informatikai rendszereinek, hálózatainak szolgáltatásai az állami működés, a gazdasági élet és a magánszféra egyre növekvő jelentőségű feltételét képezik. A kibertér biztonságának megteremtése és fenntartása alapvető jelentőségű feladat, amely a kiberbiztonsági szervezetek szoros együttműködését igényli. Az együttműködés feltétele az interoperábilis információcsere. Jelen publikáció célja a sérülékenység kezeléshez kapcsolódó kiberbiztonsági információk cseréjét támogató megoldások bemutatása, és a kiberbiztonsági szervezetek ehhez kapcsolódó feladatainak meghatározása.

Kulcsszavak: kiberbiztonsági információcsere, interoperábilis információcsere, sérülékenység kezelése

Bevezetés

A kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatások napjaink életének egyre fontosabb, folyamatosan növekvő jelentőségű feltételét képezik, befolyásolják az állami működés hatékonyságát, a vállalkozások eredményességét és versenyképességét, az állampolgárok életminőségét. Emiatt egyre növekszik a szerepe a kibertérben jelentkező kockázatok és fenyegetések kezelésének, a megfelelő szintű kiberbiztonság garantálásának.

A kiberbiztonság megteremtése és fenntartása – számos más szereplő mellett – erre a célra létrehozott kiberbiztonsági (információbiztonsági, informatikai biztonsági) szervezetek feladata. Mivel a kibertér informatikai rendszerei, hálózatai globális, szövevényesen összekapcsolódó rendszert alkotnak, az egyik rendszer biztonságának sérülése általában elvezet egy másik rendszer biztonságának sérüléséhez. Ebből következően a kiberbiztonság fenntartása több szereplőre kiterjedő és széles körű együttműködést igényel.

A szereplők, szervezetek közötti együttműködés alapját a kiberbiztonsághoz kapcsolódó információk cseréje képezi, amelyben a feladatok bővülésével, a gyors reagálás szükségességének előtérbe kerülésével a hagyományos, strukturálatlan (telefonos,

szöveges, e-mail) információkra épülő megoldások mellett egyre inkább előtérbe kerülnek a kiberbiztonsági tevékenységet támogató informatikai rendszerek, adatbázisok közötti, emberi közreműködést nem igénylő cserére épülő megoldások.

Az informatikai rendszerek közötti adatcsere eredményességének alapvető feltétele ezen adatok szándékolt jelentésének, értelmezésének megőrzése, az informatikai interoperabilitás. Ennek kialakítása és fenntartása akkor jelent komolyabb feladatot, ha az információcserében (adatcserében) érintett felek között eltérések vannak az adatok értelmezésében. Az eltérések, heterogenitás feloldásának alapvető lehetősége az előzetes egyeztetésre épülő közvetítő reprezentációk kialakítása és alkalmazása.

Jelen publikáció célja, hogy rendszerezze a sérülékenység kezeléséhez kapcsolódó kiberbiztonsági információk cseréjét támogató megoldásokat, és meghatározza a kiberbiztonsági szervezetek ehhez kapcsolódó feladatait. Ennek érdekében a következőkben:

- meghatározzuk az interoperábilis információcsere-megoldás alkalmazott értelmezését, és rendszerezzük ezek alapvető típusait;
- rendszerezzük és jellemezzük a sérülékenység kezeléshez kapcsolódó kiberbiztonsági információcserét támogató megoldásokat;
- végül megvizsgáljuk ezen megoldások szerepét a kiberbiztonsági szervezetek tevékenységében, és meghatározzuk az alkalmazásukhoz szükséges feladatokat.

Jelen publikáció egy nagyobb kutatás részét képezi, amelyben korábban elemeztük a kiberbiztonsági szervezetek főbb típusait, és ezek funkcióit, feladatait, [1] a kiberbiztonsági szervezetek által kezelt, illetve a köztük áramló információkat, és az információcsere alapvető jellemzőit, [2] valamint a kiberbiztonsági információcseréhez kapcsolódó interoperabilitási problémákat, követelményeket. [3]

Ez a publikáció, mint alcíme is jelzi, a kiberbiztonsági információcserén belül a sérülékenységi információk cseréjére összpontosít. Terjedelmi okokból nem foglalkozik a kiberbiztonsági tevékenység más feladataival, mint az eseménykezelés (biztonsági eseménykezelés), a fenyegetéskezelés, vagy a megfigyelt események, tárgyi leletek kezelése. Ezen területek interoperábilis információcsere megoldásainak vizsgálata további kutatások tárgyát kell képezze.

Interoperábilis információcsere-megoldások alapjai

Jelen kutatás tárgyát a kiberbiztonsági szervezetek közötti interoperábilis információcsere-megoldások képezik. A következőkben először meghatározzuk, hogy jelen publikációban mit értünk interoperábilis információcsere-megoldás alatt, majd összegezzük és rendszerezzük ezen megoldások alapvető típusait. Az interoperábilis információcsere-megoldások alapjainak összegzése az információs interoperabilitásra,

illetve az informatikai interoperabilitásra vonatkozó korábbi elképzeléseimre, kutatási eredményeimre épül.

Interoperábilis információcsere-megoldások fogalma, értelmezése

A címben szereplő interoperábilis információcsere-megoldások fogalmának értelmezéséhez először tisztáznunk kell, hogy ezek az információcsere milyen problémájára, feladatára jelentenek megoldást, és hogy mi ennek a megoldásnak a tartalma, lényege, mivel segítik az – esetünkben a kiberbiztonsági szervezetek közötti – információcsere alkalmazói igényeknek megfelelő megvalósítását.

Az *interoperábilis információcsere-megoldás* jelen publikáció értelmezésében egy információs interoperabilitási problémára nyújtott megoldás. Interoperabilitás témánk szempontjából „az együttműködést támogató, az eredményes és hatékony együttes működést biztosító kölcsönös képesség". [4: 22] Az eredményes és hatékony együttműködés pedig elképzelhetetlen a szereplők közötti kiterjedt információcsere nélkül. Ehhez kapcsolódóan „az információs interoperabilitás különböző szereplők kölcsönös képessége információk közös értelmezésen alapuló, a hatékony együttműködéshez szükséges cseréjére". [4: 41]

Információs interoperabilitási probléma nem áll fent, így interoperábilis információcsere-megoldásra sincs szükség, ha az együttműködő felek között nincs eltérés (heterogenitás) a kezelt információk körében, azok értelmezésében, és az együttműködő szereplők közötti cseréjük során alkalmazott formákban, reprezentációkban. Ez azonban elvileg is csak azonos rendeltetésű, közös irányítás alá tartozó, egymással tartós és szoros együttműködésben álló szervezetek esetében lenne lehetséges. Napjaink együttműködési környezeteit viszont – így az együttműködő kiberbiztonsági szervezeteket is – dinamikusan változó partneri kör; rendeltetésbeli, eljárási, értelmezési különbözőségek; illetve az alkalmazott rendszerek, eszközök eltérései jellemzik. A fentiekből következően minden valós együttműködési körben alapvető feladat a szereplők közötti interoperábilis információcsere feltételeinek megteremtése és fenntartása, az ehhez szükséges megoldások kidolgozása és alkalmazása.

Az *interoperábilis információcserére* vonatkozó *megoldások rendeltetése,* hogy feloldja az együttműködő, információt cserélő felek közötti különbözőségeket, amelyek a következő három szinten jelentkezhetnek:

- az információkat hordozó adatok anyagi reprezentációi szintjén (fizikai szint);
- az információkat hordozó adatok formátumának szintjén (szintaktikai szint);
- valamint a fogalmak, az adatokhoz rendelt jelentés szintjén (szemantikai szint).

A különbözőségek, heterogenitás elsődlegesen az egyes szereplők által kezelt információk körében, értelmezésében, valamint az ezeket hordozó adatok formátumában állnak fent. Amennyiben az együttműködő felek információikat (például adatbázisaikat) a partnerek számára elérhetővé teszik, akkor ezek a különbözőségek közvetlenül, ennek hiányában csak közvetve, az információcsere során alkalmazott tartalmon és formátumon keresztül jelentkeznek.

Az interoperábilis információcsere megvalósításának egyik lehetősége a heterogenitás kiküszöbölése. Ez azonban a legtöbb esetben – legalábbis teljes mértékben – nem lehetséges, vagy nem célszerű. Erre egyedül a fizikai szinten van valós lehetőség, mivel itt kialakult néhány széles körben alkalmazott vezetékes és vezeték nélküli megoldás, amelynek alkalmazása könnyen, és felhasználói szempontból „láthatatlanul" megvalósítható. A másik lehetőség a heterogenitás tudomásul vétele, és jelentésmegőrző átalakítások közbeiktatása az információk lekérdezése, vagy az információcsere folyamatába.

Az interoperábilis információcsere-megoldások alapja a gyakorlatban szinte mindig egy *közvetítő reprezentáció,* amelyet az együttműködésben részt vevő felek alakítanak ki, egyeztetnek és fogadnak el. Az információcsere során használt közvetítő reprezentáció (adattartalom, adatcsere formátum és annak egyeztetett előírt értelmezése), valamint az adatcsere eljárásrend együttműködési körön belüli szabványosítása biztosítja az információcsere-igényeket kielégítő információáramlást. [4: 174]

Az egyeztetett közvetítő reprezentáció mint az interoperábilis információcsere-megoldások egyik előnye, hogy szabadságot biztosít az együttműködő felek számára az információcserében érintett információk belső reprezentációjának – saját érdekeiknek megfelelő – meghatározására, módosítására vagy megtartására. Ezzel együtt azonban az együttműködő felekre hárítja a belső reprezentáció és a közvetítő reprezentáció közötti jelentésmegőrző átalakítás feladatát. Ez az átalakítás a két reprezentáció közötti különbözőségek függvényében lehet szükségtelen (nincs eltérés), szűkebb körű (kisebb eltérések) vagy jelentős (jelentősebb eltérések).

Amennyiben egy szereplő csak egyetlen együttműködési csoportnak tagja, akkor csak egy közvetítő reprezentációhoz kell biztosítania a megfelelő átalakítást. A gyakorlatban azonban egy szereplő több együttműködési kör szereplőivel is cserélhet információkat, ebben az esetben több közvetítő reprezentációhoz is kell rendelkeznie átalakítási képességgel. Ezek általában eltérő célokat szolgálnak, így kisebb, vagy jelentősebb egymás közötti különbözőségekkel is rendelkeznek.

Egyetlen közvetítő reprezentáció esetében egy szereplő – amennyiben az információk saját felhasználási igényei, és egyéb feltételek ezt lehetővé teszik – belső reprezentációját a közvetítő reprezentációhoz igazíthatja, és ezzel megszüntetheti, vagy jelentősen csökkentheti a két reprezentáció közötti átalakítás „ráfordításait". Ezt azonban a közvetítő reprezentáció fejlesztése, változásai esetében is fenn kell tartani. Több együttműködési

kör, több közvetítő reprezentáció esetében pedig már általában nincs reális lehetőség a valamennyi közvetítő reprezentációhoz igazított belső reprezentáció kialakítására.

Interoperábilis információcsere megoldásainak típusai

Amennyiben a szereplők közötti heterogenitás feloldása egy egységesen értelmezett közvetítő reprezentáció alkalmazása, a megoldások lényegében a közvetítő reprezentációra, vagy annak egyes összetevőire vonatkozó specifikációk, szabványok. Ezek célja lehet a megosztott információk jelentésének egységesítése (szemantikai szint), az információcsere során használt formátumuk szabványosítása (szintaktikai szint), vagy kiterjedhet mindkettőre.

A kiberbiztonsági szereplők közötti információcseréhez kapcsolódó interoperabilitási megoldások közül a szemantikai szinthez tartoznak az elemi információk lehetséges értékeit rögzítő ellenőrzött szótárak, a fogalmakat hierarchikus osztályokba soroló taxonómiák, valamint a fogalomrendszerek formális specifikációi, az ontológiák. A szintaktikai szint megoldásai közé az üzenet- és adatelem-formátum specifikációk sorolhatók.

Az *ellenőrzött szótár,* felsorolás (controlled vocabulary, enumeration) egy adott elemi információ, egy objektum egy jellemzője lehetséges értékeinek és azok egyértelmű meghatározásainak szabványosított listája. Rendeltetése, hogy biztosítsa a benne szereplő – az információcsere során használt – értékek egységes, következetes, azonos módon értelmezett használatát. [5: 326]

Egy ellenőrzött szótár esetében először meg kell határozni az információ tárgyának, valamint az adott jellemzőnek a fogalmát, majd ezt követően fel kell sorolni a jellemző lehetséges értékeit, amelyek szintén fogalmak. Ezen fogalmak egységes értelmezését a gyakorlatban szöveges leírások biztosítják.

Az ellenőrzött szótárak azonosítást, típusokba sorolást, csoportosítást, osztályozást szabványosítanak. Mivel minden azonosítás, csoportosítás, osztályozás valamilyen célt szolgál, és annak a célnak megfelelő szempontok alapján történik, így különböző felek saját feladataikhoz általában eltérő szótárakat is használnak. Az interoperábilis információcsere során ezért jelentős feladat a saját szótár, és az egyeztetett szótár közötti átalakítás.

Számos interoperabilitási megoldásban találkozunk nyílt szótárakkal (open vocabularies) is, amelyek formailag megegyeznek az ellenőrzött szótárakkal, de megengedik a listában nem szereplő értékek használatát is, amennyiben a listában szereplő értékek nem megfelelőek a megosztandó információ cseréjére. A nyílt szótárak alkalmazása természetesen csak akkor hatékony, ha a bennük szereplő értékek a gyakorlatban előforduló esetek jelentős részében megfelelőek, mivel a listában nem szereplő értékek csak megnevezésükkel tudják jelezni szándékolt értelmezésüket.

A *taxonómia* fogalmak többszintű, hierarchikus osztályokba sorolása, egymással alá-fölé rendelt viszonyban álló fogalmak rendszere. [5: 326] Az információ tárgyát először a legmagasabb szinten sorolják osztályokba, majd az egyes osztályok további, alacsonyabb szintű osztályokra bomlanak. Az így kialakított fogalomrendszer egyrészt lehetőséget biztosít osztályozási jellemzők különböző szintű – átfogóbb vagy részletesebb – megadására, valamint egy adott osztályozási jellemző érték alapján az információ tárgyának más, magasabb szintű osztályokba történő besorolására is.

A kiberbiztonsági információcsere során alkalmazott taxonómiák egy része egyszerűen „csak" egy ellenőrzött lista kiegészítése magasabb szintű csoportosításokkal, osztályokkal. Az információcsere során ebben az esetben csak a legalacsonyabb szintű, legrészletesebb osztályozás értékeit lehet használni. A magasabb szintű osztályokba sorolást, az átfogóbb fogalmak az információk feldolgozása, elemzése, szintetizált, összegzett bemutatása során használják fel.

Az információcsere interoperabilitásának támogatása általában szükségessé teszi azonos jellemzők különböző ellenőrzött listáinak, vagy taxonómiáinak integrálását. Ebben egy olyan taxonómia létrehozása a cél, amelyre jelentésmegőrző leképezhetők a különböző megoldások. Ennek segítségével „felfelé" (a részletesebb osztályozásból az átfogóbb osztályozás felé) megoldható az információmegosztás. „Lefelé" viszont erre csak akkor van lehetőség, ha az ellenőrzött lista tartalmaz „pontosan nem besorolható" tartalmú értéket is.

Az *ontológia* mint tudásreprezentációs eszköz, egy közösen használt fogalomrendszer egyértelmű, formális specifikációja. Rendeltetése, hogy fogalmi alapot, egységesen elfogadott háttérismereteket biztosítson egy alkalmazási terület számára. [5: 327] Egy ontológia alapvető tartalmi összetevői közé entitások (dolgok, tulajdonságok és kapcsolatok) azonosítói (az ontológia „szókészlete"), entitásokból összetettebb entitásokat létrehozó konstrukciós formulák (kifejezések), valamint entitásokra vonatkozó igaznak tekintett állítások (axiómák) tartoznak. A dolgok lehetnek az általános fogalmaknak megfelelő osztályok és az egyedi fogalmaknak megfelelő egyedek. Az ontológia a taxonómia alá-fölé rendeltségi kapcsolatainak körét kibővíti fogalmak közötti tetszőleges kapcsolatok meghatározásának lehetőségével.

Az ontológia szoros kapcsolatban áll az adatmodellezés fogalmi adatmodell fogalmával, amely egy adatbázis, formatizált üzenet, vagy más adatstruktúra adatai által leírt egyedek, tulajdonságok és kapcsolatok formai és fizikai megvalósítástól független – vagyis szemantikai szintű – leírása. Minden adatmodell alapján elkészíthető a megfelelő ontológia, azonban az adatmodellek általában az ontológiánál egyszerűbb, kevesebb szemantikai információt tartalmazó specifikációk, így kiegészítésre szorulnak. Céljuk ugyanis nem egy ismeretanyag reprezentációja, hanem a közreműködés egy adatstruktúra tervezéséhez.

Az ellenőrzött szótárakhoz és taxonómiákhoz hasonlóan az ontológiák is célorientáltak, alkalmazásiterület-specifikusak, így ugyanazon dolgok, tulajdonságok és kapcsolatok eltérő ontológiákkal is leírhatók. Eltérő ontológiát, fogalomrendszert használó szereplők közötti együttműködés, információcsere során a különböző ontológiákat harmonizálni kell, meg kell teremteni az egyikből a másikba, vagy egy közös referencia ontológiára (és így azon keresztül egymásra) történő átalakítás feltételeit.

A gyakorlatban alkalmazott *információcsere szabványosítási megoldásai* három nagyobb csoportba, a dokumentumformátum-szabványok, az üzenetformátum-szabványok és az adatelem-szabványok közé sorolhatók. [4: 188] Ezek közül az *adatelem-szabványok* szűkebb területre – az adatbázisok közötti adatcsere során, vagy a formatizált üzenetekben felhasznált adatelemek egységesítésére – összpontosítanak. A szabványos adatelemek meghatározása magában foglalja az adatelemmel reprezentált információ tartalmi leírását, illetve lehetséges értékeinek és ezek formátumának definiálását, vagy összetett adatelem esetében összetevőinek megadását. A szabványos adatelemek tárházában ugyanazon információ leírására különböző változatok is szerepelhetnek.

A szabványos adatelemekre épül az interoperábilis információcsere egy másik megoldása, az egy közös közvetítő reprezentáció alapját képező *információcsere adatmodell*. Ennek keretében, egy adott alkalmazási terület információcsere igényeit felmérve, egy egységes adatmodellbe rendezve kialakításra kerülnek az ehhez szükséges szabványos adatelemek. Az információcsere adatmodell alapvető jellemzője, hogy abban minden adatelemnek csak egyetlen változata lehet, meghatározva annak tartalmát, formátumát és lehetséges értékeit. Ennek olyannak kell lennie, hogy valamennyi kapcsolódó információcsere igény kielégítését biztosítsa. [4: 191]

Az üzenetformátum-szabványok az információcsere adatmodell tartalmát meghaladóan az információkat hordozó egyes üzenetek tartalmát, formátumát, egyes esetekben az üzenetcsere rendjét, protokollját is szabályozzák. Ezek a szabványok tulajdonképpen egy speciális formális nyelvet definiálnak, amelyen a tervezett információk a szereplők között jelentésmegőrző módon megoszthatók, kicserélhetők. Ez a nyelv általános jellemzőinek leírásán túl azt is meghatározza, hogy milyen formátumú üzenetek a helyesek, és azok tartalmát hogyan kell értelmezni.

Sérülékenységinformációk cseréjének megoldásai

A sérülékenységek olyan hibák vagy gyengeségek egy hardver, vagy szoftver összetevőben, amelyeket egy fenyegetés (támadó) kihasználhat, egy rendszer vagy hálózat biztonságának megsértése során. A sérülékenység kezelés (vulnerability management) egy széles körben használt meghatározás [6] szerint sérülékenységek azonosításának, osztályozásának, megszüntetésének és kockázatuk csökkentésének ciklikus folyamata.

A konkrét sérülékenységek életciklusa felfedezésüktől megszüntetésükig tart, amelyhez több kiberbiztonsági szerep is tartozik:

- a kiértékelő fedezi fel a sérülékenységet, és tájékoztatja erről a kiberbiztonsági szervezetet, vagy az érintett összetevő gyártóját;
- a gyártó dolgozza ki és adja közre a sérülékenységet megszüntető javítást;
- a kiberbiztonsági eseménykezelő szervezet segíti a kapcsolatot a kiértékelő és a gyártó között, és nyújt segítséget a sérülékenység elhárításában. [7: 2–3]

A sérülékenységek feltárása, elemzése, értékelése történhet többféle kiberbiztonsági szereplőnél is (kiberbiztonsági eseménykezelő központok, speciálisan e célra létrejött szervezetek, informatikai összetevőket gyártó cégek), a sérülékenységek korlátozása, vagy megszüntetése pedig a kiberbiztonsági műveleti központok feladata.

A sérülékenységek kezelésének részeként az érintett szereplők a következő információkat oszthatják meg, cserélhetik egymás között:

- a sérülékenységek azonosítására vonatkozó információk;
- a sérülékenységek értékelésére vonatkozó információk;
- az érintett informatikai összetevőkre vonatkozó információk;
- a konfigurációs beállításokra vonatkozó információk;
- sérülékenységvizsgálatokra vonatkozó információk.

A sérülékenységek mellett a konfigurációs beállítások is jelentős mértékben befolyásolják egy rendszer, hálózat biztonságát. A helytelen beállítások biztonsági kockázatot jelentenek, a beállítások megfelelő megválasztásával az érintett rendszer biztonságosabb lesz (hardening). Ebből következően a sérülékenységek mellett a javasolt konfigurációs beállításokra vonatkozó információk cseréje is a biztonsági kockázatok kezelésének része.

A szakirodalomban több publikáció foglalkozik a kiberbiztonsági információk cseréjét, megosztását támogató megoldások áttekintésével, összehasonlító elemzésével. Az Európai Hálózat- és Információbiztonsági Ügynökség egy 2014-es dokumentuma [8] 53 információcsere-szabványt és -eszközt dolgoz fel, amelyeket öt csoportba sorol: alacsony szintű adatformátumok, megfigyelési alapadatok (observables), ellenőrzött szótárak (enumerations), mérési keretrendszerek, és jelentési formátumok. Egy 2015-ös konferencia-előadás [9] 24 adatformátumot és protokollt mutat be hat alkalmazási területre csoportosítva: erőforrás-nyilvántartás, konfigurációs útmutató, sérülékenységelemzés, fenyegetéselemzés, behatolásjelzés és eseménykezelés. Végül egy 2017-es konferencia-előadás [10] 14 ellenőrzött szótárat, mérési keretrendszert és megosztási szabványt, valamint 13 ontológiát tárgyal.

A következőkben ezek közül az információcsere-megoldások közül a sérülékenységkezeléshez kapcsolódóakat vesszük sorra.

Sérülékenységinformációk azonosításának megoldásai

A sérülékenységi információk cseréjének alapvető eleme az azonosító. A kiberbiztonsági színtéren több sérülékenység-adatbázis működik, amelyek közül azonban kiemelkedik a MITRE cég által kezelt *Sérülékenységek Listája* (Common Vulnerabilities and Exposures, CVE), az Egyesült Államok arra épülő, azt kiegészítő *Nemzeti Sérülékenység Adatbázisa* (National Vulnerability Database, NVD). Mindkettő azonosítója a CVE-azonosító, amelynek egyediségét egy eljárás- és szervezetrendszer biztosítja. [11]

2004–2016 között működött az Open Security Foundation által üzemeltetett, közösségi alapú *Nyílt Forrású Sérülékenységi Adatbázis* (Open Source Vulnerability Database, OSVDB), saját azonosítóval, amelyben leállításakor több sérülékenység szerepelt (mintegy 60 ezer), mint a CVE-ben (mintegy 45 ezer). [12]

Napjainkra a CVE-azonosító vált de facto információcsere szabvánnyá, számos információcsere formátumban jelenik meg összetevőként. Emellett természetesen léteznek más szervezetek, mindenekelőtt gyártó cégek, illetve kiberbiztonsági eseménykezelő szervezetek által fenntartott, saját céloknak megfelelő sérülékenység-adatbázisok saját azonosítóval, ezeket az azonosítókat azonban csak korlátozottan (cégen belüli, vagy a felügyelt szervezetekkel folytatott információcsere körében) használják fel.

Szükséges megjegyezni, hogy – mint azt az első CERT egy tanulmánya [13] is tartalmazza – a CVE-azonosítónak is vannak korlátai. Kiterjedése korlátozott, nem minden sérülékenységhez kerül hozzárendelésre CVE-azonosító, nem minden CVE-azonosítóhoz tartozik megfelelő rekord a CVE-adatbázisban. Nem egyértelmű az „elemi sérülékenység" fogalma, hogy egyes jelentésekhez egy, vagy több CVE-azonosítót rendeljenek hozzá. Az USA Nemzeti Sérülékenységi Adatbázisa történelmi okokból a hagyományos számítástechnikai platformokat (Windows, Linux, OS X, Unix-szerű operációs rendszerek) érintő sérülékenységekre összpontosít, és csak felületesen tartalmazza más platformok (például mobil, beágyazott rendszerek, webhelyek, felhőszolgáltatások) sérülékenységeit.

Sérülékenységértékelési információk cseréjének megoldásai

A sérülékenységek cseréje, megosztása során továbbíthatják a sérülékenység osztályozását, az érintett informatikai összetevők körét, a kihasználás feltételeit és következményeit, valamint a sérülékenység súlyosságát.

A *sérülékenységek osztályozásának* széles körben alkalmazott megoldása a MITRE cég *Gyengeségek Felsorolása* (Common Weakness Enumeration, CWE), amely a szoftver gyengeségek típusainak szervezett, belső kapcsolatokat tartalmazó listája, és amelyet az NVD használ a CVE-lista elemeinek besorolására. A lista 2008-ban jelent meg, jelenlegi 3.1 verziójában [14] a több mint 700 egyedi gyengeségtípus között mintegy

90 gyengeségosztály, több mint 300 alapgyengeség és mintegy 300 gyengeségi változat található.

A CWE mellett léteznek más osztályozások is, amelyek közül jelentősebb szerepet egy nyílt nonprofit szervezet, az OWASP sérülékenységlistájának osztályozása játszik. A szervezet háromévente bocsátja ki a *Tíz Legkritikusabb Biztonsági Kockázatú Webalkalmazás* című *(OWASP Top 10)* listáját, [15] amely mindig tíz átfogó sérülékenységkategóriát tartalmaz. Az egymás utáni kiadványok kategória listája értelemszerűen változik. A CWE osztályozási rendszer (több más mellett) leképezéseket tartalmaz az egyes OWASP Top 10-es listákra.

Sem a CWE, sem az OWASP Top 10 kategória listának nem létezik a szövegestől eltérő szabványosított formátuma. A CWE-azonosítókat (CWE-9…99) több információcsere-formátumban felhasználják.

A *Sérülékenységmérési Rendszer* (Common Vulnerability Scoring System, CVSS) egy szabványos értékelésirendszer-megoldás a sérülékenységek alapvető jellemzőinek megadására és súlyosságának értékelésére. A 2004-ben létrehozott értékelési rendszer kezelője az Eseménykezelő és Biztonsági Csoportok Fóruma (Forum of Incident Response and Security Teams, FIRST), jelenlegi 3.0 változata 2015 júniusában jelent meg. [16]

A CVSS három értékelési jellemzőcsoportot tartalmaz. Az alapvető jellemzők közé a kihasználhatóság négy jellemzője, a hatókör kibővítése és a biztonság összetevőire gyakorolt hatás tartozik. Az időben változó jellemzők: a kihasználhatóság szintje, a rendelkezésre álló megoldás szintje, és a jelentés megbízhatósága. Végül a külső jellemzők közé tartoznak a biztonság összetevőire vonatkozó követelmények, valamint a módosító tényezők.

Az egyes jellemzőkhöz kötött értékkészlet, és azokhoz numerikus értékek tartoznak, amelyek alapján egy 0–10 közötti CVSS-pontszám keletkezik, ami egy ötfokozatú súlyossági skálára is leképezésre kerül (0 = nincs; 0.1–3.9 = alacsony; 4.0–6.9 = közepes; 7.0–8.9 = magas; 9.0–10.0 = kritikus). A CVSS az értékelés eredményének cseréjére az értékelési vektor karaktersorozat formátumát szabványosítja, de létezik szabványos XML-formátum is.

A *Gyengeségmérési Rendszer* (Common Weakness Scoring System, CWSS) a CWE-listában szereplő szoftvergyengeségek alapvető jellemzői megadásának és súlyossága értékelésére kidolgozott, a CVSS-hez hasonló szabványos értékelési rendszer. A szabványt a MITRE cég dolgozta ki 2008-ban, 1.0.1 változata 2014-ben jelent meg. [17] A megoldást 2015-ben a Nemzetközi Távközlési Unió is szabványosította. [18]

A CWSS három értékelési jellemző csoportot tartalmaz. Az alapvető jellemzők közé a technikai hatás, megszerezhető jogosultság, megszerezhető jogosultság szint, belső biztonsági intézkedés hatékonyság, megítélés megbízhatósága tartozik. A támadási felület jellemzői: szükséges jogosultság, szükséges jogosultsági szint, elérési vektor, hitelesítés erőssége, emberi közreműködés szintje, telepítettség köre. Végül a külső jellemzők közé

tartozik a szervezeti hatás, felfedezés valószínűsége, kihasználás valószínűsége, külső biztonsági intézkedés hatékonysága, előfordulás gyakorisága.

A CWSS-ben – a CVSS-hez hasonlóan – az egyes jellemzőkhöz kötött értékkészlet, és azokhoz numerikus súlyok tartoznak, amelyek alapján a három jellemzőcsoportra részpontszám (0–100, 0–1, 0–1), majd ezek összeszorzásával egy 0–100 közötti CWSS pontszám keletkezik. A CWSS az értékelés eredményének cseréjére az értékelési vektor karaktersorozat formátumát szabványosítja.

A *Közös Sérülékenység Jelentési Keretrendszer* (Common Vulnerability Report Framework, CVRF) egy XML-alapú nyelv, amelynek segítségével a különböző szereplők szabványos módon oszthatnak meg egymással kritikus sérülékenységi (és más kiberbiztonsági) információkat. A megoldást az ICASI ipari konzorcium dolgozta ki 2011-ben, jelenlegi 1.1 verziója 2012 májusában jelent meg. [19] A CVRF a teljes sérülékenység kezelési életciklust támogatja a felfedezéstől, a javítócsomag telepítéséig. Egy CVRF-dokumentum (jelentés) két alapvető tartalmi eleme a sérülékenységeket, valamint az érintett informatikai összetevőket (termékeket) leíró rész.

A sérülékenységek esetében a CVRF saját belső azonosítót használ, a leíró információk közé pedig a megnevezés, a felfedezés dátuma, a közzététel dátuma, a küldő fél típusa és részvételi állapota, a CVE-azonosító, a CWE-azonosító és -leírás, érintett összetevők állapota, fenyegetések (hatás, kihasználhatóság állapota, célok), CVSS-értékelés, rendelkezésre álló megoldások, valamint hivatkozások, megjegyzések, és köszönetnyilvánítások tartozhatnak. A megoldás csak néhány saját ellenőrzött szótárat tartalmaz.

Az érintett erőforrások információcseréjének megoldásai

Valamennyi sérülékenység meghatározott erőforrásokhoz, azok csoportjához kapcsolódik, így a sérülékenységinformációk interoperábilis cseréjének alapvető feltétele az érintett erőforrások egyértelmű azonosítása. Ezen a területen több javasolt, gyakorlatban is alkalmazott megoldással találkozhatunk.

A *Platformok Felsorolása* (Common Platform Enumeration, CPE) informatikai összetevők strukturált megnevezéseinek listája. A lista rendeltetése egy szervezet informatikai erőforrásai egyértelmű, szabványos módon történő azonosításának és leírásának támogatása. A lista első változatát a MITRE cég adta ki 2007-ben, 2010 óta az Egyesült Államok szabványosítási szervezete kezeli, aktuális változata a 2011-ben kibocsátott 2.3 verzió. [20]

A CPE az informatikai összetevők (termékek) következő információit tartalmazza: típus (alkalmazás, operációs rendszer, hardver), gyártó, terméknév, verzió, módosítás, szoftverkiadás, szoftverplatform, hardverplatform és nyelv. Az informatikai összetevő

egyértelmű azonosítója (strukturált megnevezése) megjeleníthető URI-formátumban és formatizált karaktersorozat formájában.

A *Szoftverazonosító Címkék* (Software Identification Tags, SWID) megoldás a telepített szoftvereket egyértelműen és hitelesen azonosító információk leírását, valamint ezeknek az információknak az elhelyezésére, alkalmazására vonatkozó követelményeket határozza meg. A szabványos megoldást a TagVault cég dolgozta ki, első változatát a Nemzetközi Szabványosítási Szervezet 2009-ben szabványosította. [21]

A szabvány 7 kötelező és mintegy 30 opcionális előre definiált címkét tartalmaz, amelyek felhasználó által definiált címkékkel tetszőleges módon bővíthetők. Az SWID-címkék szabvány által meghatározott XML-formátumban adhatók meg és cserélhetők.

A sérülékenységekkel érintett informatikai összetevők (termékek) leírását az előző pontban ismertetett *Közös Sérülékenység Jelentési Rendszer* is lehetővé teszi. Ezek esetében a CVRF saját belső azonosítót használ, a teljes terméknév kötelező megadásával, és lehetővé teszi a CPE-azonosító megadását is. Az egyedi termékek számos szempont alapján hierarchikus csoportokba szervezhetők, illetve köztük különböző kapcsolatok adhatók meg. [19]

Erőforrás-információk megosztását, cseréjét támogathatja az Egyesült Államok Szabványosítási Szervezetének két szabványa, az *Erőforrás-azonosítás* (Asset Identification, AID) és az *Erőforrás Jelentési Formátum* (Asset Reporting Format, ARF). Ezek nem kapcsolódnak közvetlenül a sérülékenységekhez, rendeltetésük az erőforrás-nyilvántartás támogatása, azonban egy szervezeten belül, illetve a kiberbiztonsági műveleti központok és a kiberbiztonsági eseménykezelő központok között felhasználhatók az informatikai erőforrásokra vonatkozó információk cseréjére. A két szabvány első változata 2010-ben jelent meg, jelenleg a 2011-es 1.1 változat van érvényben. [22] [23]

Az *Erőforrás-azonosítás* hét erőforrástípus (személy, szervezet, rendszer, szoftver, adatbázis, hálózat, szolgáltatás, adat, számítástechnikai eszköz, áramkör, webhely) leírását szabványosítja, de ezek köre bővíthető. Az egyes típusok azonosítását különböző jellemzők támogatják, további leírásukra típusonként eltérő számú, 1–6 jellemző használható, köztük különböző kapcsolatok írhatók le. A fenti információk XML-formátumban adhatók meg, cserélhetők.

Az *Erőforrás Jelentési Formátum* az Erőforrás-azonosítás szabvány szerinti erőforrás-leírásokat egészíti ki jelentési igények, jelentések, köztük fennálló kapcsolatok, és kiegészítő információk jelentéscsomag formájában történő szabványosításával. A jelentési igények meghatározhatók több más XML-alapú szabványos kiberbiztonsági információcsere formátumban is.

Konfigurációs információk cseréjének megoldásai

A rendszer biztonságát növelő konfigurációs beállítások cseréjének a sérülékenységekhez hasonlóan alapvető feltétele az egyes konfigurációs beállítások egyértelmű azonosítása. Emellett szükség van a konfigurációs beállítások ellenőrzési rendjét leíró, valamint a hibák súlyosságát értékelő információk cseréjére.

A *Konfigurációs Beállítások Felsorolása* (Common Configuration Enumeration, CCE) a különböző dokumentumokban, köztük kiberbiztonsági útmutatókban szereplő elemi – esetleg paraméterekkel rendelkező – konfigurációs beállítások egyértelmű azonosítóval ellátott listája.

A szabványos listát a MITRE cég hozta létre 2007-ben, felügyeletét jelenleg a NIST szabványosítási szervezet végzi, aktuális változata a 2013-ban kiadott CCE v5. [24] A lista a konfigurációs beállításokat az 5. verziótól kezdve a főbb platformok szerint csoportosítva tartalmazza. A konfigurációs beállítások felhasználhatók konfigurációkezelési, vagy biztonsági ellenőrző, értékelő rendszerekben. A lista Microsoft Excel táblázat formájában kerül közreadásra, de rendelkezésre áll XML-formátumban is.

A *Kiterjeszthető Konfigurációs Ellenőrző Lista Formátum* (Extensible Configuration Checklist Description Format, XCCDF) biztonsági ellenőrzőlisták XML-alapú szabványos formátuma, amely támogatja ezen ellenőrző listák automatizált futtatását. Az XCCDF első változatát 2005-ben adta ki a NIST, aktuális változata a 2012-es 1.2 változat. [25]

Az ellenőrzőlista egy adott típusú rendszerre vagy platformra érvényes szabályok szervezett, testre szabható rendszere, amely felhasználható egy rendszer biztonsági állapotának meghatározására, vagy előírt biztonsági előírásoknak való megfelelés ellenőrzésére. Egy ellenőrzési szabályra megadható az (esetleg összetett) ellenőrzési kritérium, amely valamely szabványos ellenőrzési nyelven (például OVAL, OCIL, lásd később) írható le. A szabály az ellenőrzési kritérium mellett többek között tartalmazhatja a követelménynek történő megfeleléshez szükséges tevékenységet, a nem teljesülés súlyosságát. Az XCCDF egységesíti az ellenőrzés egyes szabályok ellenőrzésének eredményei alapján kialakított összegzett eredményének formátumát is.

A *Konfigurációs Mérési Rendszer* (Common Configuration Scoring System, CCSS) a szoftver biztonsági konfigurációs beállítás sérülékenységek súlyosságának értékelésére kidolgozott a CVSS-hez és CWSS-hez hasonló szabványos értékelési rendszer. A szabvány első tervezetét a NIST 2008-ban bocsátotta ki, az 1.0 változat 2010-ben jelent meg. [26]

A CCSS három értékelési jellemző csoportot tartalmaz. Az alapvető jellemzők közé a kihasználhatóság (támadási vektor, szükséges jogosultság, elérés összetettsége), illetve a biztonság három összetevőjére gyakorolt hatás tartozik. Az időben változó jellemzők: általános kihasználhatósági szint, és a rendelkezésre álló megoldás általános szintje.

Végül a külső jellemzők közé tartozik a helyi kihasználhatóság (a sérülékenység helyi előfordulási mértéke, a támadás helyi valószínűségének megítélése, a megoldás helyi rendelkezésre állása), valamint a helyi hatás (a biztonság összetevőire vonatkozó követelmények, járulékos károk lehetősége).

Az egyes jellemzőkhöz kötött értékkészlet, és azokhoz numerikus értékek tartoznak, amelyek alapján egy 0–10 közötti CCSS-pontszám keletkezik. A CCSS az értékelés eredményének cseréjére az értékelési vektor karaktersorozat formátumát szabványosítja.

Sérülékenységellenőrzési információk cseréjének megoldásai

A sérülékenységkezelés alapvető feladata a folyamatos ellenőrzés, a biztonsági követelményeknek történő megfelelés ellenőrzése, és az eredmények értékelése. Ennek hatékonyságát automatizált eszközök segíthetik, így az információcsere részét képezik a sérülékenység-ellenőrző tesztek leírásai, és azok eredményei. Erre két megoldás is született, az egyik a teljesen automatizált tesztelésre, a másik a személyes felhasználói közreműködésre épülő. Emellett az Egyesült Államok központi kiberbiztonsági szervezete létrehozott egy átfogó keretrendszert is.

A *Nyílt Sérülékenység és Értékelő Nyelv* (Open Vulnerability and Assessment Language, OVAL) sérülékenységellenőrző tesztleírások és teszteredmények megosztását, automatizált tesztelést támogató XML-alapú szabványosított nyelv. A nyelv legtöbb eleme tartalmaz a konkrét platformokhoz igazodó bővítési lehetőségeket. A nyelvet a MITRE cég hozta létre 2002-ben, 2015 óta a Center for Internet Security felügyeli, aktuális változata az 5.11.2. [27]

Az OVAL-nyelv alapvető összetevőit a sérülékenységelemzés során felhasznált konfigurációs információkat, a sérülékenységet ellenőrző teszteket, és az ellenőrzés eredményét leíró részek képezik. A tesztesetek az érintett rendszer állapotára vonatkozó elemi ellenőrzések logikai függvényei. Egy elemi teszt egy objektum és egy, vagy több állapot (jellemző) közötti előírt viszony. Az ellenőrzés eredményét a végrehajtott tesztesetek köre, az értékelt rendszer megfigyelhető állapota, és az értékelés részletes eredményei képezik.

A *Nyílt Interaktív Ellenőrzési Nyelv* (Open Checklist Interactive Language, OCIL) egy teljesen automatizáltan végre nem hajtható, felhasználói közreműködésre (kérdésreválaszra) épülő kiberbiztonsági ellenőrzést leíró XML-alapú nyelv. A nyelvet a MITRE cég hozta létre 2008-ban, jelenleg a NIST felügyeli, aktuális változata a 2011-ben megjelent 2.0. [28]

A nyelv alapvető eleme a kérdőív (teszt), amely kérdésekből áll. Az egyes kérdésekre adott válasz vagy meghatározza az eredményt, vagy újabb kérdés feltételéhez vezet. A kérdések lehetnek eldöntendők, illetve numerikus, szöveges vagy listából választható

választ várók. Az egyes kérdések vagy a teljes teszt eredménye lehet: sikeres, sikertelen, ismeretlen, hibás, nem alkalmazható, kihagyott.

A *Biztonsági Tartalom Automatizált Kezelésének Protokollja* (Security Content Automation Protocol, SCAP) egy XML-alapú keretrendszer, amely szabványok egész sorozatára építve támogatja az automatizált sérülékenységkezelést, -vizsgálatot valamint egy szervezetben üzemeltetett rendszerek előírásoknak történő megfelelősége ellenőrzését. Az SCAP gyakorlatilag az Egyesült Államok Nemzeti Sérülékenység Adatbázisának (NVD) alapja, amely formailag egy SCAP-alapú biztonsági információ gyűjtemény. Az SCAP első változatát a MITRE cég dolgozta 2006-ban, a szabvány kezelője a NIST, aktuális változata a 2018-ban megjelent 1.3 verzió. [29]

Az SCAP alapját képező (az előzőekben ismertetett) összetevők a következők:

- biztonsági ellenőrzéseket, értékeléseket leíró nyelvek: XCCDF, OVAL, OCIL;
- jelentési formátumok: ARF, AI;
- azonosítási szabványok: CPE, SWID-címkék, CCE, CVE, CWE;
- mérési rendszerek: CVSS, CCSS.

Egy SCAP-dokumentum lehet leíró- vagy eredménydokumentum. A biztonsági előírásokat, teszteket rögzítő SCAP leíró dokumentumokat tartalom-előállítók készítik, és adják közre. Ezeket a felhasználók alkalmazzák, dolgozzák fel és állítanak elő ezek alapján eredménydokumentumokat. Egy leíródokumentum egy XML-keret, amely egy vagy több leírást, és az ezek által felhasznált – az alapot képező szabványok formátumában megadott – összetevőket foglal magában. Az SCAP eredménydokumentumok egy vagy több SCAP leíródokumentum feldolgozásának – szintén az alap szabványok formátumában megadott – eredményeit tartalmazzák.

Kiberbiztonsági szervezetek interoperábilis információcsere-megoldásokhoz kapcsolódó lehetőségei, feladatai

A rendelkezésre álló kiberbiztonsági információcsere-megoldások az egyes kiberbiztonsági szervezetek számára egyrészt lehetőséget, másrészt kényszert, feladatot jelenthetnek ahhoz, hogy más szereplőkkel interoperábilis módon információt tudjanak cserélni. Lehetőséget egy már meglévő és kipróbált eszköz alkalmazására, vagy kényszert, amelyet egy már létező együttműködési körhöz való csatlakozás von maga után. A következőkben először megvizsgáljuk, hogy az információcsere-megoldások milyen szerepet játszanak egy kiberbiztonsági szervezet életében (milyen figyelmet kell rájuk fordítaniuk), majd elemezzük, hogy a szervezeteknek az információcsere-megoldások alkalmazásához milyen feladatokat kell megvalósítaniuk.

Kiberbiztonsági információcsere-megoldások szerepe, jelentősége

Az interoperábilis információcsere-megoldásoknak az egyes kiberbiztonsági szervezetek életében betöltött szerepét, jelentőségét elsősorban két tényező befolyásolja. Elsőként – és közvetlenül – a más szereplőkkel aktuálisan folytatott kiberbiztonsági információcsere jellege: hogy az hagyományos, vagy elektronikus, és ha az utóbbi, akkor azon belül strukturálatlan, vagy félig strukturált/strukturált. A második – közvetve befolyásoló, de hosszabb távon jelentősebb – tényező pedig a szervezetek tevékenysége: hogy milyen feladatokat látnak el, és ezek során milyen kiberbiztonsági információkat osztanak meg, cserélnek másokkal.

A *kiberbiztonsági információcsere jellege,* amennyiben az hagyományos módon, vagy elektronikus úton, de strukturálatlan formában (például szöveges e-mail-üzenetekkel) történik, látszólag feleslegessé teszi az előzőekben bemutatott információcsere-megoldások figyelembevételét. A kiberbiztonsági szereplők ezen megoldások alkalmazása nélkül is képesek információkat cserélni egymással, sőt napjainkat még elsősorban a hagyományos megoldások alkalmazása jellemzi. Ebben az esetben az információcsere „interoperabilitását", az átviendő információk jelentésének megőrzését a (szak)emberi tudás, a szükség esetén „fejben" történő átalakítás biztosítja.

Az egyes megoldások gyakorlati alkalmazásáról kevés információ áll rendelkezésre a szakirodalomban. A bemutatott megoldások legszélesebb körben az Egyesült Államok kiberbiztonsági szervezetei körében alkalmazzák, amit az is magyaráz, hogy ezek nagy része az Egyesült Államok kiberbiztonsági rendszerében született meg, és annak felügyelete alá is tartozik. Ez sem jelent azonban kiterjedt használatot. Az európai szervezetekről az ENISA egy 2013-as anyaga szerint tíz adatcsere-formátumból csak három van használatban. Az alkalmazott formátumok túlnyomó többsége szintaktikai szinten XML- vagy CSV-alapú volt (egy szervezet használt JSON-alapú megoldást). [30: 25]

Az *ENISA 2017-es fenyegetéseket feltérképező jelentése* külön kiemeli, hogy a kiberfenyegetés elleni információszerzés és -értékelés (hírszerzés) (Cyber Threat Intelligence, CTI) automatizált támogatása korlátozott. „A strukturáltfenyegetés-információk különböző szabványainak létezése ellenére a jelentések szerint még mindig a CSV a leggyakrabban használt formátum. Ez a CTI-szabványok által igényelt (előre)strukturált formátumok iránti viszonylag alacsonyabb szintű igényt jelzi. Bár a fogadó oldalon CTI-szabványokat használnak, a generált hírcsatornák többnyire hatékonyabb, egyszerűbb CSV-fájlokat szolgáltatnak. Sok esetben tömeges adatfeldolgozás esetén a CSV-formátum használata teljesítménybeli kérdésekhez kapcsolódik. Ezenkívül a CSV használatának egyik fő oka kontextusfüggetlen jellege lehet. Egy másik ok a rendelkezésre álló képességekhez kapcsolódhat." [31: 17]

Egyetértés van abban, hogy a szabványosított megoldások (információcsere-formátumok) alkalmazása növeli az interoperabilitást, és az információcsere sebességét. A nem strukturált formátumok cseréje alkalmas lehet áttekintő fenyegetésjelentések, vagy egyedi jelzéseket hordozó információk megosztására, amely elsősorban a kiberbiztonsági szakemberek számára, és nem gépi feldolgozásra szól. Ezek azonban fenyegetés-, sérülékenységjelzések időkritikus cseréjére, és automatizált feldolgozására már nem alkalmasak.

Mindez arra a következtetésre vezet, hogy nem az aktuális, nem a strukturált információcsere jellege határozza meg elsősorban a szabványos információcsere-megoldások szerepét. Előre kell tekinteni, és már előre fel kell készülni ez utóbbi megoldások alkalmazására, amely elkerülhetetlen, meg kell vizsgálni, hogy mely megoldások alkalmazása várható, és ezek alkalmazásához milyen feladatok végrehajtása szükséges.

Elsődlegesen tehát a *kiberbiztonsági szervezetek által végzett feladatok* határozzák meg, hogy egy kiberbiztonsági szervezetnek, szereplőnek kell-e egy megoldással foglalkoznia, befolyásolja-e tevékenységét. Ez pedig azon múlik, hogy az adott tevékenységek használnak-e fel az adott megoldás által hordozott információkat, az adott szervezetnek kell-e ilyeneket más szereplőknek küldenie, kaphat-e más szereplőktől ilyen információkat. A következőkben a feladatok elemzését az első kiberbiztonsági eseménykezelő szervezetet létrehozó egyetem kézikönyvében [32] foglaltakra alapozzuk, azok közül három esetében egyértelműen igazolható az információcsere-megoldások szerepe.

A *sérülékenységek kezelése* részeként az eseménykezelő központok különböző forrásokból fogadnak, szereznek sérülékenységekre vonatkozó információkat, értékelik azok jelentőségét a felügyelt szervezeteikre (érintik-e azokat), vagy más eseménykezelő központok számára, majd az információmegosztási irányelvek alapján továbbítják az értékelt, esetleg kiegészített információkat, szükség esetén az érintett gyártó számára. [32: 28] Az üzemeltetést közvetlenül támogató kiberbiztonsági műveleti központok elsősorban fogadnak sérülékenységekre vonatkozó információkat, végrehajtják ezen sérülékenységek keresését az üzemeltetett rendszerben, hálózatban, majd megteszik a megszüntetéshez szükséges lépéseket.

A *kiberbiztonsági ellenőrzések és értékelések* [32: 30] részét képezi, hogy a szervezet által meghatározott, valamint az iparági szabványokban, bevált gyakorlatokban foglalt követelmények alapján folyamatosan és részletesen felülvizsgálják és elemzik az üzemeltetett rendszer összetevőit, hogy tartalmaznak-e ismert sérülékenységeket. Ehhez a kiberbiztonsági eseménykezelő központok más szereplőktől átvesznek és kidolgoznak, a felügyeletük alá tartozó kiberbiztonsági műveleti központok pedig fogadnak és felhasználnak sérülékenység-ellenőrzési információkat, majd utóbbiak jelentik az ellenőrzés eredményét az őket felügyelő eseménykezelő központoknak. A hatósági jogkörrel rendelkező kiberbiztonsági szervezetek maguk is végezhetnek sérülékenység-ellenőrzést, illetve megfelelőségvizsgálatot.

A *rendszerek, alkalmazások, infrastruktúrák konfigurációja és karbantartása* [32: 31] azt célozza, hogy az üzemeltetett összetevők beállításai, konfigurálása megfeleljen az előírt biztonsági követelményeknek. Ehhez a kiberbiztonsági eseménykezelő szervezetek nyújtanak iránymutatást konfigurációs információk, ellenőrzőlisták közreadásával, vagy működnek közvetlenül is közre ezek ellenőrzésével, érvényesítésével. A konfigurációs beállítások ellenőrzése szintén képezheti részét a megfelelőségvizsgálatnak.

Összességében tehát megállapítható, hogy az előző pontban bemutatott valamennyi információcsere-megoldás olyan kiberbiztonsági információk megosztását, cseréjét támogatja, amelyek alapvető szerepet játszanak a kiberbiztonsági szervezetek tevékenységében, alapfeladataik ellátásában.

Kiberbiztonsági információcsere-megoldások alkalmazásának feltételei, feladatai

Ahhoz, hogy egy kiberbiztonsági szervezet egy adott információcsere-megoldást alkalmazzon, részt vegyen egy erre a megoldásra épülő együttműködési környezetben, kapcsolatban, meghatározott feltételeknek kell eleget tennie. Az alkalmazásra kerülő megoldás megválasztása lehet előírt, vagy saját döntésen alapuló.

Egy együttműködési kör már létező információcseréjéhez történő csatlakozás esetén a csatlakozó kiberbiztonsági szereplőnek nincs választási lehetősége, olyan megoldást kell választania és alkalmaznia, amelyet az együttműködési kör már használ. Egy (vagy több) megoldás kiválasztására tehát közös mérlegelés, egyeztetés alapján csak akkor van szükség, amennyiben két fél, vagy egy együttműködési kör még nem használ informatikai alapú információcserét, de döntött annak bevezetéséről.

Egy információcsere-megoldás alkalmazásának alapvető feltétele – amelyből további feltételek, feladatok következnek – az, hogy a szervezetnek képesnek kell lennie saját információit az alkalmazott belső formátumról az adott megoldás szabványos közvetítő formájára alakítani, illetve erről a formáról a saját belső formátumára alakítani. Ennek vannak tartalmi (szemantikai) és formai (szintaktikai) összetevői.

A *választott információcsere-megoldás alkalmazásának szemantikai feltétele,* hogy az adott szervezet által alkalmazott (formálisan megfogalmazott vagy a kezelt információkból levezethető) *fogalmi modell, ontológia összhangban legyen* az adott megoldás mögött álló fogalmi modellel. Ami azt jelenti, hogy az elemi információk által leírt dolgok (objektumok), azok jellemzői, és a köztük lévő kapcsolatok az együttműködéshez, az információcsere céljához szükséges mértékű pontossággal megfeleltethetők legyenek egymásnak. Ez a feltétel viszonylag könnyen teljesíthető, mert a sérülékenységkezelés alapvető fogalmainak (sérülékenység, érintett erőforrás, gyártó stb.) értelmezése a kiber-

biztonsági szervezetek körében viszonylag egyértelmű. Ha eltérések vannak, akkor azok inkább a részletesebb és az átfogóbb leírás számlájára írhatók.

A következő – magától értetődő, de nem feltétlenül teljesülő – feltétel az, hogy az adott kiberbiztonsági szervezet *rendelkezzen azokkal az információkkal,* amelyeket más szervezeteknek meg kell küldenie, más szervezetekkel meg kell osztania. A hagyományos, vagy strukturálatlan információcseréről a szabványos információcsere-megoldásokra történő áttérés során tehát feladatként jelenhet meg a korábban nem kezelt, rendelkezésre nem álló információk beépítése a kiberbiztonsági szervezet eljárási rendjébe, informatikai rendszerébe.

Erre természetesen csak az információcsere-megoldás kötelezően megadandó információi esetében van szükség, a nem kötelező információk esetében nem. Éppen ennek a feladatnak a csökkentése, és a minél szélesebb körben történő alkalmazhatóság érdekében a szabványos információcsere-megoldások jellemzően csak a legfontosabb információk kötelező megadását írják elő, az ezeket kiegészítő, akár jelentős információk pedig a választhatóan megadandó körbe tartoznak.

Egy információcsere-megoldás alkalmazásának fontos feltétele a kiberbiztonsági szervezet által alkalmazott *azonosító rendszerek összhangja* az adott megoldásban alkalmazott azonosító rendszerekkel. Ez a sérülékenységek esetében egy viszonylag könnyen biztosítható feltétel, mivel bár a kiberbiztonsági szervezetek jelentős része saját sérülékenységazonosítási rendszert használ, de ezekhez hozzárendel CVE- vagy gyártói azonosítót is.

Komolyabb feladatot jelent viszont az érintett erőforrások azonosítása, amelyre egyrészt nincs széles körben egyértelműen elfogadott megoldás, másrészt sok szervezet jelenleg még nem alkalmazza egyik szabványos megoldást sem (CPE-, SWID-címkék). Pedig csak a szöveges formátumnál pontosabb erőforrás-azonosítás biztosíthatja a sérülékenységekre vonatkozó információk hatékony szelektív továbbítását, vagy továbbítás utáni szűrését azon – például egy kiberbiztonsági eseménykezelő központ szolgáltatásait igénybe vevő támogatott – szervezeteknek, amelyek rendelkeznek ezen erőforrásokkal. Hasonlóképpen komolyabb feladatot jelent a konfigurációs beállítások szabványos azonosítása, amely alapját képezi a konfigurációs beállítások ellenőrzésének, a hatóságimegfelelőség-vizsgálatoknak.

A *választott információcsere-megoldás alkalmazásának szintaktikai feltétele* az adott megoldás alapját képező formátum (XML, JSON, CSV stb.) kezeléséhez szükséges, vagy felhasználható szoftverösszetevők, -eszközök, -alkalmazások rendelkezésre állása, beszerezhetősége. A választást befolyásolhatja az is, hogy ezek ingyenesen vagy térítés ellenében férhetők hozzá.

Az egyes megoldások alkalmazásához szükség van az adott formátumot előállító, és feldolgozó alkalmazásösszetevőkre. A széles körben alkalmazott formátumok esetében számos további támogató eszköz is rendelkezésre állhat, amelyek hatékonyan segíthetik

a kiberbiztonsági szereplők tevékenységét a köztük megosztott információk (dokumentumok, jelentések, üzenetek stb.) megjelenítésével, szerkesztésével, formai ellenőrzésével stb.

Egyes megoldások esetében rendelkezésre állhatnak a támogató eszközöknél bővebb szolgáltatásokat nyújtó komplex rendszerek, alkalmazások (esetleg más megoldásokat is integrálni képes keretrendszerek), amelyek az információcsere mellett biztosítják a kiberbiztonsági szereplők között megosztott információk bevitelét, szerkesztését, tárolását, visszakeresését, más alkalmazások általi elérhetőségét. Ezek azonban túlnyomórészt piaci termékek.

Az információcsere-megoldások alkalmazásához szükséges szintaktikai szintű feladatok alapvetően az informatikai rendszerek közötti információcserét biztosító rendszerek, alkalmazások, összetevők beszerzéséhez vagy kifejlesztéséhez, illetve az alkalmazott információcsere-megoldásokban bekövetkező változásokhoz igazodó továbbfejlesztéséhez kapcsolódnak, amelyek az érintett kiberbiztonsági szereplő alkalmazói állományát nem érintik (számukra láthatatlanok). Ezentúl – amennyiben ilyenek felhasználásra kerülnek – szükség lehet még az alkalmazott megoldáshoz kapcsolódó támogató eszközök alkalmazására történő felkészítésre.

Összegzés

Ahogy a bevezetőben is megállapítottuk, a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatások napjaink alapvető, egyre növekvő jelentőségű feltételét képezik, így hasonló jelentőségű feladat a kibertér biztonságának fenntartása is. A *kiberbiztonság megteremtése és fenntartása* számos szereplő, kiberbiztonsági feladatokat megvalósító szervezet szoros együttműködését igényli, amely nem lehetséges eredményes és hatékony információcsere nélkül. A kiberbiztonsági szervezetek közötti információcsere ma még jelentős mértékben hagyományos módon, vagy strukturálatlan adatok elektronikus úton történő cseréjével történik, de nem kerülhető el az információcsere informatikai rendszerek közötti, félig strukturált és strukturált adatok formájában történő megvalósítása.

A kiberbiztonsági szervezeteket – mint a gyakorlatban szinte minden együttműködési kör szereplőit – kisebb-nagyobb mértékben rendeltetésbeli, eljárási, értelmezési *különbözőségek,* a kezelt információk körében, tartalmában, és formájában fennálló *eltérések,* illetve az alkalmazott rendszerek, eszközök különbözőségei jellemzik. Ez a heterogenitás, amelynek megszüntetése a legtöbb esetben nem lehetséges, vagy nem célszerű, teszi szükségessé valamilyen *interoperabilitási megoldás* alkalmazását, amely általában egy egyeztetett közvetítő reprezentáció, amelynek együttműködési körön belüli szabványosítása biztosítja az információcsere-igényeket kielégítő információáramlást. Ez a megoldás

szabadságot biztosít az együttműködő felek számára az információcserében érintett információk belső reprezentációjának – saját érdekeiknek megfelelő – meghatározására, módosítására, vagy megtartására. Ezzel együtt azonban az együttműködő felekre hárítja a belső reprezentáció és a közvetítő reprezentáció közötti jelentésmegőrző átalakítás feladatát.

Az interoperábilis információcsere-megoldások lényegében a *közvetítő reprezentációra,* vagy annak egyes összetevőire *vonatkozó specifikációk, szabványok,* amelyek egységesítik a megosztott információk jelentését (szemantikai szint), és az információcsere során használt formátumot (szintaktikai szint). Az előzőek közé az elemi információk lehetséges értékeit rögzítő ellenőrzött szótárak, a fogalmakat hierarchikus osztályokba soroló taxonómiák, valamint a fogalomrendszerek formális specifikációi, az ontológiák, az utóbbiak közé az üzenetformátum és adatelemformátum-specifikációk sorolhatók.

A *sérülékenységek kezelése* a kiberbiztonság egyik alapvető feladata, amely magában foglalja a sérülékenységek feltárását, elemzését, értékelését, korlátozását, vagy megszüntetését. Ennek érdekében a kiberbiztonsági szervezetek a sérülékenységek azonosítására, leírására; értékelésére; az érintett informatikai összetevőkre; a konfigurációs beállításokra; valamint sérülékenységi vizsgálatokra vonatkozó információkat osztanak meg, illetve cserélnek egymással.

A sérülékenység kezeléshez kapcsolódóan napjainkra – elsősorban az Egyesült Államok kiberbiztonsági rendszerében – számos interoperábilis információcsere-megoldást dolgoztak ki, és szabványosításra, amelyek közé napjainkban elsősorban a következők tartoznak:

- sérülékenységek azonosítása (CVE);
- sérülékenységek osztályozása, értékelése (CWE, CVSS, CWSS, CVRF);
- érintett erőforrások azonosítása (CPE, SWID, AID, ARF);
- konfigurációs beállítások azonosítása, ellenőrzése, értékelése (CCE, XCCDF, CCSS);
- sérülékenységek ellenőrzése (OVAL, OCIL, SCAP).

A rendelkezésre álló kiberbiztonsági információcsere-megoldások az egyes kiberbiztonsági szervezetek számára lehetőséget jelentenek egy már meglévő és kipróbált eszköz alkalmazására, vagy kényszert, amelyet egy már létező együttműködési körhöz való csatlakozás von maga után. *A létező megoldásoknak az egyes kiberbiztonsági szervezetek szempontjából vett szerepét, jelentőségét* nem elsősorban az aktuálisan alkalmazott – ma még jellemzően nem strukturált – információcsere jellege határozza meg, hanem hosszabb távon a szervezetek tevékenysége (milyen feladatokat látnak el, és ezek során milyen kiberbiztonsági információkat osztanak meg, cserélnek másokkal). Elkerülhetetlen az előretekintés, a felkészülés az informatikai rendszerek közötti automatizált, félig strukturált, vagy strukturált információcserére. Az ismertetett információcsere-megol-

dások elemzése azt mutatja, hogy mindegyikük olyan kiberbiztonsági információk megosztását, cseréjét támogatja, amelyek alapvető szerepet játszanak a kiberbiztonsági szervezetek tevékenységében, alapfeladataik ellátásában.

Egy *információcsere-megoldás alkalmazásának alapvető feltétele,* hogy a szervezetnek képesnek kell lennie saját információit az alkalmazott belső formátumról az adott megoldás szabványos közvetítő formájára alakítani, illetve erről a formáról a saját belső formátumára alakítani. Ennek vannak tartalmi (szemantikai) és formai (szintaktikai) összetevői. A szemantikai feltételek közé tartozik az információk fogalmi modelljének, ontológiájának összhangja; a megküldendő információk rendelkezésre állása; az alkalmazott azonosítórendszerek összhangja. A szintaktikai feltételek közé tartozik az adott megoldás alapját képező formátum kezeléséhez szükséges szoftverösszetevők rendelkezésre állása. Amennyiben ezek a feltételek nem teljesülnek, a kiberbiztonsági szervezet feladata ezek megteremtése. A szemantikai feltételek teljesítése alapvetően felhasználói szintű feladat, míg a szintaktikai feltételek teljesítése üzemeltetői, támogató feladat.

Összességében megállapítható, hogy a kiberbiztonsági szervezetek közötti együttműködés eredményességéhez és hatékonyságához elkerülhetetlen az informatikai rendszerek közötti automatizált, félig strukturált vagy strukturált információcsere feltételeinek biztosítása. Ehhez a sérülékenységkezelés területén alapvetően rendelkezésre állnak szabványos információcsere-megoldások, amelyek alkalmazására – bár jelenleg az információcserét a hagyományos, strukturálatlan megoldások jellemzik – a kiberbiztonsági szervezeteknek fel kell készülniük, az ehhez szükséges feladatokat el kell végezniük.

Felhasznált irodalom

[1] Munk S.: Kiberbiztonsági szervezetek rendeltetése, feladatai. *Hadmérnök,* 13. évf. 2. szám, 2018, 427–436.

[2] Munk S.: Kiberbiztonsági szervezetek közötti információcsere. *Hadmérnök,* 13. évf., 2018, megjelenés alatt.

[3] Munk S.: A kiberbiztonsági információcsere interoperabilitási kérdései. *Hadmérnök,* 13. évf., 2018, megjelenés alatt.

[4] Munk S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései.* MTA doktori értekezés, Magyar Tudományos Akadémia, Budapest, 2007.

[5] Munk S.: Szemantika az informatikában. *Hadmérnök,* 9. évf. 2. szám, 2014, 311–331.

[6] Foreman, P.: *Vulnerability Management.* CRC Press Taylor & Francis Group, Boca Raton – London – New York, 2010.

[7] *Vulnerability Handling. Handbook, Document for teachers.* European Union Agency for Network and Information Security, Heraklion, 2014. 09.

[8] *Standard and tools for exchange and processing of actionable information.* European Union Agency for Network and Information Security, Heraklion, 2014. 09.

[9] Steinberger, J. – Sperotto, A. – Golling, M. – Baier, H.: How to Exchange Security Events? Overview and Evaluation of Formats and Protocols. In: *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM).* Ottawa, 2015. 05. 11–15., 261–269.

[10] Mavroeidis, V. – Bromander, S.: Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In: *Proceedings of the European Intelligence and Security Informatics Conference,* Attica, Greece, 2017. 09. 11–13. 91–98.

[11] *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Rules. Version 1.1.* MITRE Corporation, 2016. 09.
[12] http://blog.osvdb.org (a letöltés ideje: 2018. 06. 07.)
[13] Householder, A. D. – Wassermann, G. – Manion, A. – King, C.: *The CERT® Guide to Coordinated Vulnerability Disclosure. Special Report.* Carnegie Mellon University, Software Engineering Institute, CERT Division, Pittsburgh, 2017. 08.
[14] *Common Weakness Enumeration. A Community-Developed Dictionary of Software Weakness Types. CWE Version 3.1.* MITRE Corporation, 2018. 03. 29.
[15] *OWASP Top 10 – 2017. The Ten Most Critical Web Application Security Risks.* The OWASP Foundation, 2017. 11.
[16] *Common Vulnerability Scoring System v3.0: Specification Document*. FIRST. Org Inc., 2017.
[17] https://cwe.mitre.org/cwss/cwss_v1.0.1.html (a letöltés ideje: 2018. 06. 07.)
[18] *ITU-T Recommendation X.1525, Series X: Data Networks, Open System Communications and Security. Cybersecurity information Exchange – Vulnerability/state exchange. Commons weakness scoring system.* International Telecommunication Union, 2015. 04.
[19] Schiffman, M.: *The Missing Manual: CVRF 1.1* – The Internet Consortium for Advancement of Security on the Internet, 2012. 04.
[20] *NIST Interagency Report 7695, Common Platform Enumeration: Naming Specification Version 2.3.* National Institute of Standards, Gaithersburg, 2011. 08.
[21] *ISO/IEC 19770-2:2015(E), Information Technology – Software asset management, Part 2: Software Identification Tag. Second Edition (2015-10-01). Corrected Version (2017. 02).* International Organization for Standardization-International Electrotechnical Commission, Genf, 2017. 02.
[22] *NIST Interagency Report 7693, Specification for Asset Identification 1.1*. National Institute of Standards, Gaithersburg, 2011. 06.
[23] *NIST Interagency Report 7694, Specification for Asset Reporting Format 1.1* – National Institute of Standards, Gaithersburg, 2011. 06.
[24] https://nvd.nist.gov/config/cce/index (a letöltés ideje: 2018. 06. 07.)
[25] *NIST Interagency Report 7275 Revision 4, Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2.* National Institute of Standards, Gaithersburg, 2012. 03.
[26] *NIST Interagency Report 7502, The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*. National Institute of Standards, Gaithersburg, 2010. 12.
[27] https://github.com/CISecurity/OVALRepo (a letöltés ideje: 2018. 06. 07.)
[28] *NIST Interagency Report 7692, Specification for the Open Checklist Interactive Language (OCIL) Version 2.0*. National Institute of Standards, Gaithersburg, 2011. 04.
[29] *NIST Special Publication 800-126 Revision 3, The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.3.* National Institute of Standards, Gaithersburg, 2018. 02.
[30] *Alerts, Warnings and Announcements. Best Practices Guide.* European Union Agency for Network and Information Security, Heraklion, 2013. 11.
[31] *ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends.* European Union Agency for Network and Information Security, Heraklion, 2018. 01.
[32] West-Brown, M. J. et. al.: *Handbook for Computer Security Response Teams (CSIRTs). 2nd Edition.* Carnegie Mellon University, Software Engineering Institute, Pittsburgh, 2003. 04.

Interoperable Information Exchange Solutions For Cybersecurity Organisations (Vulnerability Management)

Sándor Munk

Services of the cyberspace IT systems and networks are increasingly important conditions of the operation of the state organisation, the economic life, and the private life. Creating and maintaining cyberspace security is a key task that requires close cooperation between cybersecurity organisations. Precondition of this cooperation is interoperable information exchange. The purpose of this publication is to present the solutions supporting cybersecurity information exchange for vulnerability management, and to determine the related tasks of cybersecurity organisations.

Keywords: cybersecurity information exchange, interoperable information exchange, vulnerability management

Estók Sándor

Unfolding the Development of Modern-day Logistics Science

Interactive and Virtual Integration of Info-communicational Network System Logistics

A new era has begun in modern logistics, yet unknown even for those who apply it. This is the era of info-communicational and network centric system logistics. Smart info-communication develops at the speed of light and it requires the interdisciplinary design of scientifically organized logistic systems and the improvement of their quality. A new era is emerging and evolving in logistics: the future economy and society of knowledge-based, network centric, virtual, interactive and smart system logistics, constructed and working in the whole sector. A new era is also emerging in network economy; system logistics is being linked to the new science of networks. This cooperation can evolve into a partnership over the years to come.

Keywords: system logistics, interdisciplinarity, info-communication, new era, network economy

Dimension Change of Modern-day Logistic Science

Plenty of events and memories flash up when thinking of the modern-day development of logistic science. Looking back at the past century, it is hard to tell when modern logistics science emerged. We can state, supported by evidence, the prestigious event, from where we count the beginning of modern logistics. Another important criterion would be: who was the researcher whose activity determined the development of modern logistics?

M. E. Porter's vision and thinking in the '80s was a shock in America, economists were startled by the new possibilities. [1: 14] First he revealed the importance of the company and it's potential. He was capable of seeing new economic dimensions. His genius opened up new possibilities for companies, whose objectives were competition, strategic goals and profit. The managers and economic leaders of companies positioned themselves and their companies. They came up with a new mission where strategy and competition were parts of corporate objectives. Thus the science of management evolved with a global vision shaping the economy. This new and global vision was accepted worldwide. M. E. Porter built his concept on corporate strategy, which was recognized as a new

trend worldwide. However, it generated many debates in America, where his innovative concept was not recognized.

M. E. Porter was the economist who unfolded the development of modern logistics science.

- He defined competition strategy and formulated the motive power of competition in the industry,
- he set up the concept, construction and steps of competition,
- he gave new directions to economic thinking,
- he defined strategy, which companies accepted as a basic means,
- he created new quality and vision through his value chain,
- he introduced the value system into the flow process of products,
- he interpreted the creation of added value through value references,
- he organized the information and relations in the value chain,
- he linked strategy development to economic principles,
- he made strategy a corporate practice,
- he made the science of management a more disciplined science,
- he brought about a change of vision in the supply chain – cost reduction, optimization, later formation of management.

The Role and Influence of Hungarian Logistics Researchers on Emerging Logistic Science

The last two decades of the 20th century had a great impact on logistics in Hungary as well, and brought new challenges to the representatives of the emerging modern logistic science. In the '80–'90s two main economist researchers founded logistics in Hungary, namely Dr. Knoll Imre and Dr. Chikán Attila. They did constructive and operative logistic research independently of each other. Knoll Imre was actively involved in Hungarian and European logistics and was a founding member of the European Logistics Association (ELA 1984). This same year, he became the founding President of the Hungarian Logistics Association. Right after the registration of the Association he launched a comprehensive project in Hungarian economic sectors.

In 1992 he founded the first Hungarian Logistics Department at the University of Gödöllő.

He published his first work on logistics in 1999 – *Logistics in the 21st Century,* in which he sketches a vision of logistics.

"According to the classical philosophy of logistics, – in Knoll's words – *it is a vision and resulting activity, which synthetizes through a global scientific approach the correlating systems of supply and service processes."* [2: 9]

The logistic way of thinking starts from a philosophy of a multiple approach and reaches the new definition of 21st century logistics, which he puts in the following way:

"Logistics is the science of being able to handle globally and integrally the correlating economic and social processes. Its objective is to produce the maximal results possible on the economic and social level, constantly relying on the impact assessments of the micro and macro environment." [2: 14]

He recognized future power in applied logistics and assumed its development would be dynamic. Based on his researches, he emphasizes the principle of continuity.

He discusses both in theory and practice the examination of the value chain, the supply chain and value-adding processes. He examined the treatment of social problems in production and services, through an interdisciplinary approach and multiple impact assessments.

He examines logistics, marketing and computer science together with a common thinking and application. He considers their cooperation primordial in the supply chain, since they can only validate an interdisciplinary impact together, and this cooperation should be applied widely. The basis of logistic contribution is the operable supply chain. These are the basic principles of the forward-looking *Knoll-logistics.*

Knoll Imre was an iconic figure of logistics science, a committed engineer, who achieved a lot; economist and doctor of the Academy, he passed away in September 2016.

During the last two decades of the 20th century, the transformation of the value chain of industrial sectors was already taking place. The basics of the value chain by M. E. Porter were known already. Chikán Attila analyzed the procedures of value-adding procedures [3: 1–17] and carried out a detailed exploration of their correlations. His results led to the discovery of a new quality. First the value-adding procedures, then the corporate value chain and the supply chain.

His works primarily touched activities within the company. Creating added value focused on satisfying consumers' needs through primary activity within the company, bearing in mind the profit set as a goal in corporate strategy.

Added value as a success factor also appears on the corporate side [4] and it qualifies the work performed, without ignoring the satisfaction of human needs. Chikán Attila revealed the triple content of added value creation, the process system of production, the two-way information flow in the processes and value flow.

Cost effectiveness (what can be produced with little input) is crucial in value creating processes, as well as *efficiency* (how the company is performing). Core competences of the company are extremely important – this shows whether the company has the necessary conditions to produce added value. Based on the above criteria the efficiency of the business activity can be outlined.

The research of Chikán deals with every detail in corporate environment. Priorities are production, services and logistics. This gives new directions in the future, of which

the keystone, the value chain and the supply chain is the company. His book on *Corporate Economics* [5] deals with corporate processes, publishing new results and definitions. It sketches a complex context of social and economic factors affecting company operations, such as CSR, globalization or the increased role of knowledge. He is recognized on both national and international level in the economic and logistic field, whether in theoretical or practical environment, having carried out studies for several decades on the logistic value chain, the supply chain and value creation. Thus he is the only living *icon* in Hungary to represent *Chikán's logistic trend (school)* and to have contributed and still contributing to Hungarian and international logistics science.

The end of the 20th century dazzled scientists at that time with new possibilities and challenges, while they were looking for solutions to the events on the economic front. They were willing to give answers to the then unknown processes. Scientists and researchers limited the challenges of the end of the century and addressed the theoretical and practical issues in a very moderate way, based on economic science. At the end of the '90s, the above led to the creation of a new science: *the science of logistics.*

The 21st Century Giving New Impetuous to Applied Logistics

At the end of the past century, intense and well-organized networks and supply chain systems emerged. Their goal was to increase competitive advantage and profit, and also to keep their results and positions at a stable condition. To achieve this, the re-organization of companies had become more and more important in the hope of becoming professionally significant top companies. This is how logistic supply chains developed into global networks in the first decade of the third millennium. At the same time, the competitive supply chain – as an individual dynamic force – created innovative info-communicational capabilities and interdisciplinary relations on the world market. It was capable of transforming itself into a new organization, creating a new strategy and entering the market with new products and vision. At the same time, it was linked to other networks and thanks to *networking* entered in a stable position *in a new organization.*

Horizontally Organized Network Logistics

Several different logistic supply chains and networks were linked to each other. The elements of a gigantic system established economic relations – they set up a strategic relationship of individual legal entities cooperating with close settlements. However, the market remained at the center. The connection between them was *communication, coor-*

dination and cooperation. All this, based on the standards of the last century, proved to be too slow in the 21st century; there were quality defects in the operation of logistical capacities.

The horizontal logistic industry was created in global economy. This might have sounded positive first for the operators but altogether it had slowed down development by creating an effect similar to an impending war. It had frozen the dynamically operating supply chains and networks.

The international market made it possible to expand abroad, to re-organize the supply chain, to strengthen positions and to build up a new strategy. Circumstances show that services have become more important, both internationally and nationally. The quality of services should approach consumer needs. The balance of value, price and needs of logistic services can be validated on the services market. If we compare the values of global and local environment, it is clear that the most favorable method is to approach service providing to demands within a circle of a radius of 20–30 km.

The first decade has given new impetuous to logistics and the supply chain, but fundamentally the scientific trends of the past century appeared in the logistic vision and thinking. Innovation and R&D also carried the traces of past dimensions. As a result, global and business logistics have become a congestion of the world. [6] This can be recognized in *environmental protection and truck traffic.* Computer science was a great support for logistics, which had helped its development throughout the last decades.

Commerce was accelerated, which resulted in the qualitative and quantitative development of the global market – which served as a basis for recovery. This was the *silent revolution of local and global distribution systems,* [6] depositary of logistic development. Today's logistics can give new answers to numerous challenges, and restore trust in relationships, in supplying – manufacturing – distribution systems, in micro and macro economy, in everyday relations of social actors, in the realization of their needs and interests.

The *spirit of the revolution of stealthy logistics* passes by silently step by step; we should "*watch out, so that it won't pass by us.*" [6: 223]

Info-communicational Network Centric System Logistics

The operation of the system treated above had become an obstacle to the development of logistics. There were two possible solutions to this situation. One of them was to make use of the possibilities of the info-communication system. It became necessary to transform horizontal logistics with the close cooperation of logistics and info-communication systems. Horizontal system logistics should be converted into vertical logistics. Today the info-communicational knowledge, technology and technological developments add up to a system of info-communication. Information moves in virtual and physical space

as needed. A *Just in Time* is emerging in info-communication, *which lets information and info-communication* flow according to user requirements. This is a dynamic element and driving force of system logistics:

- Information is individual and organized – every authorized strategic partner organizes, transforms, uses it on demand, 0/24;
- the virtual interactive space is already operational, as well as Information JIT, without which the functioning of network centric system logistics is impossible;
- the transfer of image, sound, data and digital signals – is a reality in Cyber, Virtual and Cosmic space, as well as the three dimension of the Earth.

The other solution: the transformation of horizontal logistics into vertical. In this procedure several factors lead to the desired result.

- Integrated logistics should be transformed into interactive logistics;
- a vertical *network centric logistic system* should be created from the logistic network;
- a virtually organized info-communication system should be formed from the information system;
- information and info-communication systems must be placed into virtual space;
- information should proceed in every system in an organized way, from the starting point to the endpoint;
- there is an organized flow of material, information and synergy in the systems;
- in the info-communication network the strategic and info-communicational flow of system logistics gets to every partner;
- all information and communication moves through and is archived by information centers (2 of them); there are managements in the strategic center, and logistic executives, flow systems, supply chains, value creating processes and networks of sensors in the other center.

The New Science of Networks Focuses on Network Economy and the Virtual Integration of System Logistics Relations [7: 216–236]

The modern-day concept of network economy has been redefined. According to this a complicated network is determined by the complexity of corporate relations. We are witnessing a new scientific revolution, the new science of networks, present and future. It is possible that we cannot even fully understand the content of these new phenomena. We can define network economy and system logistics as a complex network, where systems, partners, companies are endpoints. Links between them are business, economic and

financial relations. However, there are also fusions, reorganizations, cessations – when certain endpoints disappear – this is unique and normal in network economy. [7]

Links and relations are becoming more and more important and it is crucial for mere survival in modern economy to understand network phenomena.

Economy in the past century was based on a network, which resembled a tree upside down and solutions did not require new knowledge, rather unskilled work to manufacture mass products.

In today's globalized world information and new ideas mean value. It is quite possible that there is no obstacle before them, when production facilities are the issue. A 3D scanner is already in use, although it can still be improved.

The whole structure of production has changed; [7] it has become a horizontal network, with interrelations where virtual integration of the hubs became increasingly important. The new cooperation requires a new construction and new structure. Tasks are carried out in groups, inside and outside the company. The dynamic network organization can be easily configured and its operation is more flexible. Global economy has forced a change in the inner structure of companies. One of the keystones of *networking* is cooperation, which also contributes to adapting successful methods. Another key factor is the relationship of managers with other companies. Their participation in boards of directors becomes useful, and networks become crucial in relationships. Linking experiences in the board to spread habits within the company increases economic influence. Directors, thanks to acquaintance, can vouch for their colleagues – this "companionship" has enormous economic influence. [7: 223]

Market has been revaluated, *"(...) market is nothing else but a controlled network, where companies, concerns, financial institutions, governments and all other possible actors are an endpoint each (...)"* [8: 226] The financial market is also quite far from the economic value interpretation.

We are witnessing a new network economy, where strategic relationships and alliances are keystones of survival. *"It is a lot more beneficial to networks, if they cooperate and trust each other in the long run."* [8: 226]

Network economy will accompany both macro and micro economy for a long time. Outsourcing is very popular in this process system. Globalization spans over all national and geographic boundaries. To work things out, a new vision and approach of network economy and an understanding of interconnectedness will be necessary. The way of thinking always reflects the given civilization and the given continent. The principle of operation of this new network economy remains unchanged – links, endpoints, relations widen, strengthen and are being reorganized along new ideas, interests and trends. Based on scientific discoveries, the intelligent application of modern logistics opens up new horizons where, concerning development, the sky is the limit.

Available capacities show that system logistics is organized around two info-communicational centers – along with a multitude of network centric relationships. It can function in an interdisciplinary relationship with strategic partners who have the capacity to contact logistics in order to achieve their goals. It is possible to organize and to create a complex operation of system logistics, together with the related interdisciplinary partners. The relationship is only authorized after the management approved and controlled the capabilities.

Future Value of our Century: Network Economy, [7: 216–235] System Logistics, Info-communication and Interactive Virtual Reality

The cooperation of system logistics and info-communication is the highest level of strategic connection in the light of the past decades. The common value creating activity of these two areas is very powerful. They are the future values of our century and they have a key role as far as the results of the decades to come are concerned. A new era has begun, where logistic organizations, corporations, supply chains, networks, companies make up a network-centric system.

Future values give rise to development:

- Logistic systems and infrastructures based on logistic science function in a reliable manner and their development is dynamic and promising,
- logistic and info-communicational systems and their sub-systems function on knowledge base,
- interdisciplinary, interactive supply chains, networks, production, supply, distribution and service systems are all linked, optimized and organized,
- logistic technological processes and flows are organized and controlled according to modern standards and they have the ability to develop,
- information in logistic systems is well-organized and individual; it passes through the whole system, from the first member of the system to the last partner; new information is distributed to strategic partners and the passing through of every new information brings renewed information to the system; to achieve this, participating partners can add new information about themselves, their products, their business, which they can upload to the information network ever in movement, which contributes to the value creating work of the partners by new knowledge, solutions, data and information transfer,
- virtual logistics is becoming more and more effective and interactive; thus system logistics becomes a strong future value,

- a crucial element concerning future values is the high performance intelligent computer network, which links people and technical devices in order to find the best possible solutions; smart technologies assist the capacity to solve tasks,
- qualified, professional, well-prepared, selected IT and logistic personnel and groups can also be regarded as future values,
- the future value of strategy and its significance in the productive as well as in the services sector lies in human relations in business, where the partners are skilled, they monitor consumer needs and their satisfaction is a priority,
- the cooperation of system logistics and info-communication places partnerships into a new dimension among those who take part in it by authorization; this relationship is crucial as far as operation is concerned; this is enhanced by information, *information just in time* and information flow; the information center provides every information according to the partners' needs, through a system of relations and principles of business, cooperation and competition,
- in this whole value-creating system, maintaining the diversity of the flow of physical procedures (matter, synergy, semi-finished and finished products, human resources, services) perpetuates the *superposition of network centric logistics.*

Vision for the Near and Further Decades

The future will be encountered by the multitude of very complicated and accelerated set of events, which is almost impossible to predict. Because of the sharp changes in economic flows, horizontal and virtual network centric systems build up with countless connections. Information receives a key role in logistic systems. The system can develop dynamically under the influence of multiple information flow. This is the direction of the future, which will dominate in network economy and network centric system logistics.

In the future, network systems will cover all of the operations and areas of companies. The functioning of integrated, virtual, interactive systems is aided by smart devices and technologies in an organized and systematic way.

Info-communication systems will be able to transfer information to the members of the network according to their demands, when they need it at any time of the day. The system of this information flow is *Information Just in Time;* this transmits all information to those who require it in the strategic network.

Nuclear fusion, mimicking solar energy production is very promising. The experimentation and building of a thermonuclear fusion reactor is the great energy promise of the future. [9] Today, there is a big challenge and competition: who will be the fastest to come up with mobilized version of the fusion reactor on the market. NASA, together with the Departments of Energy and Defense, is preparing a small modular reactor, in

which fusion energy is directly converted into electricity, without side effects. For the nuclear fusion they plan to use Helium-3. The prototype is a 50 megawatt unit, which is supposed to be ready in 2019. Several experiments are going on worldwide and the first one may be made commercially available in 2020. A great challenge related to this is the exploitation of the Moon: the mining of Helium-3 on the Moon, its transport to Earth and its processing are at stake. Several countries compete and the first one to do so will dominate the energy market. The building of mobile version of the thermonuclear fusion reactor is decisive but it is equally important who will make it commercially available first. The first thermonuclear fusion reactor is being constructed in France. The gigantic international experiment is expected to be ready around 2030.

A new 5th generation mobile internet is at the center of interest, whether business or general. The researchers of Telenor achieved a bit rate of 1,215 Gbps. Besides speed and capacity, the equally important short response time is 10 milliseconds (ms). As far as the mobile internet network is concerned, short response time is important, so that communication can be smooth between two systems. This can be used in network business, online connections, telemedicine and car racing. 5G is of strategic importance, it will have an important effect on the economy and society in the years to come.

The "Internet of Things" (IoT) – the future of anthropocentric technologies is the technology for people, which shapes human life every day, helps our work, our way of life. Learning technologies are highlighted – *"think for people".*

"Technology for people" – its significance is to expand and boost human capabilities, so this way of thinking may cause the most progress. Technology is shaping our everyday life and work. It raises important social issues and creates new possibilities, while changes are really controlled by people.

IoT-Strategy Director – almost every company needs a digital director. There is a new stage of innovation in the world, where multifunctional directors are needed. Soon a multitude of *IoT-Strategy Directors will emerge in the management system of companies.* They will be capable of bridging the gap between operation, network economy, system logistics and IT solutions, thus to solve a set of tough issues pressing on companies. They work together with everyone, from plant managers to chief information officers and CEOs. The key is that they are *responsible for implementing the changes.* It is only then, that their company is certified to comply with the *requirements of the fourth industrial revolution.*

Summary

When studying the evolution of modern logistics science, I had the thought right from the beginning: how it was possible that an economist established *logistics from econo-*

my? The *value chain* was the first known formula of M. E. Porter to bring the attention of all the world. In a few years, *management science* appeared in Porter's thoughts and writings. By the last decade of the 20th century, we speak of *logistics, value chain and supply chain.* A few years before the turn of the 3rd millennium we witnessed the appearance of *Logistics science.* The above listed scientific events happened during 15–20 years. As years have passed, logistics organized itself in theory as well as in practice. An impressive development has begun in logistics, in the largest companies as well as the smallest enterprises. Logistics appears as a *phenomenon* traversing regions, boundaries, civilizations, continents including economy and society. I witnessed this process myself, but back then, I had a different idea about it than today. I know that every science has to work out its own language, only then can it develop and withstand the test of time in the great melting pot of history.

The almost two decades that have passed in the 20th century have given sufficient impetuous to logistics science, supply chain, networks, network centric logistics, system logistics and along with them to several sciences that are in an interdisciplinary partnership with them, like info-communication, with which the strategic partnership dates back a quarter of a century. I think it is quite possible that the two fields will merge in some areas. They developed considerably together, since they mutually assisted interactive cooperation and the humanization of virtual reality.

Meanwhile, in the United States Barabási Albert László laid down the foundation of a new science, which he called the *New Science of Networks.* In this discipline economy is regarded as a complex network, including new quality changes of the development of modern logistics, together with different sub-systems and other elements. System logistics is a part of this, since I defined it in the beginning of my research (2007) as *network centric logistics.* This is a milestone, a new result that inspires me in my field of research to be even more effective. I think my postgraduate students will also find this interesting and this will have an impact on elaborating on their field of research.

After the development of the past decades, modern logistics science has been unfolded even more, since the development ahead of us is accelerating more and more in the near and further future. New horizons open up, system logistics will soon expand to the Moon, mainly to areas that can be mined, but I could also list several other logistic fields. The most important is the transportation of Helium-3 to Earth, by rocket transport logistic means, thus a hybrid system of logistics will be formed – of practical, mining and transport operations. There is a crucial phase in the supply chain between the Earth and the Moon: the operational logistic support of the nuclear fusion reactor.

In the decades later on, the focus will be on Mars, where the main task will be to create viable conditions in a harsh environment. Logistic operations will be adapted by system logistics according to the possibilities offered by Mars, in order to sustain life in all circumstances, in a creative and value-creating economic environment. International

integration should be created for the project, and a program of implementation adapted to the operating capabilities. In order to achieve this, smart technologies and technical possibilities are used according to today's standards and capacities.

Bibliography

[1] Porter, M. E.: *Competitive Strategy.* 2006.

[2] Knoll I.: *Logisztika a 21. században. Profitnövekedés logisztikai eszközökkel.* [Logistics in the 21st Century. Increasing Profit by Logistic Means.] KIT Képzőművészeti Kiadó, Budapest, (3rd edition), 2001.

[3] Chikán A. – Demeter K.: Értékteremtő folyamatok menedzsmentje. [Management of Value Creating Processes.] 5th edition, Aula Kiadó, Budapest, 2006.

[4] Chikán A.: *Vállalatgazdaságtan.* [Corporate Economics.] KJK Aula Kiadó, Budapest, 1992.

[5] Chikán A.: *Vállalatgazdaságtan.* [Corporate Economics.] Aula Kiadó, Budapest, 2008.

[6] Chikán A.: Lopakodó forradalom. [Stealthy Revolution.] *Logisztikai Híradó,* [Logistic News] Vol. 26, No. 5. 2016.

[7] Barabási A. L.: *Behálózva.* [Linked.] Helikon Kiadó, Budapest, 2008.

[8] Powell, W. W.: Neither Market for Hierarchy: Network of Organization. *Research in Organizational Behavior,* Vol. 12, 1990, 295–336.

[9] Szentgyörgyi Zs.: *A jövő nagy energiaígérete.* [The Great Energy Promise of the Future.] 2015. 02. 04. www.metropol.hu

A modern logisztikatudomány fejlődésének kapuja kitárva. A hálózati infokommunikációs rendszerlogisztika interaktív, virtuális integrációja

Sándor Estók

Elkezdődött a modern logisztikai korszak, amely a logisztika alkalmazói számára még nem ismert. Ezt az időszakot az infokommunikációs- és hálózatközpontú rendszerlogisztika neve és képessége fémjelzi. A fénysebességgel haladó okos-infokommunikáció fejlődése megköveteli a tudományosan szervezett logisztikai rendszerek interdiszciplináris kialakítását, minőségének javítását. Új logisztikai korszak körvonala rajzolódik ki és alakulóban van a jövő gazdaságának és társadalmának tudásalapú, hálózatközpontú, virtuális, interaktív, okos-rendszerlogisztika felépítménye és működése teljes vertikumban. A korszakváltás lépteit hallani a hálózati gazdaságnak, a rendszerlogisztikának és kapcsolódása a hálózatok új tudományához. Az együttműködő kapcsolat az évek során partneri kapcsolattá fejlődhet.

Kulcsszavak: rendszerlogisztika, interdiszciplináris, infokommunikáció, korszakváltás, hálózati gazdaság

Réger Béla

A telefonra készített applikációk alkalmazási lehetőségei a multinacionális oktatási programokban a Logisztika 4.0 szellemében

A negyedik ipari forradalmat jelölő Ipar 4.0 koncepciója szerint a digitalizáció kulcsszerepet kap a gyártási folyamatainak irányításában. Ez a felismerés hívta életre az Logisztika 4.0-t, amely jövőbe mutató kutatási projektként azt vizsgálja, hogy a digitalizáció és az információs technológia miként állítható a logisztikai folyamatok tervezésének és irányításának szolgálatába.

Kulcsszavak: Logisztika 4.0, NATO hadműveleti felvonulás tervezése, okoseszközök a logisztikában, DIY-mobilapplikáció

Bevezetés

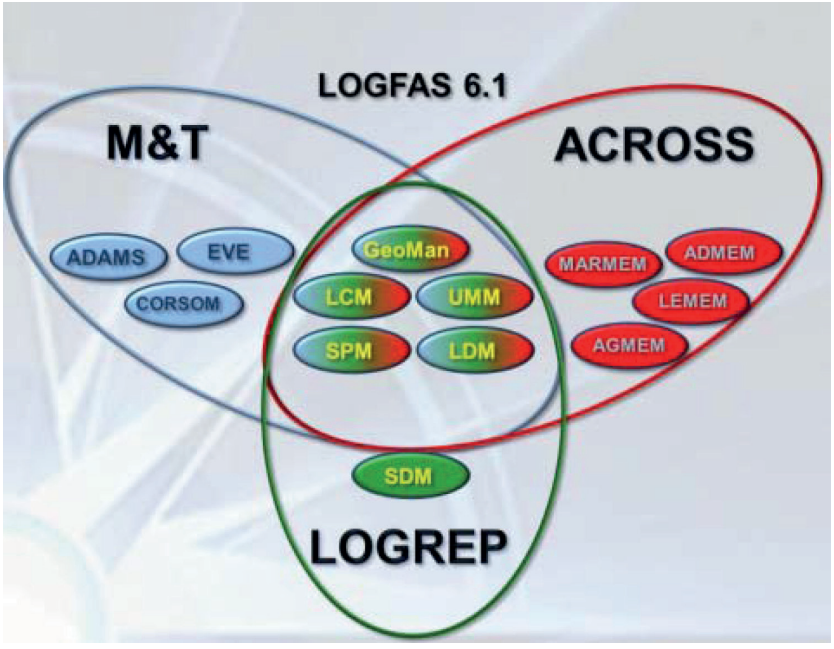
A digitalizáció folyamata kihat a katonai logisztikai felsőoktatásra is. Fő cél már napjainkban, hogy a tisztek, tisztjelöltek oktatásának ne a magolás és a felmondás legyen az alapja, hanem a 21. század kihívása, a mobil smart eszközök alkalmazása. Ez nem informatikai feladat, hanem alkalmazható a logisztika bármely területén is, különösebb programozási nyelv ismerete nélkül. Ebben a tanulmányban a MAGLITE oktatási programon végzett kísérleti projektről számolok be.

A nemzetközi gyakorlatok az oktatási folyamat nagyon fontos részei. A MAGLITE multinacionális oktatási programot több mint 15 évig vezettem a magyar részről, amelynek során a kidolgozói csoportokat és a hallgatók felkészítését végeztem. Másik részről a FOURLOG logisztikai képzési programba tervezőként-fejlesztőként a tervezés NATO-kompatibilis eszközeinek alkalmazását vezettem be. Az elmúlt években, mint már külsős szakértő, az MSc- és a BSc-hallgatók felkészítését segítem az újszerű módszerek alkalmazásával.

Jelenlegi tervezési rendszer

A NATO (Észak-Atlanti Szövetség) már korábban felismerte egy olyan tervezést segítő rendszernek az előnyeit, amely biztosítja az egységes keretek közötti munkát. Ennek a rendszernek a segítségével a nemzetek és a nemzetközi parancsnokságok képesek egymással üzeneteket váltani a logisztika és a mozgatással kapcsolatos adatok, tervek egységes formátumú felhasználásával.

Az NC3A (NATO konzultációs vezetési és irányítási hivatal) egy közös adatbázisú alapokon nyugvó, több programból álló rendszert fejlesztett ki, amely a logisztika valamennyi területét lefedi. Ez a LogFAS (Logistics Functional Area Services [1] – Logisztikai funkcionális terület információs szolgáltatási rendszere). [2] A LogFAS a NATO Stratégiai Parancsnokság Automatizált Információs Rendszerének része, és így szorosan együttműködik a többi, az Automatizált Vezetési és Információs rendszerhez kapcsolódó rendszerrel is. Képes érvényesíteni a NATO elveit, csökkenti a tervezés idejét, minden résztvevő számára biztosítja a tervezéshez szükséges logisztikai adatokat és egységes formátumban képes terveket továbbítani, elemzéseket végrehajtani. A LogFAS több alrendszerből áll, amelyek lefedik a logisztika funkcionális területeit.



1. ábra – A LogFAS funkcionális alrendszerei [3]

Az ábrából a megértés kedvéért a főelemeket emelem ki és fordítom magyar nyelvre.

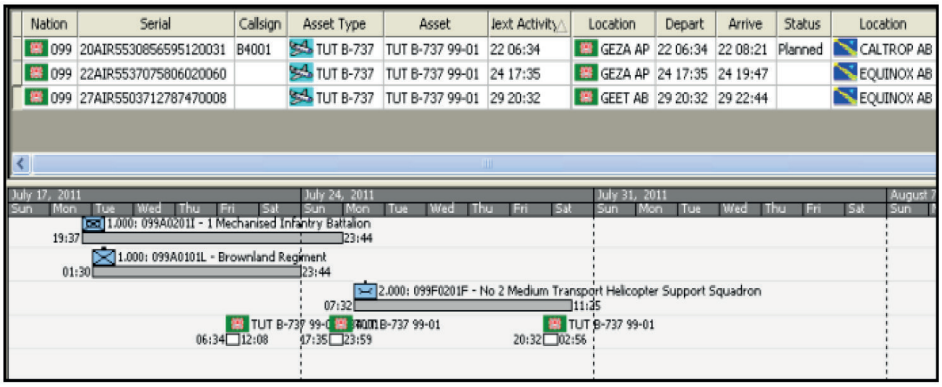
- M&T: a csapatmozgásokat és a szállítást tervező-koordináló rendszer. A tanulmány ezt elemzi, ezért csak ezt részletezem:
  - ADAMS: felvonulási tervezés, modellezés, elemzés.
  - EVE: szállítások vizuális nyomon követési rendszere.
  - CORSOM: koalíciós erők fogadása, állomásoztatása és továbbjuttatást tervező rendszer.
- LOGREP: Logisztikai jelentő és képességértékelő rendszer.
- ACROSS: Erőforrás Optimalizáló Rendszer (fenntartási és készletképzési tervezés, kezelés). Nem részletezem, mert a MAGLITE feladat szempontjából nem domináns.

A rendszer alapját a kialakított LogBASE logisztikai adatbázis képezi.

A tervezés szintjei alapján a tagállamok a NATO parancsnokságokkal koordinálják a felajánlott erőket, ez a *nemzeti szint. A stratégiai szinten* az ADAMS-rendszer alkalmazásával a műveleti alkalmazás tervezése és az EVE-rendszer alkalmazásával a műveleti területeken a vizuális nyomkövetés valósul meg. Az EVE képes a szállítási tervet akár vizuális modellezett térképen is megjeleníteni.

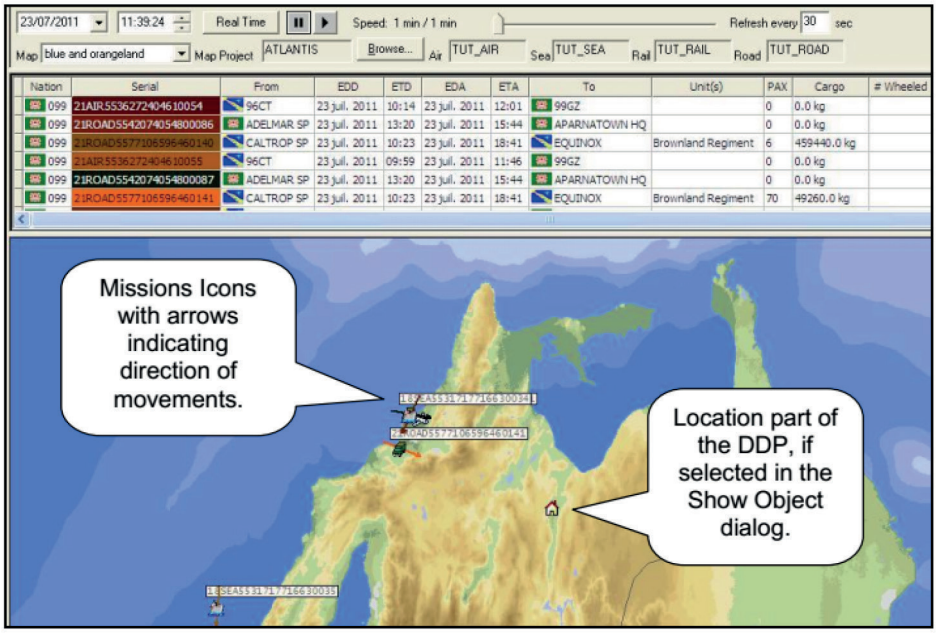
Le kell szögezni, hogy ez a megjelenítés *nem valóságos, hanem szimulált.* A menetrend terv szerinti állapotát mutatja, és nem a valósidejű helyzetet. A valós helyzet megjelenítéséhez a központba beérkezett híradórendszeri vagy informatikai rendszeri adatok alapján a szaktisztek frissítése szükséges. A programrendszer alapvetően lokális rendszerként működik, az adatok a másik tagállam rendszerével export-import kapcsolatokon keresztül jutnak el jellemzően.

Az átláthatóság és a nyomkövetés lehetőségeinél az EVE már Gantt-diagram alkalmazásával is képes bemutatni az időrendi helyzetet. Hiányossága, hogy nem derül ki a szállítmányok közötti kapcsolat és az a kritérium, hogy melyik szállítmánynak kell megelőznie vagy követnie a másikat, és hogy milyen kapcsolatban vannak. Például ha egy RORO-hajó (csapatszállító hajó) késik, hogyan és melyik szállítmányok időrendjét befolyásolja. Így sajnos nem látható a hálótervezés szabályai (CPM – kritikus út módszer) alapján, hogy melyik szállítmány pontatlansága esetén „borul" a hadműveleti terv, illetve melyik szállítmány mennyi tartalék idővel rendelkezik.



3. ábra – A csapatszállítmányok időbeni sorrendje [4]

A CPM-hálótervezés lehetőségeire és ennek részleteire nem térek ki, ezt a következő tanulmányban elemzem.



4. ábra – A szimulált csapatszállítmányok tervezett helyzete a terv alapján [4]

Ebben a részben bemutattam a jelenlegi tervezési módszert, most rátérek az újszerű tervezési módszer lehetőségeire, hogy a logisztikai törzsben hogyan lehet kiegészíteni ezt a rendszert egy korszerű mobiltelefonos applikációval.

A Logisztika 4.0 kihívásai és hatásai a logisztikai tervezésre

Az Ipar 4.0 egy frappáns megjegyzés szerint *„a gőzerővel digitalizálódó világunk”.* Ebben a szójátékban benne van egyrészt, hogy gyorsan fejlődik, másrészt arra utal, hogy az első ipari forradalom a gőzgépek alkalmazásával kezdődött, és a negyedik a digitalizált világ.

A Logisztika 4.0 az Ipar 4.0 terméke. Mint ismert, a logisztika nem csak anyagáramlással, hanem információáramlással is foglalkozik. Ezek elválaszthatatlanok, és most az információáramlás a digitalizálásával került előtérbe. Ennek a nagy adatfolyamnak a részét képezik a felhőalapú szolgáltatások is, amikben nem lokálisan helyi adathordozón tárolnak el szoftvereket és adatokat, hanem egy vagy több szolgáltató eszközein. Ez a technológia már ma is a hétköznapok részét képezi, például telefonos névjegyeinket vagy a teendőink listáját nem a telefonunkban tároljuk el, hanem egy más eszközről is hozzáférhető központi szerveren. Ezáltal adatainkat könnyen, több platformról is elérhetően, biztonságosan tudjuk tárolni. Az iparban ez olcsó és biztonságos adattárolást és hozzáférést biztosít, rugalmas infrastruktúra kialakítását teszi lehetővé.

Az AppSheet nevű program az Egyesült Államokban került napvilágra. Praveen Seshadri startup cégéről van szó, amely egy „önkiszolgáló” programot ad a felhasználóknak. Az AppSheet egy bárki által fejleszthető (pontosabban javaslattétel útján, amennyiben az ötlet jó, programozzák és belekerül a javaslat) programcsalád, amely rendkívül széles körű felhasználhatóságot tesz lehetővé. Úgy tudunk programot írni, hogy nincs szükségünk semmiféle programozási nyelv ismeretére. Mivel alapvetően táblázatára épül, a használata végtelenül egyszerű lehet, ha valaki ért valamilyen táblázatkezelő programhoz, például Google Sheet vagy Excel, és beszél annyira angolul, hogy szerkeszteni tudja a webes alkalmazás alatt futó felületet. A programrendszer különleges előnye, hogy úgynevezett platform-független, így az alkalmazás képes futni mind androidos, mind iOS-felületen, de akár Windows operációs rendszeren is. A program ingyenesen elérhető bárki számára, tehát igazán „emberbarát”. Az, hogy ennyire egyszerűen kezelhető programról van szó, nem véletlen, miután Praveen Seshadri professzor asszisztensként dolgozott a világ egyik legjobbnak tartott kutatóegyetemén, a New York-i Cornell Egyetemen. 1999-től 2011-ig a Microsoft alkalmazottja volt, így, azt hiszem, kézenfekvő, hogy egy olyan alapra épített, ami a világon szinte mindenhol ismert brand, és rengeteg ember által használt program. Az AppSheet egy olyan platform, amely lehetővé teszi a vállalkozások számára

a mobiltermelékenység-alkalmazások létrehozását percek alatt – kód, fejlesztők és költségek nélkül. [5]

Jellemzője a felhőalapú adatbázis alkalmazása például a Google Drive vagy a Dropbox. Így az alkalmazás felhasználói között közvetlen kapcsolatot teremt interneteléréssel.

A másik fő jellemzője a digitális okoseszközökön való működés. Így mindig kéznél van, „zsebünkben az eszünk".

A harmadik meghatározó pontja a felhasználó által készített azaz DIY (ejsd: dí áj váj) Do It Yourself – „Csináld magad"-tervezés.

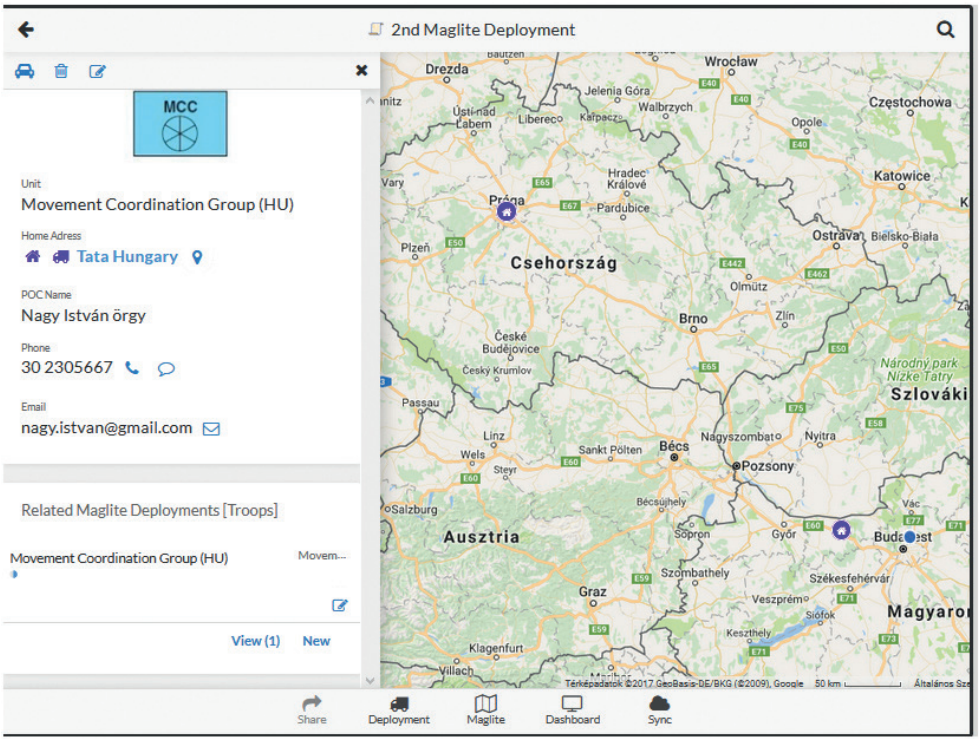
Az új rendszer alkalmazása a MAGLITE-gyakorlat felkészülésnél

A MAGLITE-gyakorlatra való felkészülés folyamatában az MSc osztály hallgatóival egy kísérleti projektet vezettem le. A lényege az volt, hogy a Logisztika 4.0 szellemében az okostelefonok, tabletek alkalmazásával hogyan lehetne a gyakorlat végrehajtás tervezését támogatni.

A nemzetközi oktatási program feladatleírásában szereplő részt vevő kontingensek közül alapvetően a magyar és cseh kontingens adataival dolgoztunk. A feladatban két lövészzászlóalj, egy szállítózászlóalj és egy mozgáskoordináló központ vett részt. A berakodási hely Tata vasútállomás, a kirakodási hely a tengeri szállításhoz Koper szlovéniai kikötő. A szállító zászlóalj előkészítő részlege közúton menetet hajt végre a kikötőbe a tengeri berakás előkészítése céljából.

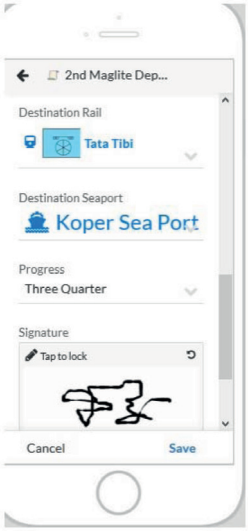
Első ütemben a feladatban szereplő szervezetek, a ki-, berakodó helyek adatait és a kapcsolattartó személyek elérhetőségét adtuk meg a táblázatban. Az applikációban már a beírt telefonszámok valós hívható elérhetőségek lettek, és az üzenet vagy az e-mail sem csak adat, hanem kiválasztás esetén működőképes elérhetőség. Interaktív térképen lett megjelenítve, ahol a szállítójárművel jelzett ikon kiválasztásával a hozzátartozó adatok is feltűntek, ahogy az 5. ábrán látható. A kontingens adatainál az egyezményes NATO-jeleket alkalmaztuk, így ez az együttműködésben minden tiszt számára érthető volt.

A mintapéldában bemutatom, hogy a megjelenítés hogyan látható tableten vagy okostelefonon. Mindkettő hordozható, így bármelyik alkalmazható a feladat során. A mai okoseszközöknek már alaptartozéka a GPS és a felhő-adatbázis elérhetősége az interneten keresztül.



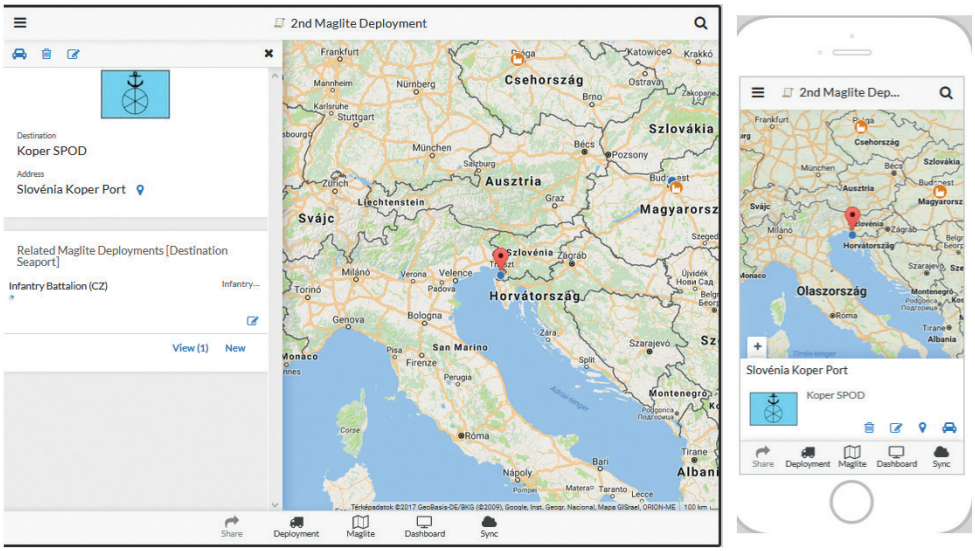
5. ábra – Az MCC (mozgás koordináló központ) elérhetősége az interaktív térképen tableten ábrázolva (a szerző saját szerkesztése)

A második ütemben a be- és kirakodó helyek adatait rögzítettük a táblázatban, ami az applikációban már a NATO-jelekkel és az elérhetőségekkel jelent meg. Például a helyzetjelentések bekérésekor a vasútállomáson lévő kontingens kijelölt tisztje az úgynevezett progress pontban a készenléti állapotról is tud jelentést adni, vagyis hogy negyedig, félig vagy háromnegyedig van-e már a feladat végrehajtva. Ez a vizuális menedzsment szabályai szerint a térképen már jellel jelenik meg, például ○ = nincs elkezdve és ● = befejezve, nem pedig szöveggel. A helyzetjelentést adó tiszt digitális aláírásával igazolja a jogosultságát. Ez az információ online a felhő-adatbázisba kerül, és a tervezőtörzsben is azonnal látható.



6. ábra – A rakodás állapotáról a helyzetjelentés leadása mobiltelefonon (a szerző saját szerkesztése)

Az interaktív térkép előnye, hogy a be- és kirakodási helyeknek SPOD (tengeri), RPOD (vasúti), APOD (légi) nemcsak a földrajzi adatai, hanem az objektumhoz csatolt kontingensek is megjeleníthetők. Így naprakészen látjuk a szállítási helyzetet az adott objektumoknál. Ez a 7. ábrán látható tableten való megjelenítéssel. A tabletnek még az az előnye, hogy a törzsben most már könnyen kapcsolódhat egy kivetítőhöz is, és így az információt a teljes tervező törzs és a döntést hozó parancsnok is láthatja.

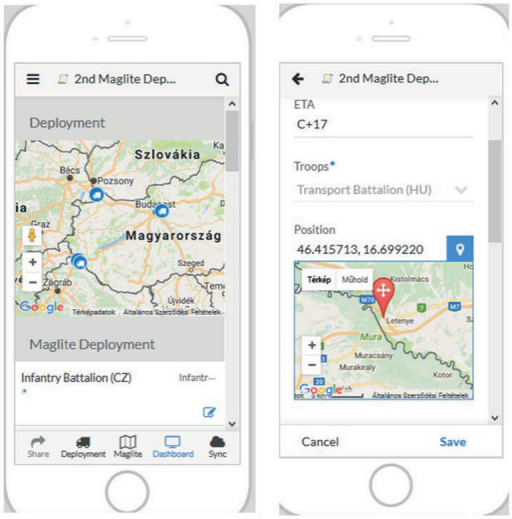


7. ábra – A SPOD Koper kikötőbe tervezett berakodás tableten, illetve mobiltelefonon (a szerző saját szerkesztése)

A *harmadik ütemben* az interaktív track-tracking, vagyis a nyomon követés helyzetét elemeztük a megadott C-naphoz (Cargo day) viszonyítva. Mint ismert, a NATO-műveleteknél a tervezéskor, ha még a pontos dátumot nem tudjuk, akkor kódolva nevezzük meg a napokat. Így D-nap a támadás napja, [2: 64] [6] a C-nap a szállítás kezdetének a napja a G-nap az adott térség területére település (deployment) stb. A csapatok mozgásakor az MCC, a mozgáskoordináló központ és a szállítmányban résztvevők is adhatnak adatokat a helyzetükre vonatkozóan. A „C" naphoz viszonyítva tervezzük az indulási időt, angol rövidítése az ETD és a tervezett érkezési időt, aminek az angol rövidítése az ETA.

A feladat végrehajtása során a szállítóoszlopban lévő kijelölt tiszt a nála lévő mobiltelefonon megnyomja a Position pontnál a térképjelet, és telefonja a beépített GPS-vevő alapján frissíti a helyzetét, amit a több száz vagy ezer kilométerre lévő tervező törzs az internetkapcsolatban lévő felhő-adatbázison keresztül egyből lát, és szükség esetén be is tud avatkozni. Tehát az ADAMS EVE rendszerével ellentétben ez nemcsak egy tervezett szimulált helyzet, hanem a „való világ".

Kitekintve a FOURLOG gyakorlatra, ezt a részt kiválóan lehetne használni Brno körletében az ellátó század telepítésénél. Itt interaktívan látható akár konténerre lebontva, hogy melyik alegységét, raktárat hova tervezzük telepíteni.



8. ábra – Interaktív track-tracking nyomkövetés lehetősége mobiltelefonon

A kísérleti projekt az MSc-s osztályban nagy népszerűségnek örvendett és a szaktisztek elkezdték a saját szakmai területükön is megvizsgálni az alkalmazás lehetőségét.

Összefoglalás

Megállapítható, hogy a Logisztika 4.0-nak nagy jövője és lehetőségei vannak a katonai műveletek alkalmazásában is. A meglévő NATO-rendszerek mellett a nemzeti kontingensek alkalmazásának tervezésekor nem szabad lemondanunk erről a lehetőségről. Az első kísérlet megvolt, ezen az úton célszerű továbbhaladni a jövő felsőoktatás digitalizált oktatás minőségi javítása érdekében.

Irodalomjegyzék

[1] www.isglimited.com/yahoo_site_admin/assets/docs/ISG_LOGFAS_Support_Services.21174635.pdf (a letöltés ideje: 2018. 07. 03.)

[2] NATO ADAMS-tanfolyam https://aktivity.unob.cz/logfas/SiteAssets/Stranky/Tutorial/ADAMS_61_1108.pdf (a letöltés ideje: 2018. 07. 03.)

[3] LogFast EVE Tutorial https://aktivity.unob.cz/logfas/SiteAssets/Stranky/Tutorial/EVE_61_1111_User.pdf (a letöltés ideje: 2017. 11. 26.)

[4] https://aktivity.unob.cz/logfas/SiteAssets/SitePages/Tutorial/EVE-61e.pdf (a letöltés ideje: 2018. 07. 03.)

[5] A LogSheet kialakulása. www.linkedin.com/in/praveenseshadri/ (a letöltés ideje: 2017. 11. 26.)

[6] www.stanag6001.com/aap_6_nato_glossary_of_terms_and_definitions/ (a letöltés ideje: 2018. 07. 03.)

The Potential of Smart Tool Applications in Multinational Education Programs

Béla Réger

According to the industry's fourth concept of Industrial Revolution, digitization plays a key role in controlling its production processes. This realization gave birth to Logistics 4.0, which examines future-oriented research project on how digitization and information technology can serve the planning and management of logistics processes.
Keywords: logistics, NATO LogFas system, smart system, smart mobile application

Lakatos Péter

A Közszolgálati Lenyomat Ludovika Kutatócsoport 2017-es tevékenysége és kutatási eredményei: a rendőrség 2016-os karbonlábnyoma és a reverz logisztika aspektusai

A fenntartható fejlődés napjaink tudományának komplex, multidiszciplináris kutatási területe. A Nemzeti Közszolgálati Egyetemen (NKE) komoly előzményei vannak a vízbiztonság, illetve a klímaváltozás kutatásának. Létrejött egy korábbi kutatóműhely, a Katonai Ökológiai lábnyom Kutató Központ (KÖKK), angol nevén Military Ecological Footprint Center (MEFC) bázisán a Közszolgálati Lenyomat Ludovika Kutatócsoport és ez által egy nemzetközi kutatási kapacitás, amely alapján az NKE a fenntartható fejlődés egyik elismert hazai felsőoktatási kutatóhelye lehet. A 2017. november 14-én megtartott képzés rámutatott a szén-dioxid-kibocsátás karbonlábnyom-mérésének fontosságára a közszolgálati hivatásrendek, így a rendőrség szintjén. Ez akár az NKE Jó Állam indikátorainak egyike lehet a jövőben. A cikk a *Közszolgálat és fenntarthatóság* c. könyv egyes fejezeteire épül, és ismerteti a legfrissebb kutatási eredményeket a rendőrségről.
A távlati tervek között szerepel egy kiválósági központ létrehozása és működtetése, amiben nemzetközi kutatóhálózat működik majd közre.

Kulcsszavak: fenntarthatóság, közszolgálat, rendőrség, karbonlábnyom, jó állam

Bevezetés

„Nekünk magunknak kell annak a változásnak lennünk, amit a világban látni akarunk."

Mahatma Gandhi

„Susan Murcott (Murcott, 1997) 57 eltérő fenntarthatóság definíciót gyűjtött össze 1979 és 1997 között készült publikációkból, és minden bizonnyal legalább még egyszer ennyi lenne összegyűjthető az azóta eltelt közel ugyanolyan hosszú időszakból is. E jelenség elsősorban arra hívja fel a figyelmet, hogy érdemes nagyon óvatosnak lenni bármiféle

definíció átvételekor, mert szinte minden szerző saját értelmezést fűz a fenntarthatóság jelenségéhez, és ezek között a megállapítások között nagyon sok a hiányos, egyoldalú, vagy éppen hibás, téves, torz, a fenntarthatóság lényegét éppen elfedni, elkenni próbáló meghatározás.

Érdemes ugyanakkor azt is világosan látni, hogy az egymásba ágyazott rendszerekre vonatkozó értelmezés miatt valóban többféle meghatározás is kialakítható a fenntarthatóságról. A szigorú, rendszerelvű és általánosítható kritériumok általában a külső rendszerrel, azaz az ökoszisztémával és a természeti erőforrásokkal való kapcsolatra fókuszálnak. Bármiféle emberi tevékenységre, folyamatra (legyen az például *energiatermelés*, vagy egy *település működése*, vagy éppen egy ország *közigazgatási rendszere*) egyformán igaz az, hogy csak akkor lehet fenntartható, ha tiszteletben tartja ezeket a külső feltételeket, vagyis az erőforrás-használata nem lépi túl ezen erőforrások újratermelődésének az ütemét, és kibocsátásai nem haladják meg a Föld hulladékfeldolgozó kapacitását." [1: 25] Az ilyen outputok vagy emissziók mérésére szolgálnak a különböző fenntarthatósági indikátorok.

Fenntarthatósági indikátorok [2]

„Magyarországon az Országgyűlés 18/2013. (III. 28.) OGY határozata rendelkezik a Nemzeti Fenntartható Fejlődés Keretstratégiáról. A Keretstratégia négy erőforrást különböztet meg: emberi, társadalmi, természeti és gazdasági erőforrásokat. A stratégia megvalósulását vizsgáló végleges indikátorrendszer kiválasztása és véglegesítése jelenleg is tart." „A fenntartható fejlődés mérését szolgáló indikátorok változásainak nyomon követése alkalmas módszer a folyamatok értékelésére (Valkó, 2015). A tendenciák ismerete teszi lehetővé a döntéshozók számára a stratégiai beavatkozásokat, és visszacsatolást jelent a már elvégzett feladatokról. A Központi Statisztikai Hivatal 2007 óta kétévente jelenteti meg a fenntartható fejlődés indikátorait. A 2015-ös kiadvány 100 jelzőszámot közöl, 33 a környezet, 44 a társadalom, 23 pedig a gazdaság állapotát mutatja be." [3]

A mintegy 100 indikátort egységes rendszerben mutatják be egy-egy oldalon; valamennyi esetében a hazai trendet ismertető ábrával és a hazai mutató nemzetközi összevetésben elfoglalt helyének érzékeltetésével.

Jó állam indikátorok

„A Jó Állam Jelentést az NKE államreform központja készíti partnerek bevonásával, de ez az egyetem egészének szellemi terméke." [2] A Jó Állam Jelentést minden alkalommal megtárgyalja az Államreform Bizottság is. A jelentés mára éretté vált, és egyre több szempontot vesz figyelembe a kormányzati teljesítmény értékelésekor.

Dr. Kaiser Tamás szerint: „A jelentéssel az a célunk, hogy egy tudományos hátterű munkát végezve egyfajta visszacsatolást adjunk a kormányzati képességekkel kapcsolatban." [2] Egyre nagyobb szerepet kapnak az olyan témák, mint az innováció és a versenyképesség, a digitalizáció vagy a fenntarthatóság. [2]

A nemzeti energiastratégia [4] 2030 értelmében „[a] jövő útja, hogy az energiahatékonysági intézkedések hatására csökkenő energiafogyasztást új, innovatív technológiák alkalmazásával biztosítsuk és célzott szemléletformálással karbon-tudatossá tegyük a társadalmi szereplőket".

A Nemzeti Fenntartható Fejlődési keretstratégia 2012–2024 [5] szerint „ki kell dolgozni a jelentős anyag- és energiaigénnyel, számottevő területhasználattal járó beruházások és fejlesztések esetében a legjobb (a társadalmi, környezeti, ökológiai externáliák figyelembe vételével számított) költség-haszon arányra tervezés módszerét. Emellett indokolt a projektszintű karbonlábnyom és a komplex éghajlat-változási kockázatelemzés módszereinek bevezetése is, tehát a Közszolgálati Lenyomat Ludovika Kutatócsoport e fenti célokhoz tud a maga eszközeivel, kutatási eredményeivel hozzájárulni.

Az ökológiai lábnyom fogalma és használata

Az ökológiai lábnyom azt méri, hogy az emberi igények kielégítése milyen mértékben veszi igénybe a Föld ökoszisztémáját. Ezt az igényszintet összeveti a Földön rendelkezésre álló, újraképződő bioprodukttummal, az ökológiai kapacitással.

A hektárban mért ökológiai lábnyom azt a biológiailag termékeny földterületet és vízfelületet jeleníti meg, amely ahhoz szükséges, hogy a népesség által elfogyasztott források regenerálódjanak, és az ehhez tartozó hulladékmennyiség elnyelődjön. Így megállapítható, hogy például 2013-ban az emberiség éves fogyasztásának egy év alatti újratermeléséhez 1,54 földgolyóra lenne szükség, azaz az emberiség már 54%-kal túllépi a fenntartható bolygóhasználat megengedhető mértékét. Az eljárás szemléletessége abban van, hogy a sokdimenziós emberi fogyasztás összetevőit (energia, nyersanyag, élelmiszer és biomassza, építőanyag, víz, hulladékemésztés, szén-dioxid-semlegesítés) egyetlen dimenzióra, a szükséges földterületre konvertálja, és így összehasonlíthatóvá teszi. Ugyanakkor a földfelszínről nagyon könnyen képesek vagyunk belátni, hogy véges készletről van szó, adott mennyiséggel gazdálkodhatunk.

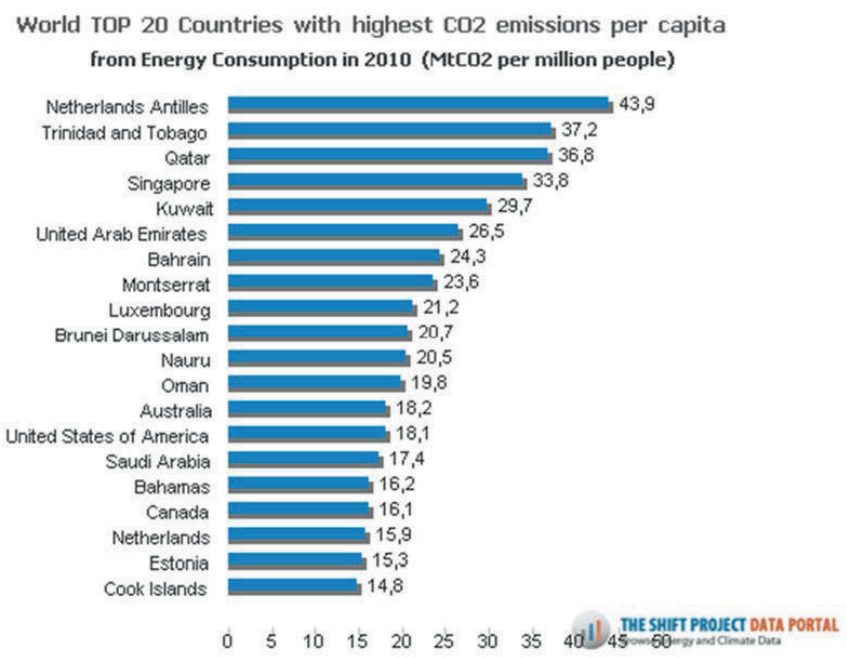
Az egy főre eső lábnyom alkalmas arra, hogy érzékeltesse a különböző emberek, csoportok vagy nemzetek életstílusát, fogyasztási mintáját; azt részben egymáshoz lehet hasonlítani, részben a Földön egy főre rendelkezésre álló átlagos területhez, de ugyanígy az adott országban rendelkezésre álló területhez is. [1: 86–87]

Szén- vagy karbonlábnyom és vízlábnyom

Az ökológiai lábnyom azt példázza, hogy meglévő statisztikai mérőszámok csoportosítása helyett lehet olyan új indikátort is alkotni, amelyik valamely újonnan felmerült tudományos jelenség – esetünkben a fenntarthatóság – sajátos logikájából indul ki, annak a sajátosságait tükrözi. Az ökológiai lábnyom mintájára más próbálkozások is indultak specifikus mérőszámok, indexek kialakítására.

Körülbelül 2005-től indult meg a szakirodalomban a *carbon-footprint*, vagyis a szénlábnyom emlegetése. Kialakítása azt a nyilvánvaló igényt tükrözi, hogy a klímaváltozás egyre jobban előtérbe kerülő kérdésköréhez kapcsolódva, ezen belül is az üvegházhatású gázok, illetve a szén-dioxid-kibocsátásának középpontba kerülésével párhuzamosan rendelkezésre álljon egy olyan indikátor, amelyik éppen ezt a jelenséget minősíti. A népszerű elnevezés tulajdonképpen gyorsabban elterjedt, mintsem annak a pontos jelentése rögzült volna, és sokan megalkották a maguk meghatározását. Geoffrey Hammond arra hívja fel a figyelmet, hogy az, amit karbonlábnyomként emlegetnek, az tulajdonképpen nem *lábnyom* abban a területhez kapcsolódó értelemben, ahogy az ökológiai lábnyom esetében szerepel, hanem inkább egy főre vagy egyes tevékenységekre vetített *karbonsúly* kilogrammban vagy tonnában.

A kérdéskört áttekintő tanulmányukban Wiedmann és Minx meghatározása szerint a szénlábnyom annak a teljes szén-dioxid-kibocsátásnak a mértéke, amit az egyes tevékenységek közvetve vagy közvetlenül okoznak, vagy ami felhalmozódik egy termék életciklusai során. [6] A meghatározás tovább pontosítható, és a szénlábnyom minden kibocsátott üvegházhatású gáz szén-dioxid-egyenértékre történő átszámított értékére vonatkoztatható, ahol az átszámítás alapja a létrehozott üvegházhatás mértéke. [1: 33–34]



1. ábra – Egymillió főre jutó CO_2-kibocsátás top 20-as halálozási lista 2010-ben [4]

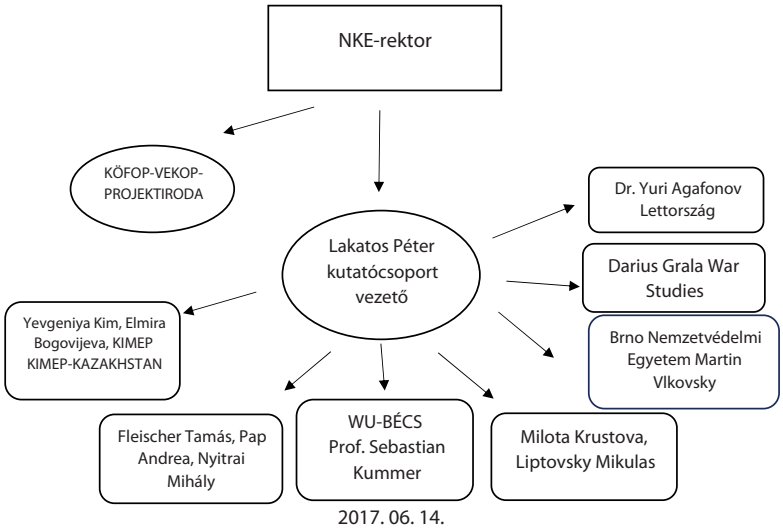
A Nemzeti Közszolgálati Egyetemen (NKE) komoly előzményei vannak a vízbiztonság, illetve a klímaváltozás kutatásának, az Intézmény Fejlesztési Terv (IFT) szerint ki kell fejleszteni azt a kutatási kapacitást és fel kell építeni azt a nemzetközi partnerséget, amely alapján az NKE a fenntartható fejlődés egyik elismert hazai felsőoktatási kutatóhelye lehet. [7]

Közszolgálati Lenyomat Kutatócsoport

A Közszolgálati Lenyomat Kutatócsoportot a Nemzeti Közszolgálati Egyetem Közszolgálat és Közigazgatásfejlesztési Operatív program keretében alapította meg rektori jóváhagyással. A kutatócsoport vezetője Lakatos Péter egyetemi docens. A kutatócsoport egyfajta jogutódja a korábbi rektori pályázat alapján létrehozott Katonai Ökológiai Lábnyom kutató Központnak, amelyet 2014-ben indított el ugyancsak Lakatos Péter, akkori alapító tagjai Szeker László, Pap Andrea és egy demonstrátor hallgató, Verbényi Dávid voltak.

A Közszolgálati Lenyomat Kutatócsoport már rendelkezik együttműködő partnerekkel, úgymint a Bécsi Gazdálkodási Egyetem – WU – Sebastian Kummer professzor vezette Logiszitkai és Közlekedési Intézete, vagy a szlovákiai Liptovsky Mikulasban el-

helyezkedő Milan Rastislav Katonai Akadémia menedzsment tanszéke, Milota Kustrova képviseletében. A pályázat keretében pedig Fleischer Tamás, a Világgazdasági Regionális Kutató Intézet kutatója a tagja és Nyitrai Mihály alezredes doktorandusz hallgató, valamint a korábban említett kutatócsoportból Pap Andrea alezredes asszony, tanszékvezető.



2. ábra – Közszolgálati Lenyomat kutatócsoport (a szerző saját szerkesztése)

A kutatócsoport fő célkitűzése, hogy a fenntarthatóságot, ezen belül is a fenntarthatóság közszolgálati aspektusait vizsgálja, úgymint:

- konferenciák szervezése a témában (hazai és nemzetközi);
- közös publikációk írása a témában – nemzetközi kutatócsoport tagjaival;
- közös pályázatok indítása, amennyiben az felmerül és lehetséges.

A kutatócsoport fő célkitűzése, hogy a fenntarthatóságot, azon belül is a CO_2-kibocsátást – karbonlábnyomot – mérje, és az oktatásban a hallgatók számára is érthetővé tegye. Szemléletüket formálja azáltal, hogy tevékenységükben majdan ők is kövessék a fenntarthatósági aspektusokat, és vegyék figyelembe a tevékenységeknél – a különböző projekttevékenységeknél a karbonlábnyom mértékét.

Ezzel egy olyan missziót tölt be a kutatócsoport, amely saját területén és saját kutatócsoporti hatókörében támogatja, hogy mind a magyarországi közszolgálat, mind Magyarország, mind európai és globális szinten a fenntarthatóság kritériumai érvényesüljenek, és a Jó Állam indikátorrendszerhez szolgáltasson adatokat. Ezeket a kutatásokat a kutatócsoport az NKE különböző hivatásrendjeinek különböző prioritásai mentén kell, hogy folytassa, ugyanakkor rengeteg egymással közös és a civil üzleti világgal is hasonló kritériumot kell vizsgálnia.

A rendőrség és a fenntartható fejlődés

Hazánk rendelkezik a Nemzeti Fenntartható Fejlődési Keretstratégiával, amely szerint a négy alapvető erőforrás megléte nélkül nem biztosítható a nemzedékek szellemi és anyagi jólétének elősegítése. A négy alapvető stratégia: az emberi, a társadalmi, a természeti és a gazdasági.

Fő célkitűzése, hogy ezen alapvető stratégiák közép-, illetve hosszú távon elősegítsék országunk fejlődését, figyelembe véve a hazai adottságokat és feltételeket.

A rendőrség ugyan külön nem rendelkezik fenntartható fejlődési stratégiával, mégis muszáj nekik is szem előtt tartaniuk.

Herman Daly[1] szerint a fenntartható fejlődésnek három kritériuma van:

1. Amit a környezetbe bocsátunk, az nem haladhatja meg a környezet befogadó/feldolgozó képességét.
2. Amit a környezetből kitermelünk, az nem haladhatja meg a környezet újratermelő képességét.
3. A nem-megújuló erőforrások felhasználásának a mértéke nem haladhatja meg azt az ütemet, amilyen arányban helyettesíteni tudjuk őket megújuló erőforrásokkal. [8]

A rendőrségi épületek energiahatékonyságának növelése

A rendőrség épületei hatékonyság szempontjából korszerűtlenek. Az energiafelhasználás csökkentése érdekében csökkenteni kell az energia végfelhasználását, a főbb rendszerelemek, hőtermelők hatásfokát javítani kell, valamint figyelembe kell venni a megújuló energiák nyújtotta lehetőségeket is.

Az energia végfelhasználását csökkenteni lehet például a nyílászárók cseréjével és az épületek hőszigetelésével. A hőtermelők hatásfokát korszerűbb kazánok beépítésével lehet növelni. A megújuló energiák közül számottevően a nap- és a szélenergiát tudják hasznosítani.

Ezek a változtatások nemcsak az alkalmazottakra terjednek ki, hanem közép- és hosszú távon szolgálják az egész rendőrség energiaellátását, valamint versenyképességének javítását.

[1] Herman Edward Daly (1938) amerikai közgazdász professzor.

A megújuló energiák rendőrségen belüli használatának növelése

A rendőrség épületeinek energiahatékonysága a mai állapotukban nem megfelelő. Sok esetben ezek az épületek már élettartamuk felén is túlhaladtak, fűtésük korszerűtlen, a nyílászárók régiek, nem gazdaságosak, villamosrendszerei elavultak.

A Környezet és Energia Operatív Program (KEOP) pályázatok

A Környezet és Energia Operatív Program (KEOP) alapvető célja Magyarország fenntartható fejlődésének elősegítése, az energiafelhasználás csökkentése, a megújuló energia felhasználásának növelése, ezáltal környezetünk megóvása.

A KEOP fejlesztései elősegítik Magyarország versenyképességének az erősödését, az elmaradottabb területek felzárkózását, a jólét növekedését.

„A programok célja az alábbi fejlesztések megvalósítása:

Megvalósítandó fejlesztések

1. Egészséges tiszta települések

– hulladékgazdálkodás,
– szennyvízkezelés,
– ivóvízminőség-javítás.

2. Vizeink jó kezelése

– jó árvízvédelmi gyakorlat kialakítása,
– komplex vízgyűjtőfejlesztés,
– a települési szilárdhulladék-lerakóinak rekultivációja,
– a környezet kármentesítése,
– a vízgazdálkodás tervezése.

3. Természeti értékeink jó kezelése

– védett természeti értékek és területek megőrzése, helyreállítása, fejlesztése,
– élőhely-megőrző beruházások, a mező- és az erdőgazdálkodás infrastrukturális alapjainak megteremtése,
– az erdeiiskola-hálózat fejlesztése.

4. A megújuló energiaforrás-felhasználás növelése

5. Hatékony energiafelhasználás

6. Fenntartható életmód és fogyasztás

– a fenntartható fogyasztás elősegítése,
– az e-környezetvédelem céljaihoz kapcsolódó fejlesztések.” [1: 179]

– A rendőrség ugyan nem kapcsolódik közvetlenül a fenntarthatósághoz, azonban hatással van rá. A szerv feladata elsősorban a rend védelme és a közbiztonság fenntartása, amely feladatok ellátásával körülbelül 50 ezer fő foglalkozik. Ennyi ember ellátása jelentős energiafelhasználást igényel, emiatt a hatékony energiafelhasználás és a megújuló energiák használatának növelése nagyon fontos.
– A rendőrségre irányuló fejlesztéseknek mindenképp hosszú távúnak kell lenniük, mivel ezek folyamatos fenntartása elengedhetetlen az ország számára, és csak így lesz fenntartható.
– Hazánkban az energiafelhasználás 40%-a az épületekben történik. A rendőrség épületei, nyílászárói, energiaellátó rendszerei korszerűtlenek, ezért ez az arány ezen épületek tekintetében a hazai átlagnál jóval magasabb.

A fosszilisenergia-felhasználás csökkentésének több lehetősége van, amelyek jellemzően a következők:

– az energia végfelhasználásának csökkentése (például az épületek külső határoló szerkezeteinek utólagos hőszigetelése, külső nyílászárók cseréje);
– főbb rendszerelemek, hőtermelők hatásfokának javítása (például hagyományos kazánok cseréje modern, magas hatásfokú hőtermelőre);
– megújuló energiák alkalmazásának lehetősége (talajhő, napenergia stb.).

A megvalósítandó fejlesztések közvetlen célja lehet az általános rendőrségi feladatok ellátására létrehozott szervek számára a költséghatékony működési környezet megteremtése, amely az egyes intézmények működési költségeit jelentősen csökkenti, az általa nyújtott szolgáltatások ár-érték arányát pedig feltétlenül tovább javítja. Ugyancsak közvetett eredményként lehet számolni a projektek demonstrációs hatásaival (megszépülő, megújuló épületek, közintézmények külső és belső állapotával kapcsolatos állampolgári elvárásoknak való megfelelés), de kitűzött célként említhetjük az intézmények alkalmazásából álló személyek környezettudatosságának növelését is.

A fejlesztések környezeti hatásterülete nemcsak az alkalmazottakra terjed ki, hanem közép- és hosszú távon a rendőrség és az egész ország energiaellátásának biztonságát és versenyképességének javítását, a környezeti állapot megőrzését is hivatott szolgálni. A rendőrségi épületek energiahatékonyságának növelését egyszerre valósítja meg az Európai Unió, Magyarország, valamint az ÁRFSZ úgy, hogy a fenntartható fejlődés környezet- és természetvédelmi céljait összehangolja a helyi társadalmi elvárásokkal. A már jelentős számban véghez vitt fejlesztések (KEOP-5.6.0, KMOP-3.3.3) első számú célja olyan beruházási, megvalósulási költségében céltudatos, racionális, szakaszolható kivitelezésű energetikai konstrukció megvalósítása, amely az üzemeltetési költségek vonatkozásában a környezetienergia-hasznosítás alkalmazásának többletberuházási költségeit észszerű időn belüli megtérüléssel biztosítja. A projekt a megújuló energia hasznosításával a kiemelt környezetre vonatkozó környezetvédelmi hatások tekintetében a jelenlegihez

képest jelentősen csökkenti a terhelést (fosszilisenergia-hasznosítás csökkentése, ezáltal a környezetszennyezés mérséklése).

Magyarország energiakitettsége ellen sokat tehetnek a rendőri szervek vezetői. A már lezárult és a meghirdetett (KEHOP-5.2.2, KEHOP-5.2.11) Környezet és Energia Operatív Program pályázatának általános célja a környezetet kevésbé terhelő, megújulóenergia-alapú energiatermelés elterjesztése, a megújuló energiaforrásokon alapuló hő- és villamosenergia szerepének növelése, és ezen keresztül a szén-dioxid-kibocsátás csökkentése.

A konstrukció hozzájárul az üvegházhatású gázok kibocsátásának, valamint a fosszilisenergia-felhasználás csökkentéséhez, a megújuló energiák használatának, az uniós kötelezettségvállalásának teljesítéséhez, az importfüggőség mérsékléséhez, továbbá a költségvetési szervezetek célcsoportjai energiaköltségeinek csökkentéséhez.

A megújuló energiaforrások alkalmazhatóak hő- vagy villamosenergia termelésére, illetve ezek együttes, kapcsolt előállítására, így az ilyen projektek megvalósulása a megújuló források szélesebb körű alkalmazását és nagyobb részarányát biztosítja, hozzájárulva a stratégiai célkitűzések teljesítéséhez, jól szolgálva ezzel az energetikai és a környezeti fenntarthatóságot.

Kiemelt célkitűzés a környezeti szempontok érvényesítése a gazdasági fejlődésben. Ennek egyik feltétele a megújuló energiaforrások nagyobb arányú felhasználása, ezáltal a társadalom és a környezet harmonikus viszonyának kialakítása. A rendőrség elmaradása ezen a téren sokat javult, ma már úgy nem lehet a rendőrségnek új épületet építeni, hogy annak energiaigényét zömmel ne megújuló vagy környezetbarát forrásból elégítse ki.

A Környezet és Energetikai Operatív Programokkal a rendőrségnél is kézzelfogható közelségbe került a fenntartható fejlődési pályára való ráállás támogatása, a megújuló energiák minél szélesebb körű elterjesztése, és nem utolsó sorban a környezettudatos életmód meghonosítása, hazánk és a rendőrség energiakitettségének jelentős csökkentése.

1. táblázat – A rendőrségi flotta CO_2-kibocsátása 2016-ban megyénkénti bontásban (a szerző saját szerkesztés)

2016. év							
Szervek	Gépjárművek száma (db)	Éves kilométer-futás (km)	Átlagfutás (km/gk.)	Tankolt összeg (Ft)	Tankolt mennyiség (liter)	Átlag-fogyasztás	**Karbon-lábnyom**
BRFK-kerületek	1 030	13 977 548	13 618	458 725 888	1 413 997	10,12	4 478
Baranya	252	5 612 815	22 220	149 898 192	469 581	8,37	1 487
Bács	467	10 842 248	23 321	299 957 760	921 937	8,50	2 918
Békés	331	6 298 967	19 041	170 619 168	524 424	8,33	1 661

2016. év							
Szervek	Gépjárművek száma (db)	Éves kilométer-futás (km)	Átlagfutás (km/gk.)	Tankolt összeg (Ft)	Tankolt mennyiség (liter)	Átlag-fogyasztás	**Karbon-lábnyom**
Borsod	395	10 409 596	26 244	281 509 984	867 440	8,33	2 745
Csongrád	388	6 936 085	17 844	201 703 456	626 165	9,03	1 983
Fejér	223	5 320 659	23 596	156 072 832	487 356	9,16	1 543
Győr-Sopron	259	5 612 034	21 497	171 631 312	528 713	9,42	1 674
Hajdú	289	7 300 111	25 207	208 783 760	642 818	8,81	2 036
Heves	163	4 858 772	30 089	139 064 000	428 183	8,81	1 355
Komárom	155	4 125 706	26 657	113 354 632	350 956	8,51	1 112
Nógrád	173	4 425 875	25 799	117 387 936	361 211	8,16	1 143
Pest	449	12 701 312	28 665	356 910 976	1 100 236	8,66	3 482
Somogy	248	7 818 693	31 403	207 128 624	639 471	8,18	2 025
Szabolcs	399	10 776 171	27 217	291 009 248	896 523	8,32	2 839
Jász-Nagykun	233	6 090 511	26 240	163 712 512	508 914	8,36	1 612
Tolna	151	4 084 296	27 023	118 836 632	365 867	8,96	1 159
Vas	207	3 617 428	17 467	100 605 744	309 762	8,56	980
Veszprém	199	4 781 899	23 930	130 996 384	403 587	8,44	1 278
Zala	228	4 919 224	21 652	135 063 424	418 836	8,51	1 325
RSZG	39	560 223	14 364	8 995 846	27 014	4,82	85
ORFK-szervek	350	3 591 015	10 538	83 418 896	257 036	7,16	814
készenléti rendőrség	1 267	20 433 267	18 561	675 074 371	2 109 819	10,33	6 683
reptéri rendőrség	79	843 963	10 695	24 423 360	75 213	8,91	238
BSZKI	26	268 260	10 837	7 158 368	21 883	8,16	69
NOK	19	34 677	1 825	1 370 731	3 847	11,09	12
BM-közmunka	1	35 282	35 282	766 779	2 364	6,70	7
Összesen	8 020	166 276 637	20 749	4 774 180 900	14 763 154		46 745

Forrás: dr. Németh Gyula rendőr ezredes. Számítás: [9]

Ez a táblázat megyénként tartalmazza a gépjárművek darabszámát, a megtett kilométert, az elfogyasztott üzemanyagot és a karbonlábnyom-kalkulátorral (ezen adatok alapján) CO_2-kibocsátást tonnában.

Látható, hogy az első helyen a Készenléti Rendőrség, a második helyen a BRFK, a harmadik helyen pedig a Pest Megyei Rendőr-főkapitányság áll.

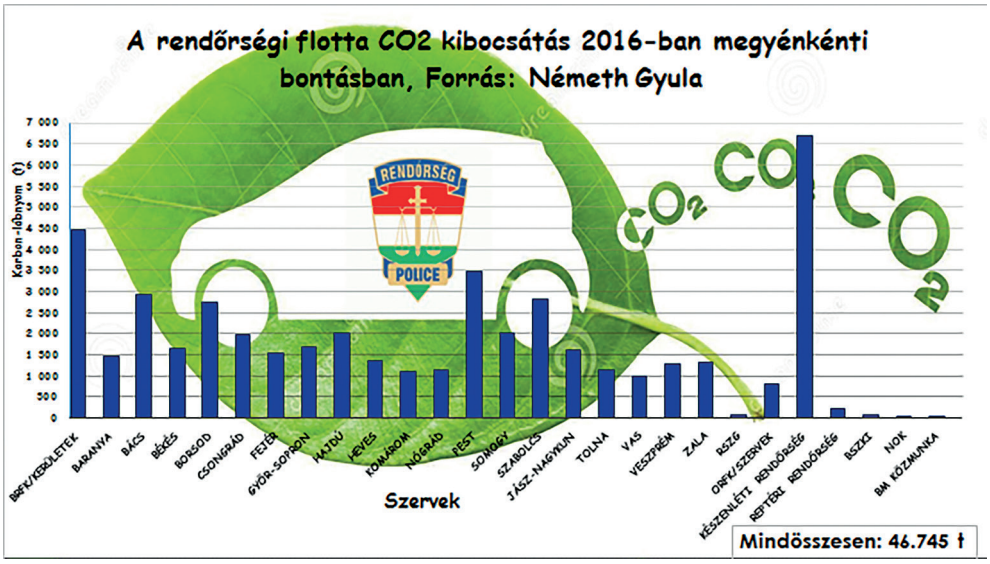
Ennek oka valószínűleg az, hogy egy nagyobb városokban nagyobbak a távolságok, több a jelzőlámpa, ami lassítja a haladást, ezáltal megnő a megtett kilométerek száma

és a fogyasztás is, így a CO_2-kibocsátás is magasabb lesz. Ezenkívül ennél a három szervezetnél és a készenléti rendőrségnél a legtöbb a gépjármű olyan feladatokat lát el, ami a magasabb CO_2-kibocsátást eredményezi.

Az utolsó három helyen a BM, a NOK és a BSZKI vannak.

Ezeknek a szervezeteknek kevesebb a feladatuk, emiatt nem kell annyit a helyszínre kiszállni, aminek következtében kevesebb lesz a fogyasztás és a CO_2-kibocsátás is, míg a három legtöbbet fogyasztó szerv szerteágazóbb tevékenységet folytat.

A megyéket tekintve pedig azt látjuk, hogy a nagyobb területű megyéknek (Bács-Kiskun, Hajdú-Bihar vagy Borsod) nagyobb az üzemanyag-felhasználásuk, így a megtett kilométer alapján a karbonlábnyomuk is ekként alakul.



1. diagram – A rendőrségi flotta CO_2-kibocsátása 2016-ban megyénkénti bontásban (a szerző saját szerkesztése)

A táblázat és a diagram adataiból jól látszik, hogy a szén-dioxid kibocsátásának mértéke egyenes arányban áll a rendőri szerv létszámával (ennek függvénye az épületek és a gépjárművek száma). A létszámviszonyok tükrözik a megye méreteit, a lakosságának számát, valamint a rendőri intézkedések mennyiségét.

2. táblázat – A rendőrség villamosenergia-felhasználásából adódó CO_2-kibocsátás 2016-ban megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

Szerv	Villamosenergia				
	Felhasználás GJ	Felhasználás kWh	Karbon-lábnyom	Költség ezer Ft	Fajlagos ktg. Ft/GJ
BRFK	26 452	7 347 778	2 338,724	227 589	8 604
Bács-Kiskun MRFK	13 000	3 611 111	1 149,381	134 082	10 314
Baranya MRFK	6 361	1 766 944	562,401	72 174	11 346
Békés MRFK	8 325	2 312 500	736,046	83 829	10 069
Borsod-A-Z MRFK	7 287	2 024 167	644,272	75 518	10 363
Csongrád MRFK	13 104	3 640 000	1 158,576	133 578	10 194
Fejér MRFK	3 881	1 078 056	343,134	42 233	10 883
Győr-M-S MRFK	6 509	1 808 056	575,486	67 345	10 347
Hajdú-B MRFK	8 060	2 238 889	712,616	88 506	10 980
Heves MRFK	3 068	852 222	271,254	32 907	10 724
Jász-N-Sz MRFK	3 974	1 103 889	351,357	45 887	11 546
Komárom-E MRFK	3 078	855 000	272,138	32 685	10 619
Nógrád MRFK	3 791	1 053 056	335,177	32 964	8 696
Pest MRFK	6 777	1 882 500	599,181	76 491	11 287
Somogy MRFK	7 754	2 153 889	685,561	69 565	8 971
Szabolcs-Sz-B MRFK	16 538	4 593 889	1 462,189	172 826	10 450
Tolna MRFK	2 966	823 889	262,236	32 903	11 092
Vas MRFK	5 632	1 564 444	497,947	54 201	9 623
Veszprém MRFK	3 517	976 944	310,952	37 419	10 639
Zala MRFK	5 954	1 653 889	526,416	57 140	9 596
Készenléti R	43 805	12 168 056	3 872,971	524 233	11 967
NSZKK	3 658	1 016 111	323,418	33 752	9 228
NOK	2 768	768 889	244,730	27 087	9 784
RRI	2 531	703 056	223,776	44 975	17 771
Adyligeti RSZKI	2 812	781 111	248,620	26 077	9 275
Körmendi RSZKI	1 249	346 944	110,429	13 477	10 789
Miskolci RSZKI	1 804	501 111	159,499	16 689	9 253
Szegedi RSZKI	1 130	313 889	99,908	13 755	12 168
	215 788	**59 940 278**	**19 078,395**	**2 269 887**	

Számítás: [9]

Ez a táblázat megyénként tartalmazza a villamosenergia-felhasználást GJ-ban, kWh-ban, ennek költségét E Ft-ban és a fajlagos költségét is, valamint a karbonlábnyom-kalkulátorral (ezen adatok alapján) a CO_2-kibocsátást tonnában.

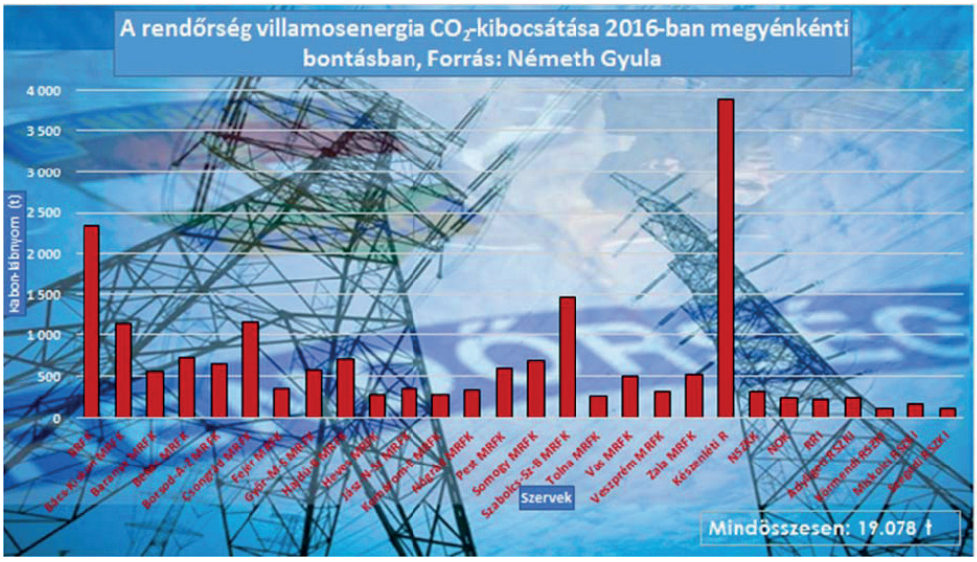
A Pest MRFK adatai kedvezőbbek a többi MRFK egységnyi szervezetre jutó részénél, aminek egyik oka az, hogy a KMOP-projekt keretében több épületet elláttak napelemes rendszerrel, a másik ok pedig az, hogy a világítótesteket is lecserélték energiatakarékos izzókra, illetve fénycsövekre.

Az első helyen a készenléti rendőrség, a másodikon a BRFK, a harmadikon pedig a Szabolcs-Szatmár-Bereg MRFK található.

Ennek oka valószínűleg az, hogy ezeknél a szervezeteknél nagyobb épületeket tartanak fent, mint a kisebb városokban, feladatkörük is szélesebb, valamint a lakosság száma is befolyásolja ezt. A nagyobb épületek miatt nagyobb a villamosenergia-felhasználás, mivel több munkavállalót kell alkalmazniuk, emiatt a CO_2-kibocsátás is magasabb lesz. A Szabolcs-Szatmár-Bereg MRFK több olyan országos feladatot is ellát, amelyek más megyéket nem érintenek.

Az utolsó három helyen az RRI (Repülőtéri Rendőr Igazgatóság), a Miskolci RSZKI és a Körmendi RSZKI áll.

Ezek kisebb szervezetek, nem igényelnek annyi foglalkoztatottat, valamint kisebb épületek is elegendők a feladatok elvégzésére, így a CO_2-kibocsátás értelemszerűen kevesebb lesz.



2. diagram – A rendőrség villamosenergia-felhasználásából adódó CO_2-kibocsátás 2016-ban megyénkénti bontásban (a szerző saját szerkesztése)

3. táblázat – A rendőrség hőenergia-felhasználásából adódó CO_2-kibocsátás 2016-ban megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

Szerv	Hőenergia			
	Felhasználás GJ	Karbon-lábnyom	Költség ezer Ft	Fajlagos költség Ft/GJ
BRFK	16 964	1 176,336	105 337	6 209
Bács-Kiskun MRFK	129	8,945	617	4 783
Baranya MRFK	10 262	711,599	59 061	5 755
Békés MRFK	1 187	82,310	2 921	2 461
Borsod-A-Z MRFK	5 330	369,599	38 276	7 181
Csongrád MRFK	475	32,938	2 792	5 878
Fejér MRFK	220	15,255	1 341	6 095
Győr-M-S MRFK	11 987	831,216	61 502	5 131
Hajdú-B MRFK	3 115	216,004	18 918	6 073
Heves MRFK	45,6	3,190	354	7 773
Jász-N-Sz MRFK	72	4,993	403	5 597
Komárom-E MRFK	5 897	408,916	35 755	6 063
Nógrád MRFK	6 064	420,497	29 889	4 929
Pest MRFK	1 633	113,237	10 745	6 580
Somogy MRFK	2 813	195,062	24 361	8 660
Szabolcs-Sz-B MRFK	4 058	281,394	27 029	6 661
Tolna MRFK	182	12,620	582	3 198
Vas MRFK	741	51,383	3 861	5 211
Veszprém MRFK	725	50,274	4 665	6 434
Zala MRFK	-	0,000	0	0
Készenléti R	4 967	344,427	26 347	5 304
NSZKK	-	0	0	0
NOK	-	0	0	0
RRI	17 446	1 209,760	64 513	3 698
Adyligeti RSZKI	-	0	0	0
Körmendi RSZKI	-	0	0	0
Miskolci RSZKI	-	0	0	0
Szegedi RSZKI	-	0	0	0
	94 312,6	6 539,955	519 270	

Számítás: [9]

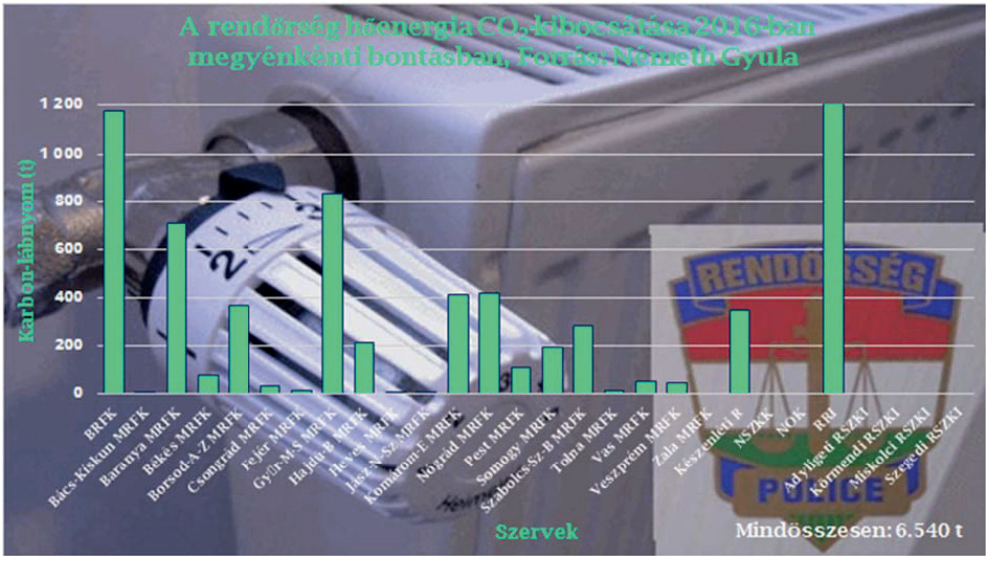
Ez a táblázat megyénként tartalmazza a hőenergia-felhasználást GJ-ban, ennek költségét E Ft-ban és a fajlagos költségét is, valamint a karbonlábnyom-kalkulátorral (ezen adatok alapján) a CO_2-kibocsátást tonnában.

Az első helyen az RRI, a másodikon a BRFK, a harmadikon pedig a Győr-Moson-Sopron MRFK található.

Az utolsó hat helyen a Zala MRFK, az NSZKK, a NOK, az Adyligeti RSZKI, a Körmendi RSZKI, a Miskolci RSZKI és a Szegedi RSZKI áll.

Ezek a szervezetek valószínűleg nem, vagy csak minimális mennyiségű hőenergiát használnak, a fűtést helyette földgázzal oldják meg, emiatt nagyon elenyésző, vagy nincs is CO_2-kibocsátásuk.

A Pest MRFK adatai jelentősen elmaradnak az átlagtól, ennek az az oka, hogy mindösszesen egy rendőrkapitányságon és egy rendőrőrsön vételeznek távhőt, a fűtést zömében földgázzal, de több helyszínen hőszivattyúval oldják meg.



3. diagram – A rendőrség hőenergia-felhasználásból adódó CO_2-kibocsátása 2016-ban megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

4. táblázat – A rendőrség földgáz-felhasználásból adódó CO_2-kibocsátása 2016-ban megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

Szerv	Földgáz			
	Karbon-lábnyom	Felhasználás GJ	Költség ezer Ft	Fajlagos költség Ft/GJ
BRFK	5 617	95 079	330 484	3 476
Bács-Kiskun MRFK	1 581	26 758	96 312	3 599
Baranya MRFK	588	9 962	38 800	3 895
Békés MRFK	1 471	24 901	81 901	3 289

Szerv	Földgáz			
	Karbon-lábnyom	Felhasználás GJ	Költség ezer Ft	Fajlagos költség Ft/GJ
Borsod-A-Z MRFK	1 647	27 880	97 454	3 495
Csongrád MRFK	1 724	29 187	125 824	4 311
Fejér MRFK	948	16 048	61 835	3 853
Győr-M-S MRFK	900	15 238	51 887	3 405
Hajdú-B MRFK	1 258	21 287	75 407	3 542
Heves MRFK	559	9 467	33 662	3 556
Jász-N-Sz MRFK	854	14 458	71 439	4 941
Komárom-E MRFK	321	5 440	24 802	4 559
Nógrád MRFK	279	4 727	20 427	4 322
Pest MRFK	1 421	24 049	88 241	3 669
Somogy MRFK	1 404	23 773	87 391	3 676
Szabolcs-Sz-B MRFK	2 520	42 653	143 313	3 360
Tolna MRFK	836	14 144	46 327	3 275
Vas MRFK	1 120	18 966	64 036	3 376
Veszprém MRFK	595	10 064	37 028	3 679
Zala MRFK	888	15 028	51 119	3 402
Készenléti R	9 654	163 431	751 109	4 596
NSZKK	465	7 870	29 165	3 706
NOK	506	8 568	35 214	4 110
RRI	0	0	0	0
Adyligeti RSZKI	839	14 197	36 267	2 555
Körmendi RSZKI	605	10 234	31 600	3 088
Miskolci RSZKI	1 022	17 306	51 450	2 973
Szegedi RSZKI	378	6 392	22 812	3 569
	39 999	**677 106**	**2 585 306**	**99 278**

Számítás: [9]

Ez a táblázat megyénként tartalmazza a földgáz-felhasználást GJ-ban, ennek költségét E Ft-ban és a fajlagos költségét is, valamint a karbonlábnyom-kalkulátorral (ezen adatok alapján) a CO_2-kibocsátást tonnában.

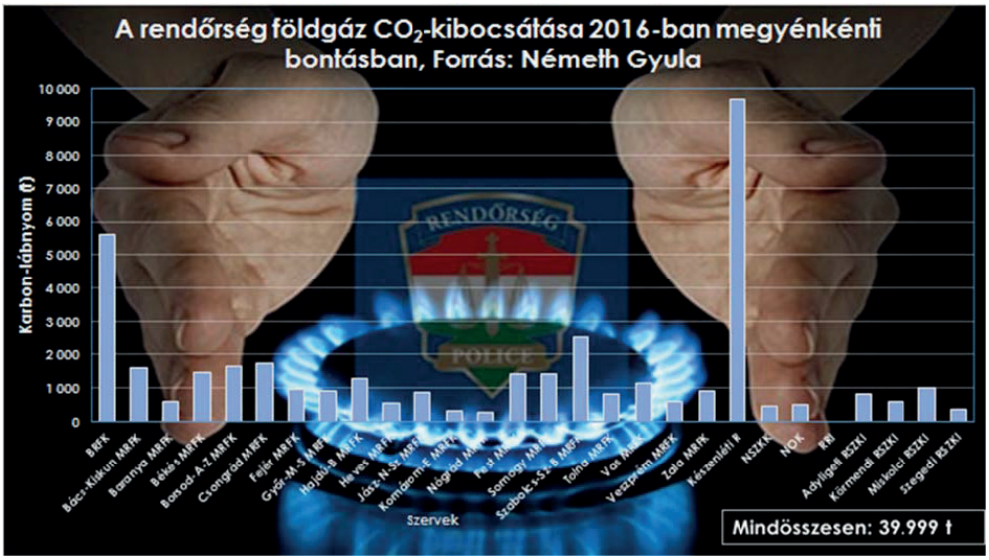
Az első helyen a készenléti rendőrség, a másodikon a BRFK, a harmadikon pedig a Szabolcs-Szatmár-Bereg MRFK található.

Ennek oka valószínűleg az, hogy ezeknél a szervezeteknél nagyobb épületeket tartanak fent, mint a kisebb városokban, feladatkörük is szélesebb, valamint a lakosság száma is befolyásolja ezt. A nagyobb épületek miatt több a földgáz-felhasználás, mivel több munkavállalót kell alkalmazniuk, emiatt a CO_2-kibocsátás is magasabb lesz. A földrajzi elhelyezkedés is befolyással lehet erre.

Az utolsó három helyen a Komárom-Esztergom MRFK, a Nógrád MRFK és az RRI (Repülőtéri Rendőr Igazgatóság) Igazgatóság áll.

Az új rendőrségi épületek építésénél igyekeznek a földgázt mellőzni. A geotermikus energia, a hőszivattyúk alkalmazása egyre nagyobb teret kap, így várható, hogy az épületek fűtésének szén-dioxid-kibocsátása jelentősen csökkeni fog.

Ezek a szervezetek Magyarország legkisebb megyéiben találhatók, így kisebb létszámmal és épületekkel működnek, ezáltal felhasználásuk is kisebb lesz. Kevesebb létszámú alkalmazottal rendelkeznek, emiatt a CO_2-kibocsátásuk itt lesz a legkisebb.



4. diagram – A rendőrség földgázfelhasználásából adódó CO_2-kibocsátása 2016-ban megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

5. táblázat – Magyarország rendőrségi szervezeteinek CO_2-kibocsátása megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése

Szerv	Gépjármű	Villamosenergia	Hőenergia	Földgáz	Összesen
BRFK	4 478	2 339	1 176	5 617	13 610
Bács-Kiskun MRFK	2 918	1 149	9	1 581	5 657
Baranya MRFK	1 487	562	712	588	3 349
Békés MRFK	1 661	736	82	1 471	3 950
Borsod-A-Z MRFK	2 745	644	370	1 647	5 406
Csongrád MRFK	1 983	1 159	33	1 724	4 899
Fejér MRFK	1 543	343	15	948	2 849
Győr-M-S MRFK	1 674	575	831	900	3 981

Szerv	Gépjármű	Villamosenergia	Hőenergia	Földgáz	Összesen
Hajdú-B MRFK	2 036	713	216	1 258	4 222
Heves MRFK	1 355	271	3	559	2 189
Jász-N-Sz MRFK	1 612	351	5	854	2 822
Komárom-E MRFK	1 112	272	409	321	2 114
Nógrád MRFK	1 143	335	420	279	2 178
Pest MRFK	3 482	599	113	1 421	5 615
Somogy MRFK	2 025	686	195	1 404	4 310
Szabolcs-Sz-B MRFK	2 839	1 462	281	2 520	7 102
Tolna MRFK	1 159	262	13	836	2 269
Vas MRFK	980	498	51	1 120	2 650
Veszprém MRFK	1 278	311	50	595	2 234
Zala MRFK	1 325	526	0	888	2 739
Készenléti R	6 683	3 873	344	9 654	20 555
NSZKK	0	323	0	465	788
NOK	12	245	0	506	763
RRI	238	224	1 210	0	1 672
Adyligeti RSZKI	0	249	0	839	1 087
Körmendi RSZKI	0	110	0	605	715
Miskolci RSZKI	0	159	0	1 022	1 182
Szegedi RSZKI	0	100	0	378	478
RSZG	85	0	0	0	85
ORFK/szervek	814	0	0	0	814
BSZKI	69	0	0	0	69
BM-közmunka	7	0	0	0	7
Összesen:	**46 743**	**19 078**	**6 540**	**39 999**	**112 360**

Számítás: [9]

Ez a táblázat megyénként tartalmazza Magyarország rendőrségi szerveinek karbonlábnyom-kalkulátorral kiszámított CO_2-kibocsátását tonnában, a gépjármű, a villamosenergia, a hőenergia és a földgáz felhasználásának tekintetében, valamint szervezetenként/megyénként összesítve is.

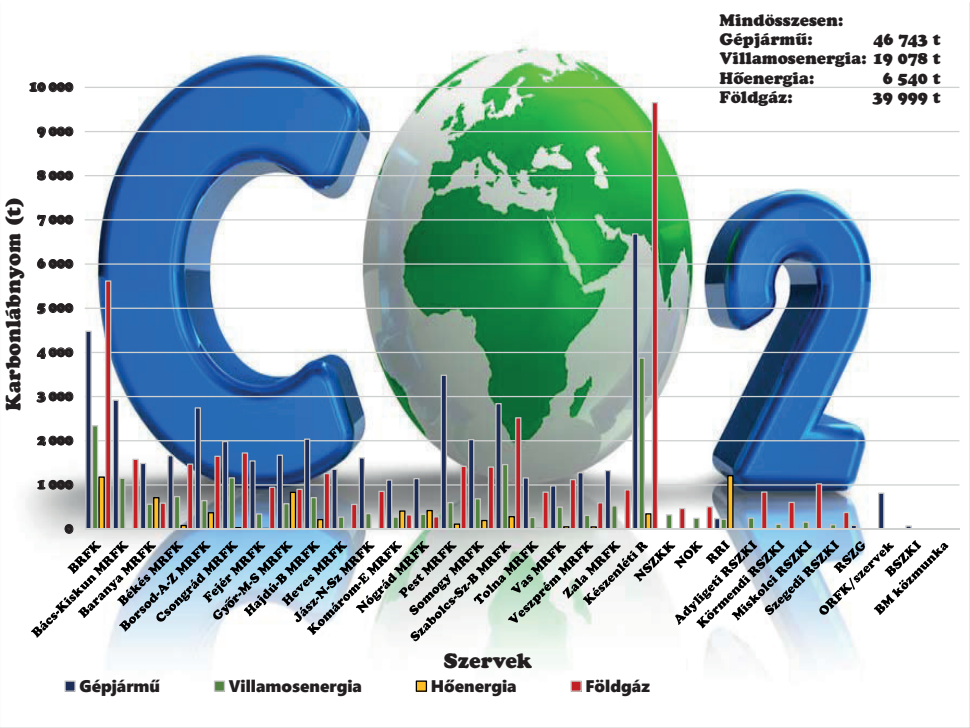
Látható, hogy az első helyen a készenléti rendőrség, a második helyen a BRFK, a harmadik helyen pedig Pest Megyei Rendőr-főkapitányság áll.

Ezek a legnagyobb szervezetek, itt a legmagasabb az alkalmazottak száma és központi feladatokat látnak el, ezért nyilvánvaló, hogy náluk a legmagasabb a CO_2-kibocsátás.

Az utolsó három helyen, ahol van mért adatunk, a Nógrád MRFK, a Komárom-Esztergom MRFK és az RRI (Repülőtéri Rendőr Igazgatóság) áll.

Mivel Nógrád és Komárom-Esztergom országunk legkisebb megyéi közé tartoznak, egyértelmű, hogy itt lesz a legkisebb a CO_2-kibocsátás. A kisebb területnek nincs szük-

sége nagy épületre és sok ember foglalkoztatására, valamint feladatkörük is keskenyebb skálán mozog. Az RRI-hez nem tartozik olyan sok feladat, így róla is ugyanezeket lehet elmondani.



5. diagram: Magyarország rendőrségi szervezeteinek CO_2-kibocsátása megyénkénti bontásban (Németh Gyula alapján a szerző saját szerkesztése)

Befejezés

A fentartható fejlődés kapcsán az 1987-es Brundtlandi Bizottság általi értelmezéshez kell visszanyúlnunk, mely szerint a „fenntartható fejlődés olyan fejlődés, amely kielégíti a jelen szükségleteit anélkül, hogy veszélyeztetné a jövő nemzedékek esélyét arra, hogy kielégíthessék szükségleteiket”. [10: 41]

Az egyre érezhetőbb éghajlatváltozás és az erőforrások végességének fenyegetése, valamint az energiabiztonság égető szükségességének kérdése világossá tette, hogy a fosszilis energiahordozók használatának globális szintekben való csökkentése elkerülhetetlenné kell hogy váljon. Úgy kell tehát a vállalatok működési keretrendszerét kialakítani, hogy

az összeegyeztethető legyen napjaink elvárásaival. Erre utal írásában Harangozó [11] is, aki hangsúlyozza, hogy „a különböző vállalati funkciókban (például termelés menedzsment, logisztika, innovációmenedzsment, pénzügy, számvitel és marketing) számos olyan részcél van, amely összeegyeztethető a karbonlábnyom csökkentésének céljával, és amelyek megvalósulása érdekében hasznos lehet a vállalati karbonlábnyom számszerűsítése, a vállalati információs rendszerbe történő integrálása és kommunikációja".

Kerekes [12] szerint, hogy a fenntartható fejlődés brundtlandi definíciója nem közgazdasági, hanem etikai jellegű, mivel a generációk közötti egyenlőség elérését célozza, és nem a természet, hanem az „ember" szemszögből tekint a kérdésre. A fenntartható fejlődés „az ökológiai, a társadalmi és a gazdasági fenntarthatóságot egyidejű harmóniaként feltételezi".

Pónusz és Horváth [13] tanulmányukban a reverz logisztika feladataival foglalkoznak kiemelten élelmiszeripari vonatkozásban, a kutatás elméleti alapjául a 4 R modell szolgált, mely szerint elkülöníthetünk megelőző és utólagos feladatokat.

Az első megelőző feladat az alapanyagok arányának, mennyiségének csökkentése *(reduction at the source),* ennek alapelve a hulladékképződés megelőzése. A megelőző feladatok sorában a következő a hagyományos alapanyagok helyettesítése környezetbarát anyagokkal, technológiákkal, amely során a biotechnológia növekvő jelentőségét kell kiemelnünk *(replacement).*

Élelmiszeripari például hűtőipari vállalat ellátási láncának elemzésével foglalkoztak különös tekintettel a zöld logisztikai vonatkozásokra. [14] Ezek a szempontok napjainkban a fenntartható fejlődés elveinek elterjedésével egyre kiemeltebb figyelmet kapnak az élelmiszer-ellátási láncokban is. Az öko kultivációs módok, a kombinált szállítások arányának növelése kevésbé környezetszennyező szállítási ágak bevonásával, zéró hulladéktermelő gyár, –20% energiafelhasználás csökkentés 2020-ra irányelv, mind hozzájárulnak a CO_2-emisszió csökkentéséhez.

A harmadik és egyben utolsó megelőző feladat az anyagok újrahasználása *(reusing),* amelyre tipikus példa a többutas csomagolóanyagok használata. Ilyenek lehetnek az üveg boros palackok, műanyag rekeszek, műanyag kannák, raklapok. Ennek a módszernek az alkalmazása jelentősen megbonyolítja a fennálló logisztikai rendszert, hiszen „a hagyományosan egyutas rendszereket kétirányúvá kell tenni". [15]

- Az reverz logisztika *utólagos feladata* az anyagok feldolgozása, újrahasznosítása *(recycling).* Ebben az esetben a termék elveszíti eredeti funkcióját, a folyamat célja a még felhasználható anyagok visszanyerése. Amennyiben a visszanyerés megfelelő minőségű, akkor felhasználható az eredeti rész gyártásához is. A feldolgozás többféle módszerrel történhet, amelyek közös jellemzője, hogy komoly mennyiségű erőforrás felhasználását igénylik, de ez a mennyiség még mindig kevesebb, mint amennyi az eredeti alapanyag előállításához kellene. [16]

A zöld beszerzés a zöld ellátási láncból egy kis szeletet érint, mely mellett még megtalálható a zöld ellátási lánc tervezés, zöld ellátási lánc megvalósítás és karbon menedzsment is. Pónusz–Kozma [17] szerint, mely Emmett és Sood *Green Supply Chain* [18] könyvének alapkoncepciója, nyújtja az egyik legösszetettebb és teljes körű felfogást a témát illetően.

Irodalomjegyzék

[1] Knoll I. – Lakatos P. szerk.: *Közszolgálat és fenntarthatóság.* ÁROP 2.2.21 Tudásalapú közszolgálati előmenetel, Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[2] www.uni-nke.hu/hirek/2017/10/18/bemutattak-az-idei-jo-allam-jelentest (a letöltés ideje: 2017. 11. 17.)

[3] Korsós-Schlesser F. – Marselek S.: Fenntarthatósági indikátorok változásainak elemzése Magyarországon, tekintettel a klímaváltozásra. *Acta Carolus Robertus,* 6. évf. 1. szám, 2016, 105–116. http://ageconsearch.umn.edu/bitstream/233908/2/10.pdf (a letöltés ideje: 2016. 10. 30.)

[4] http://2010-2014.kormany.hu/download/b/87/70000/ESTRAT%20r%C3%B6vid%C3%ADtett%20magyar%20verzi%C3%B3.pdf (a letöltés ideje: 2017. 11. 20.)

[5] www.innovacio.hu/download/allasfoglalas/2011_11_30_NFFS2012.pdf (a letöltés ideje: 2016. 10. 20.)

[6] Wiedmann, T. – Minx, J.: *A Definition of 'Carbon Footprint'.* Research & Consulting, Research Report 07-01, Durham, 2007.

[7] www.uni-nke.hu/egyetem/intezmenyfeljesztesi-terv-2015-2020 (a letöltés ideje: 2016. 10. 20.)

[8] Fordítás: Fleischer T.: *Fenntartható fejlődés: környezeti, társadalmi és gazdasági tényezők. Magyarország globális környezete 2020-ig. Háttértanulmányok a magyar külstratégiához I.* MTA Világgazdasági Kutatóintézet, Budapest, 2007.

[9] www.carbonsolutionsglobal.com/ellentetelezes/hitelesitett-karbonlabnyom-kalkulator (a letöltés ideje: 2016. 10. 20.)

[10] WCED: *Our common future.* 1987. https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf (a letöltés ideje: 2018. 04. 16.)

[11] Harangozó G.: A karbon lábnyom koncepció szerepe a vállalkozásfejlesztésben. In Dr. Csiszárik-Kocsir Á. szerk.: *Városfejlesztés a XXI. században. VI.* Budapest, 2016, 129–146. http://kgk.uni-obuda.hu/sites/default/files/11_Harangozo-Gabor.pdf (a letöltés ideje: 2018. 04. 16.)

[12] Kerekes S.: A fenntarthatóság közgazdaságtani értelmezése. In Bulla M. – Tamás P. szerk.: *Fenntartható fejlődés Magyarországon: Jövőképek és Forgatókönyvek.* Új Mandátum Kiadó, Budapest, 2006, 196–211.

[13] Pónusz M. – Horváth A.: Zöld logisztikai fejlesztések aspektusai az EU-ban. Via Futuri 2014 nemzetközi konferencia: *„Fenntarthatóság – Versenyképesség – Regionális fejlődés, Elméleti kutatások, gyakorlati alkalmazások".* 2014. november 27–28. *Marketing és menedzsment,* különszám, 150–157.

[14] Logó R. – Pónusz M. – Kozma T.: Hűtőipari vállalkozás ellátási láncának értékelése és logisztikai megoldásainak vizsgálata. In Vágány J. – Fenyvesi É. szerk.: *Multidiszciplináris kihívások, sokszínű válaszok.* BGE KVIK Közgazdasági Intézeti Tanszéki Osztály, Budapest, 2016, 115–137.

[15] Mike G.: *A logisztika környezetvédelmi kérdései és a reverz logisztika.* 19. számú műhelytanulmány, 2002.

[16] Réger B.: A logisztika aktuális kérdései napjainkban. ZMNE, Budapest, 2008.

[17] Pónusz M. – Kozma T.: (2017) Zöld ellátási láncok és innovatív megoldások. *Logisztika,* 3. évf. 2. szám, 2017, 61–66.

[18] Emmett, S. – Sood, V.: *Green Supply Chains, An Action Manifesto.* Wiley, 2010.

The Carbon Footprint of the Public Service

Péter Lakatos

Sustainable development is a complex and multidisciplinary research area of today's science.The research of water security and climate change has a considerable history at the National University of Public Service (NKE).Taking as its base an earlier research workshop (Military Ecological Footprint Centre), the Ludovika research group for the Footprint of Public Service has been established and through this an international research capacity emerged, based on which NKE may be one of the acknowledged research places of national higher education. The conference held on 04 May 2017 pointed out the importance of measuring carbon dioxide emission (carbon footprint) at the level of professional orders of public service.This may even be one of the Good State indicators of NKE in the future.This paper is based on chapters of the book entitled Public Service and Sustainability.

Future plans include the establishment and operation of an excellence centre with the participation of an international research network.

Keywords: sustainability, public service, carbon footprint, professional orders, Good State

Antal Örs

Green Infrastructure Solutions for Flood Prevention – Innovative Investment Opportunities[1]

The tendencies and consequences of recent meteorological events indicated that climate adaptive and risk-based approaches and new flood control measures became necessary for creating the conditions of long-term, sustainable flood control system in the urban areas in Hungary. The implementation of green infrastructures is the most feasible way to accomplish these goals. Using green infrastructures to mitigate urban flood risk and to promote ecosystem services is globally on the rise, since the urbanization processes, population shifts and the increasing size of built environment contributed significantly to the increase of flood risk originating from extreme weather events. This paper studies the applied green infrastructure methods and scenarios in order to promote the integration of these innovative options into the Hungarian policies and development concepts, including the possible implementation of green developments in urban areas.

Keywords: urban flood, drainage, ecosystem, runoff, multi-purpose, adaption

Introduction

Supporting the implementation of green infrastructures is a modern approach to provide safety, health and liveable environment. Furthermore, these solutions are key steps towards efficient adaption to climate change. Floods triggered by heavy rainfall events mean an emerging safety and environmental concern at global and European level, too. In close association with this, similarly to other European cities or metropolitan areas, flash floods and urban floods have caused increasing problems in Hungary in recent years. This tendency requires plans and actions for the future in order to tackle the risk of potential damages. This study examines primarily the strategical and practical aspects of green solutions in the context of flood control and water management. This assessment requires different approaches regarding urban and rural areas, since there is a significant

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Concha Győző Doctoral Program.

difference between the applicable measures. It is my conviction that one of the most efficient and available ways for the prevention of urban floods is the implementation of strategies that deal with green solutions as supplementary facilities of the urban drainage system. In this study I assess these provisions and technological solutions with regard to applicability in urban areas in Hungary. Additionally, my goal in this paper is to reveal possibilities of multi-level governance and innovative technological features for the suitability for multi-purpose usage within the framework of integrated urban water management and climate change adaption policies.

The Role of Green Infrastructures in Built Environment

The description of green infrastructures (GI) can be widespread, since these solutions incorporate a large system of natural or semi-natural territories and artificial green surfaces providing better life circumstances and operation of ecosystem elements. Hereby, a generally accepted accurate definition of green infrastructures does not exist, only comprehensive explanation can give approximate approach to GI solutions. These technologies, in general, are built up by green or blue elements and can supplement or redeem grey infrastructures such as roads, canals, tunnels, built facilities etc. [1] In other interpretation, applying green solutions ensure the beneficial effects of ecosystem services, since green strategies and solutions mean a conceptual approach aiming to establish an integrated network through the protection and development of ecosystem elements. In this context, GI solutions and green provisions contribute to the mitigation of harmful effects of global meteorological processes, such as extreme weather conditions. Additionally, in close connection with this, GI options have significant role in the resilience and adaption of urban areas to natural hazards originated from meteorological factors. [2]

Besides the environmental, social and economic benefits, relevant studies and published literature set the positive effects of GI into the following four main factors: [3]

- *Absorption:* by creating and preserving natural surfaces to absorb rainfall in order to reduce flooding and recharge water supplies (playgrounds, parks, bioswale, green roofs);
- *Connection:* by the contribution to the reduction of carbon dioxide release in transportation (green transit lines) and to the accessibility of destinations (natural trails);
- *Cooling:* by the reduction of the warming up of grey infrastructures and surfaces in urban areas during the summer period;
- *Protection:* by creating shoreline green surfaces to mitigate the harmful effects of coastal and river flooding in urban areas.

Through the above mentioned factors, the main priorities of green infrastructural investments and developments are the following objectives:

- The retention of the population by improving the conditions of quality of life and air quality (preserving health and physical activity, establishing workplaces, development of social life);
- the adaption to climate change, and the mitigation of effects of extreme meteorological events (reducing "heat-island" effect, adapting local assets such as buildings, facilities and infrastructure, flood prevention and protection measures);
- efficient resource management (preserving environmental assets and biodiversity, economical use of natural resources).

Green infrastructures can be interpreted in different scales and levels depending on land use, size and type of territory and the geographical or hydrographic features. At regional level, in rural territories conserving floodplains instead of building dams and levees is a typical adaptive green solution in water management. Preventing runoff generation in rural landscapes by temporary storage or natural barriers and stream control can relevantly mitigate the flood risk in downstream areas, furthermore, water retention has the potential to ensure water supply during drought season. [4] GI solutions cover both the natural environment and applied technology to provide their benefits, thus at local level, green roofs, bioswales, parklands, planting trees, gardens, water bodies or porous pavers, while at regional level, preserved forests and floodplains, diversion ponds, re-naturalized wetlands and territories are known as widespread solutions for implementing GI strategies.

In the following sections this study focuses on the feasibility of adaptive green infrastructures in urban areas, especially dealing with GI assets applied in flood protection and water management. For getting to know the GI technological features, it is necessary first to discuss the basis of strategies and legislation that established their application.

The Background and Situation of Green Infrastructures

GI based development plans have become emphasized in different policy strategies and local or regional development concepts over the last decade due to the ongoing urbanization processes and increasing effects of climate change. The application of GI solutions related to flood control management are indicated in the relevant document as follows:

The EU Biodiversity Strategy to 2020

GI solutions are integral part of the EU's biodiversity policy. According to the EU Biodiversity Strategy adopted by the European Commission, the protection of the increasingly endangered biodiversity and ecosystems in Europe is among the most urgent problems in the European politics and community. The Biodiversity Strategy indicates six main fields, where provisions are needed for the improvement of ecosystems and the conservation of natural resources. Some of these targets are the protection and restoration of ecosystems and the establishment of green infrastructures. The strategy mentions the importance of promoting GI solutions for the prevention of hazardous flood events besides the conservation of healthy natural ecosystems and biodiversity. In order to meet these challenges, the strategy finds it important to reconnect the fragmented ecosystems and green areas to establish the basis of functional connectivity and long-term sustainability. [5]

EU GI Strategy

The EU GI Strategy of rural and urban areas is based on the provisions specified in the Biodiversity Strategy of the Commission. The implementation of GI solutions is an integral segment of the EU's disaster risk management policy as important supplementary elements of the dedicated disaster risk mitigation infrastructure. Regarding water management, the strategy puts natural green methods in the foreground, since these solutions directly contribute to providing good water quality and the mitigation of flood and drought risk at the same time. The European Union finds it important to ensure financial instruments to support GI projects and investments under the auspices of the energy, environmental, climate and innovation politics of the EU. Additionally, the strategy mentions that the significance and return rate of GI investments is especially high in urban environments, since more than 60% of the EU's population live in urban areas. [6]

Directive on the assessment and management of flood risks

Flood risk and flood hazard maps elaborated in the framework of Directive 2007/60/EC of the EU in Hungary demonstrate potential territorial flooding and areas endangered by flooding on the geospatial digital interface in the viewpoint of river flooding. Risk assessment related to the digital map stock incorporates specific "green provisions" among the types of different scenarios for risk management measures in large river basin level, such as the termination of inappropriate land use, through the conservation and restoration of ecosystems and the transformation of vegetation and rehabilitation of foreshores. In

the context of local measures for improving green infrastructures, this directive does not specify concrete provisions. [7]

EU framework of water policy

The main objective of the EU Water Framework Directive is the conservation and restoration of aquatic ecosystems and water-dependent land ecosystems in the member states of the European Union. [8] The criteria of EU Water Framework have to be enforced in flood control measures as well, therefore, the promotion of good ecological status is a significant priority of water management. In this context, green infrastructures are feasible alternatives to bridge the gap between environmental and disaster prevention objectives in the framework of river basin management.

Best practices on flood prevention, protection and mitigation

Some of the specified objectives of the guideline proposed by the water directors of the member states of the European Union are to promote the reactivation and increase of flood effect reducing ability of natural wetlands through the following measures: [9]

- to improve the land use in river basins,
- to rehabilitate natural floodplains,
- natural reforestation,
- adequate land use of floodplains (preventive land use),
- and the increase of water-permeable terrain surfaces.

National Water Strategy

The National Water Strategy of Hungary (Jenő Kvassay Plan), approved by the Hungarian Government in 2017, considers GI solutions important in the context of agriculture to establish and improve the conditions of water retention, water supply, irrigation and change of land use. Furthermore, the strategy highlights that as part of the territorial water management, the existing flood control infrastructure is too defensive and non-resilient to the effects of the global meteorological processes. Therefore, those strategies and infrastructures are necessary to be implemented, which enable the cohesion of flood prevention and water supply efforts by supporting the ecosystem services and protecting natural wetlands. In addition, the Kvassay Plan emphasizes that the biggest professional challenge of water management for the future is to find and implement preventive and

adaptive resilient solutions. In this context, the usage of green infrastructures both at local and regional level is inevitable to fulfil these objectives. [10]

National Development and Territorial Development Concept

The Hungarian National Development and Territorial Development Concept promotes solutions based on local resources through following "green" and "blue" economic goals and principals. Among the tasks of development policy with regard to urban structural measures, the concept highlights the expansion of green areas, the rehabilitation of public parks and the separation of densely built-in areas by open, green surfaces. Another necessary provision is the improvement of green and natural areas into the network for the sustainable and compact urban structures. [11]

Long-term (2030) Development Concept of Budapest

Some of the most important strategical priorities of the Development Concept of Budapest are improving the quality of natural environment and developing the green area system and infrastructure dedicated to environment protection aspects. According to the concept, the size of green areas in the capital is decreasing since the year 1990. Besides the poor availability of green areas, the spatial distribution of public parks is uneven within the boundaries of the city. In the city center of Budapest, where the green development potential is low due to the high density of buildings, alternative solutions, such as green roofs and roof gardens are needed to be considered besides the conventional afforestation in the unoccupied transport and parking zones. For the mitigation of the "heat-island effect", the concept incorporates the following general measures:

- the usage of permeable paving,
- the mitigation of the ratio of surface paved by nonporous materials,
- and enhancing the size of green areas. [12]

The concept promotes the creation of climate-conscious built environment, although it does not mention specific GI solutions among the listed measures aiming the renewal of the flood protection system.

Integrated Urban Development Strategy of Budapest

The integrated strategy reveals the areas with significant ecological potential in Budapest, furthermore it calls attention to the climate consciousness and green approach related to city renewal programs. It notes that these developments must be implemented first in the framework of local governmental and municipal projects in order to serve as exemplary projects for further investments. In this context, the strategy specifies green roofs and green façade developments. Besides these principals, the integrated strategy mentions the flood control measures aiming the prevention of flood damages triggered by climate change as an important priority. Furthermore, regarding the riverside of the Danube, the renewal of flood protection system is also a significant medium-term task in accordance with the recreational green development of the islands and riversides along the river Danube in Budapest. [13]

Overall, the different strategies, concepts and relevant regulations point out that the implementation of GI programs or investments must be carried out in accordance with territorial development concepts and objectives, therefore the effective feasibility of GI solutions are highly dependent on integrated approach and planning. Despite the fact that GI developments in flood management have already left their early era, the urban development concepts and flood damage-relief plans do not specify concrete local interventions with GI solutions.

Adaption to Flooding with Green Infrastructures in Municipal Areas

As I mentioned before, the flood risk of a city is usually highly dependent on the provisions implemented in the framework of upstream river and floodplain management outside the city boundaries. Notwithstanding, other flood phenomena can occur as a result of weather conditions that affect directly the urban, densely inhabited areas. These potential flood types are as follows: [14: 35–36]

- *river floods* originated from heavy rainfall or intensive snow melting,
- *flash floods,* which mean the flooding of smaller river streams triggered by excessive rainfall exceeding the absorption ability of the soil,
- *urban floods* caused by the insufficient structure and capacity of urban drainage systems during intensive rainfall,
- *coastal floods* occur in coastal areas by the temporary increase of sea level,
- *groundwater flooding* is the consequence of groundwater level rising, triggered by constant precipitation.

Regarding these phenomena, it can be concluded that the flood risk of urban areas depends on local and regional factors. Local characteristics, such as drainage system, local flood control infrastructure, urban structure, street network or the degree of integration can influence the effects and consequences of local precipitation. Besides these factors, flood exposure in urban inhabited territories can be affected by external circumstances and regional measures such as upstream river and river basin management. The prevention efforts require different approaches in terms of local and regional provisions, since in enormous river catchment areas, where flood occurrence is a natural phenomenon of the rivers, actions intent to control and prevent the harmful effects by interventions aiming to improve the runoff conditions, for example. On the contrary, with regards to urban water management, in most cases the measures aim to prevent the formation of flooding by interventions in the framework of urban water management.

From the perspective of preventive measures, the physical effects of potential flood damages are the most relevant factors in urban areas, since economic, social and health related effects are usually consequences of material or physical impacts, such as the damages on transport infrastructure, buildings, environment, private and public assets, vulnerable and critical objects, public utility system etc. [14: 35] Similarly to many other European metropolitan areas, Budapest and other Hungarian big cities have to face relevant flash and urban flood risk triggered by extreme weather events. Furthermore, meteorological tendencies project increasing risk and severity for the future. In this context, the innovative and prevention focused mentality requires green approach and the usage of green infrastructures as integrated provisions in the framework of urban development strategies, since GI solutions fulfil many other criteria related to the adaption to climate change, too. The most important feature of urban GI solutions is the promotion of the capacity of soil for water retention by the increase, restoration and preservation of natural surfaces and the vegetation in order to reduce peak discharge or to impede the accumulation of water. Based on these principals, GI measures in urban areas tend to achieve the mentioned objectives by implementing the following local provisions:

- to restore, increase and maintain green surfaces inside the cities by establishing green roofs, parks, gardens, wetlands etc.
- to increase the surface runoff by building porous and permeable terrain surfaces,
- to maintain and increase beyond the boundaries of the city border by appropriate land use, forestation or re-naturalization.

The following image (Figure 1.) demonstrates the ratio of infiltration and runoff of storm-water depending on the different types of land cover. As it can be seen, the quantity of runoff can exceed by nearly 50% in the case of lands covered by highly impervious surface, which is not negligible in the context of potential flood damages.

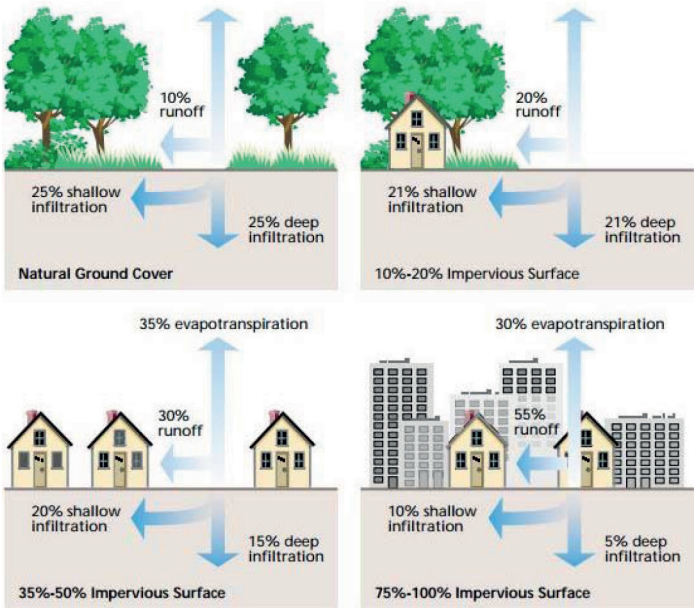


Figure 1. The impact of surface cover on runoff characteristics [15]

It should be noted that according to Figure 1 further 30% of the accumulated floodwater evaporates, though this process takes hours and depends a lot on meteorological conditions. In these circumstances, this amount of floodwater also needs to be considered, when determining the runoff volume in the case of artificial impervious land surfaces.

The EEA No 2/2012 report on urban adaptation to climate change in Europe notes that the optimal system of green infrastructures consists of connected networks of green and blue elements, since as a system, GI solutions enable urban areas to deliver economic, social, cityscape and environmental benefits in addition to the response to flooding and water quality problems. [14: 35]

The following chapter discusses specific GI solutions that have the ability to absorb and to store floodwater in order to mitigate the harmful effects of extreme rainfalls and flood events in urban areas in Hungary.

Using Green Infrastructures to Mitigate Urban Flood Risk

In the prevention of urban and flash floods in Hungary that occur in a sudden, unexpected way, it is difficult to differentiate between local and regional provisions, since regional

measures on the upstream and catchment areas are as important as local interventions with particular regard to flashfloods forming on small watercourses.

This study examines primarily those practices below, which provide local green solutions for flood control objectives in an integrated strategic framework, taking into account further environmental, social and economic benefits. Furthermore, these solutions promote the adaption of urban areas to climate change.

Bioswale

Bioswales (Figure 2.) are usually established near paved and asphalted areas (alongside sidewalks, pedestrian streets, roads or parking lots) with slopes in order to reduce surface water runoff originated from intense precipitation by the infiltration and orientation to downslope sites. Furthermore, this solution contributes to groundwater supply and recharge by planted vegetation and soil that enables higher infiltration and water filtering.

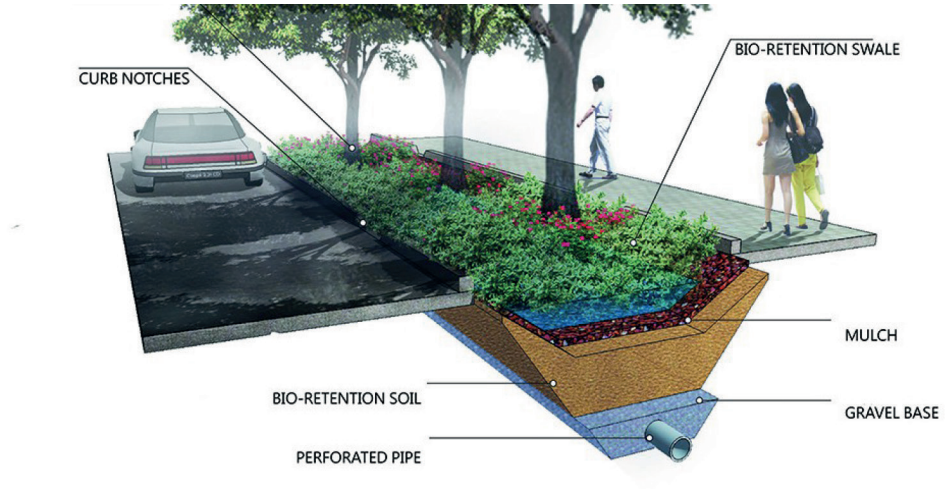


Figure 2. Bioswale [16]

Considering that bioswales are installed with an underground drainage system of their own (stone bed, gravel or overflow pipe), they are capable of collecting and carrying further excess water as part of a system or network of other GI elements. The surface of bioswale is usually covered by shrubs, grasses, flowers or sometimes trees, therefore, it delivers a better and more livable city environment and landscape. [17]

Rain gardens or bio-retention cells

The operation of rain gardens or the more complex bio-retention cells (Figure 3.) with exact design criteria is very similar to that of the bioswale. These green solutions are usually established inside grassy private areas or parks to collect and infiltrate rainwater by directing the runoff straight into the rain garden through inflow lines or pipes from roofs or non-porous surfaces. The rain garden soil components filter out pollutants from the water before entering into the ground-water circulation. [17]

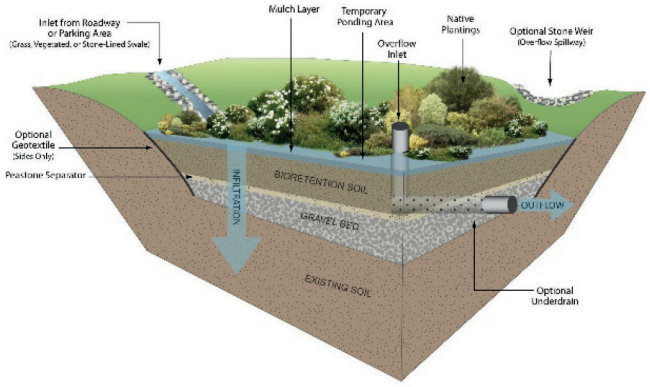


Figure 3. Bio-retention cell [18]

For bioswales and rain gardens natural soil profile is used with high permeability rate and good infiltration ability. The main difference between rain gardens and bioswale is that while bioswales convey further the large quantity of rainwater that cannot be absorbed, raingardens hold and pond the runoff. An overflow structure is designated in rain gardens and bio-cells to remove excess water in case of large rains. In this context, it is obvious that bioswales are more applicable for flood relief purposes in larger areas and surfaces.

Permeable paving

Porous pavement (Figure 4.) has the advantages similar to rain gardens and bioswales, since this solution allows runoff to infiltrate into the ground through the small gaps between the blocks of pavers made of stone, brick or concrete. In the void spaces permeable materials such as soil, sand or gravel ensure the excess water to flow down. Also, the gravel and underground media can contribute to the improvement of water quality. [17]

Figure 4. Porous pavement [19]

Porous pavements are often installed in residential and densely built-in central urban areas, where the traffic load is moderate and the axle road of the vehicles does not exceed the load carrying capacity of the pavement. Regarding sidewalks and pedestrian streets, in addition, pavements reduce ice formation in cold conditions, which makes pedestrian traffic safer, and it also comes along with a lower heat-island effect. However, the construction and maintenance costs significantly exceed the value of asphalt cover.

Green roofs

Rooftops of buildings covered by vegetation over a growing medium and drainage layer laid on waterproof moisture interception membrane (Figure 5.) reduces storm-water runoff in densely built-in urban areas by the capability of rainwater storage and retention. The excess water is carried into the sewer system through drainage and pipes, or transpired by the vegetation or simply evaporated. In this way, green roofs significantly improve the air quality and the habitat by providing outdoor areas, and reduce the heat-island effect by the evaporation and avoidance of heat-absorbing cover surfaces. [17] Furthermore, a proper insulation layer within the green roof system contributes to higher energy efficiency.

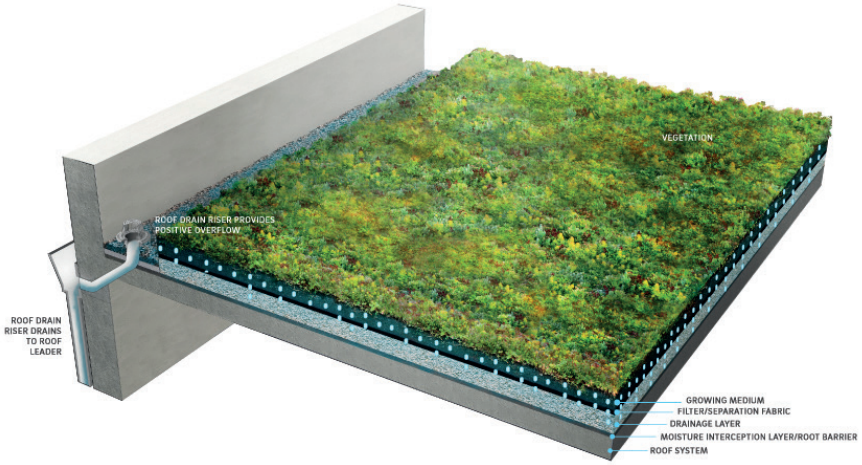


Figure 5. Green roof [20]

Blue roofs

Similarly to green roofs, another sustainable GI solution for storm-water management is establishing blue roof systems (Figure 6). The main function of these solutions is to detain excess rainwater generally in a tray or cell system established on rooftops in order to reduce and prevent runoff and sewer overflow impact on the streets.

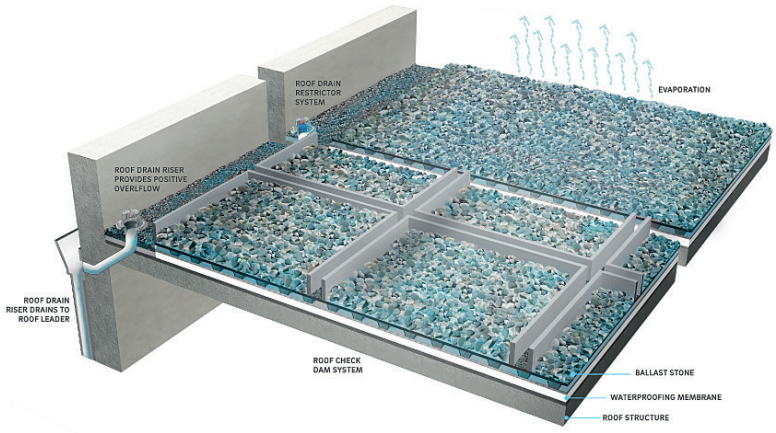


Figure 6. Blue roof [20]

The collected and detained amount of water can be used for alternate purposes, such as irrigation, cooling, water supply or specific household uses, or the water is released into the municipal sewer system. Blue roofs have the advantage over green roofs that they can also be established on roof systems whose load-carrying capacity is not sufficient for installing green roof systems. In addition, their beneficial effect on runoff mitigation is equivalent to green roofs, but the construction cost is relevantly lower.

Storm-water tree trenches

Storm-water tree plantings are usually established close to impervious areas, from where the excess water originating from precipitation is directed and collected into trenches through curb channels in order to be infiltrated into the soil. Tree roots in soil layers promote and speed up this process, in addition, tree canopies capture raindrops and help evaporation, thus diminishing the quantity of accumulated rainwater on the surfaces. Tree plantings in urban areas have numerous other advantages besides flood relief, since they provide shadow, better cityscape appearance and habitat for urban fauna (insects, birds etc.), absorb carbon-dioxide, furthermore, the presence of trees mitigates the heat-island effect, too. [17]

Green tram track

Natured tram track in urban areas (Figure 7.) must meet different requirements, since in addition to tram service, these facilities must be drivable for emergency vehicles and drainable in case of intense precipitation. In order to match these conditions, green tram tracks demand specific construction and design implemented by the following layers and elements:

- filter layer (e.g. gravel),
- isolation layer (e.g. membrane),
- grass paver or substrate (soil),
- vegetation on surface (grass or sedum),
- noise absorber device (e.g. porous rubber),
- and track drainage (optionally).

The water retention is mainly dependent on the type and thickness of vegetation. According to German guidelines, in grass tracks the thickness of the carrier medium needs to be more than 15 cm, while this parameter is 6–8 cm with regards to sedum on the surface. The evaporation rate of grass is higher, but sedum absorbs a higher proportion. The track

drainage system can be connected to the municipal sewer network thus conveying the runoff to be eliminated from the site. [21]

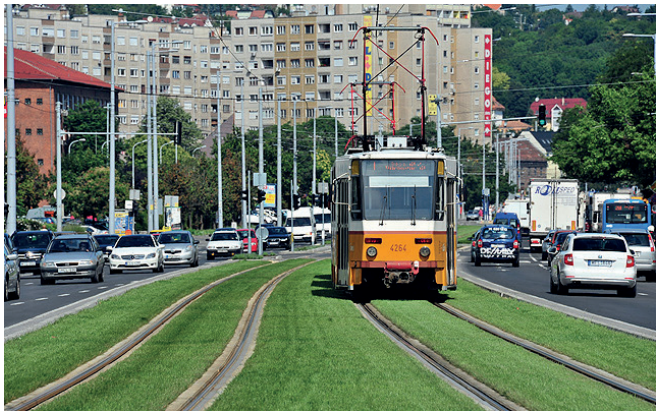


Figure 7. Green tram track in Óbuda, Budapest [22]

This GI solution also has many other beneficial effects besides flood relief. The low heat storage capacity of the planted green surface reduces the heat-island effect and the temperature in the track, which is not negligible in the context of transport safety. Evaporation and transpiration also cool down air temperature and the plants contribute to the improvement of air quality. Furthermore, this solution is much more efficient in the reduction of noise emission compared to the more rigid concrete blocks or asphalted surfaces.

Lastly, green tram tracks can be operated in urban areas with low maintenance costs and can be drivable by other vehicles in case of emergency situations.

As I mentioned, when examining the specific GI methods and solutions with regard to flood relief, it is important to make a distinction between rural and urban territories. Typical ecosystem-friendly green measures in rural areas are the restoration of wetlands, adaptive land use and the construction of emergency flood reservoirs and retention ponds. The methods described above are the most widespread and efficient solutions for applying green infrastructures for flood control purposes in metropolitan and inhabited areas. As follows from the theoretical and strategical approach of GI solutions, the important aspects of sustainable and efficient operations are the connection of different GI elements into networks and the multiple benefits providing above all climate adaptive ecosystem services. The following overall summary table (Table 1.), based on worldwide experiences and international guidelines, aims to promote the efforts to achieve these objectives and integrated approaches.

Table 1. The comparison of Green Infrastructures [Edited by the author.]

Note: ● promotes highly ● promotes moderately ● does not promote

GI solution	Reducing runoff	Ground-water recharge	Water retention/ water supply	Improving air quality	Leisure activities	Reducing heat-island effect	Potential sites/areas	Construc-tion/ Maintenance cost[2]
Bioswale	●	●	●	●	●	●	public parks, extended territories, sloped areas, parking lots, central sites	High/Low
Rain garden/ bio-cells	●	●	●	●	●	●	residential/private areas, public parks, recreation sites	Moderate/ Low
Permeable paving	●	●	●	●	●	●	pedestrian streets, sidewalks, city centers, parking lots	Moderate/ Low
Green roof	●	●	●	●	●	●	private/public buildings	High/ Moderate
Blue roof	●	●	●	●	●	●	private/public buildings	Moderate/ Low
Tree trench	●	●	●	●	●	●	parking areas, public parks, city centers, extended squares	Moderate/ Low
Green tram trench	●	●	●	●	●	●	fixed-track surface transportation	Moderate/ Low

Implementing GI strategies in Hungary

As I mentioned, planning and implementing GI investments and developments require integrated approach and multi-level governance. The concepts of protection against floods and adaption to global and regional meteorological processes appear at all levels of governance from local (municipal) to continental (European). In a given municipal area, the protection of assets and human life, and the enhancement of the level of protection

[2] Construction and maintenance costs are estimated values depending on local conditions, size and availability. The given values can be used for comparison.

against natural impacts are primarily the task of the settlement on operational level. [23] Regarding the protection against urban floods, local measures have major significance in implementing local infrastructure developments to improve the city resilience to flood hazards and climate impacts, since planning and the implementation is highly dependent on local conditions and circumstances. Therefore, integrated urban development strategies and development concepts of urban areas have a key role in this regard. The most important issues of national level are to provide GI compatible legal, regulatory and strategical frameworks, to support innovation and knowledge transfer along with the research related to adaptive solutions, and lastly to create funds and financial support systems. Regarding local actions, planning and implementation of GI strategies and urban developments through adapting local facilities, buildings and infrastructure to extreme weather events can be considered the most general tasks besides the municipal regulation and the allocation of resources.

The following figure (Figure 8.) demonstrates the main milestones in the implementation of green developments in urban areas. [14: 95–98]

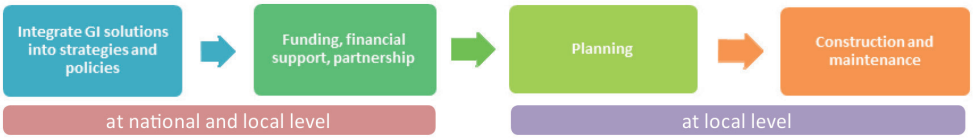


Figure 8. Recommendation for implementing GI strategies
[Edited by the author.]

Integration into strategies and policies implies particularly the following measures:

- the vindication of GI approach,
- the identification of GI options and specific solutions,
- reliance on scientific research along with international innovation and knowledge transfer,
- the promotion of multiple purposes (reducing energy use, CO_2 concentration, heat-island effect, improving air quality, community livability, city landscape and supporting water recharge, ecological services and biodiversity etc.)

Funding, financial support and partnership include:

- providing municipal resources,
- funding and financial support of research and sciences,
- state subsidies,
- tendering.

Planning has to be extended to the following tasks:

- the assessment of flood scenarios with and without green infrastructures,
- the determination of the amount of excess water that needs to be reduced or retained,
- the sufficient knowledge of local conditions (climate – especially precipitation values – geographical, geotechnical, urban structure characteristics, topography, existing infrastructure facilities and elements including the drainage and sewer system).

With regards to the above mentioned factors, besides the comprehensive knowledge of local infrastructural and geographical features, the basis of planning of GI options to reduce flooding are hazard mapping and vulnerability assessment. Highlighting the affected flood prone areas and knowing the potential damages are essential for adequate interventions. In addition to this, the digital data system of hazard mapping is an important tool of decision-making in the periods of prevention and response, too. The main factors that need to be considered in flood hazard mapping in urban areas are as follows:

- the intensity and distribution of expected rainfall,
- the topography and urban structure characteristics (to know the flow direction and flow accumulation of surface runoff),
- existing sewer system and its drainage capacity.

The regional weather conditions of the Carpathian Basin are difficult to compare to the countries affected by frequent severe monsoons, although extreme meteorological phenomena and harmful events experienced in recent years show increasing risk in Hungary, as well. Therefore, the prevention of local flood events that occur in a sudden and unexpected way became a timely question in Hungary in the framework of hillside water management, river-basin management and integrated urban water management, in organizational, regulatory and technological context, as well. The increasing tendency of extreme weather events in Hungary is confirmed by the assessments and data series published by the Hungarian Meteorological Service, which pointed out that hourly precipitation datasets showed the highest values in recent years regarding the capital city, Budapest. Furthermore, according to the weather analyses, an increase in frequency of extreme rainfall intensity can be projected to the future in urban areas, particularly during the summer months. [24]

All these circumstances make modern and adaptive prevention measures necessary within the framework of urban water management and integrated urban development, in which GI solutions and measures play an important role. Green solutions are not newfangled methods in Budapest (see for instance tram track line 1), although these implemented elements are not dedicated primarily to flood control and runoff reduction.

With attention to local characteristics and previous urban flood experiences, potential solutions and locations in Budapest can be considered as bioswales, bio-retention cells and green tram tracks on the Buda side with unique terrain characteristics, while bioswale, permeable pavings and green tracks can be applicable and efficient solutions on the denser Pest side. The implementation of green and blue roofs is primarily recommended in large numbers in residential areas and suburban regions. At the same time, it must be mentioned that GI elements themselves may not replace urban drainage and sewer systems, since green solutions can only be additional installations beside the dedicated drainage elements, with regard to flood control function. Therefore, the most effective way of implementing sustainable green developments is the combination with other solutions within the framework of integrated urban development strategies. As a first step, green infrastructures have to be shown horizontally within policy strategies and development concepts at national and local level as well, from urban planning to water management with special attention to adapting to the impacts of climate change. Based on this policy framework, the implementation of GI strategies may rely on two possible ways of co-governance: [25]

- by projects and investments initiated by the Government, where non-governmental actors are represented,
- or by projects initiated by non-state actors, where the Government plays an important role by supporting and financing the implementation.

Regarding cooperative governance, local municipalities always have a key role along with responsibility in the implementation and maintenance, too.

Summary

Regarding the urban areas in Hungary, river floods, flash floods and urban floods are relevant threatening effects, which are needed to be taken into consideration when establishing strategies, planning, prevention and response measures. Groundwater flooding is more likely in rural areas, where they can cause severe damages in agricultural territories.

Assessing the policy strategies and local or regional development concepts with respect to green solutions, in this paper I have pointed out that the role of green infrastructures in storm-water management is underrepresented compared to international policies, furthermore the documents do not define specific green provisions related to flood control methods. However, within the framework of climate change adaption, the improvement of green and natural areas and the mitigation of heat-island effect are displayed as relevant aspects. In this context, the effective feasibility of GI solutions is highly dependent on an integrated approach and strategical planning. Therefore, the im-

plementation of GI programs must be carried out in accordance with territorial or urban development concepts in which climate change adaptive, environmental, infrastructural and urban drainage improvement objectives are embedded.

Developing, building and restoring green infrastructure can be implemented in rural and urban areas differently. According to the researches and the experiences of established green design, the main aspect of adding GI solutions is to increase the green space cover in urban areas in order to reduce surface water runoff, thus to prevent sewer surcharge and overflow by limiting the discharge of the drainage system. In addition, the implementation of green measures of urban ecosystem services significantly contributes to the EU biodiversity and GI strategy. Assessing the specific GI solutions, their features and potential development possibilities, I made suggestions in this paper for the implementation of GI strategies and measures at governmental and local level. For efficient decision-making and planning I suggest to create flood hazard maps based on local urban flood threats in Hungary, and to issue a guidance related to urban flood risk management for Hungarian settlements to help and orientate the local leaders to incorporate green solutions into their integrated urban development strategies and urban flood risk management plans.

Bibliography

[1] Dige, G.: *What is green infrastructure, and why is it important?* European Environment Agency, 02.12.2015. www.eea.europa.eu/hu/articles/zold-infrastruktura-jobb-elet-termeszetes-megoldasokkal (14.08.2017.)

[2] Trust for Public Land, Adaption Clearinghouse, Georgetown Climate Center. www.adaptationclearinghouse.org/organizations/trust-for-public-land.html (14.08.2017.)

[3] Methodological guide for making the "Green Infrastructure Development and Sustainability Action Plan" (for TOP-2.1.2-15/6.3.2-15 Creating green city tender), Prime Minister's Office, Hungary, April 2016. www.kormany.hu/download/7/19/e0000/M%C3%B3dszertan_Z%C3%B6ld%20Infrast_%20Akci%C3%B3terv-hez.pdf (16.08.2017.)

[4] Nicholson, A. – Mcbain, W. – Hetherington, D. et al.: *Using green infrastructure and nature to manage flood risk.* CIRIA, 1–3.

[5] The EU Biodiversity Strategy to 2020, European Commission, European Union, 2011. COM/2013/0249 final – Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Commitee of the Regions Green Infrastructure (GI) – Enhancing Europe's Natural Capital.

[6] Directive 2007/60/EC of the European Parliament and of the Council on the assessment and management of flood risks, 23 October 2007.

[7] Directive 2000/60/EC of the European Parliament and of the Council on establishing a framework for Community action in the field of water policy, 23 October 2000.

[8] Best practices on flood prevention, protection and mitigation, European Union, September, 2003.

[9] National Water Strategy, Jenő Kvassay Plan, Government of Hungary, 2017.

[10] National Development and Territorial Development Concept, 2013.

[11] The Budapest 2030 Long-Term Urban Development Concept, Council of Budapest, February 2013.

[12] Budapest 2020 – Integrated Urban Development Strategy, Council of Budapest, February 2015. http://budapest.hu/Documents/ITS%20Integralt%20Varosfejlesztesi%20Strategia/BP_ITS_Strategia_Megalapozo.pdf (21.08.2017.)

[13] *Urban adaptation to climate change in Europe.* European Environment Agency Report No

2/2012, www.eea.europa.eu/publications/urban-adaptation-to-climate-change (22.08.2017.)
[14] Allen, T. – Franks Taylor, R. – Long, L.: *Green Infrastructure Guidance for Flood Reduction.* Great Lakes Coastal Resilience Planning Guide, June 23, 2016. http://greatlakesresilience.org/case-studies/infrastructure/green-infrastructure-guidance-flood-reduction (22.08.2017.)
[15] *Green Infrastructure Options to Reduce Flooding, Definitions, Tips and Considerations.* NOAA's Office for Coastal Management. https://coast.noaa.gov/data/docs/digitalcoast/gi-econ.pdf (23.08.2017.)
[16] *Green Earth Operations*. www.greenearthops.com/category/news/ (23.08.2017.)
[17] *The Value of Green Infrastructure.* A Guide to Recognizing its Economic, Environmental and Social Benefits, Center for Neighborhood Technology, 2010, 4. www.cnt.org/sites/default/files/publications/CNT_Value-of-Green-Infrastructure.pdf (23.08.2017.)
[18] *Bioretention Areas & Rain Gardens*, Massachusets Clean Water Toolkit. http://prj.geosyntec.com/npsmanual/bioretentionareasandraingardens.aspx (23.08.2017.)
[19] *Sustainable Capitol Region.* http://greenregionct.org/wp-content/uploads/2013/04/Green-Infrastructure-Banner1.jpg (23.08.2017.)]
[20] *Philadelphia Storm-water Plan.* www.pwdplanreview.org/upload/img/GreenRoof-WRT.png (23.08.2017.)
[21] *Effect and function of green tracks.* Grüngleis Netzwerk, Berlin, Germany. www.gruengleisnetzwerk.de/images/downloads/effects.pdf (23.08.2017.)
[22] *Forum on the extension of tram line 1*, Official website of Budapest, district III., Óbuda-Békásmegyer. https://obuda.hu/wp-content/uploads/2015/05/1-es-villamos.jpg (24.08.2017.)
[23] Hornyacsek, J.: *The defense capability with regards to diaster hazards.* "For our safety" Educational and Consultant Scientific Association, Budapest, June, 2011.
[24] Lakatos, M. – Hoffmann, L.: *Extreme rainfall in Budapest downtown.* Hungarian Meteorological Service, 30.05.2017. www.met.hu/ismeret-tar/erdekessegek_tanulmanyok/index.php?id=1885 (23.08.2017.)
[25] Buizer, M. –Elands, B. –Mattijjsen, T. et al.: The Governance of Urban Green Spaces in Selected EU-cities, January 2015. http://greensurge.eu/working-packages/wp6/files/Buizer_et_al_2015_D6.1_GREEN_SURGE_The_governance_of_urban_green_spaces_in_selected_EU_cities.pdf (30.08.2017.)

Zöld infrastruktúrák alkalamzásának lehetőségei az árvízmentesítés terén – innovatív fejlesztés

Örs Antal

A napjainkban zajló meteorológiai folyamatok tendenciái és következményei rávilágítottak arra, hogy a klímaváltozáshoz alkalmazkodó, kockázatalapú szemlélet és új árvízmegelőzési intézkedések szükségesek Magyarországon is a hosszú távon hatékony, fenntartható települési árvízvédelmi rendszerek feltételeinek megteremtése érdekében. Mindezek teljesülésére, a zöld infrastruktúrákra irányuló beruházások végrehajtása egyike a megvalósíthatóság szempontjából legkézenfekvőbb megoldásoknak. Az árvízi kockázat csökkentésére, illetve az ökoszisztéma szolgáltatások támogatására irányuló zöld infrastrukturális fejlesztések globális szinten növekvő tendenciát mutatnak, tekintve, hogy az urbanizációs folyamatok, a népesség eloszlásának változása és az épített környezet növekedése egyaránt jelentősen hozzájárultak a szélsőséges időjárási jelenségekből eredő árvízi kockázat megnövekedéséhez. Jelen kézirat vizsgálja az alkalmazott zöldinfrastruktúra-megoldásokat és -stratégiákat annak érdekében, hogy elősegítse ezen innovatív lehetőségek beintegrálását a hazai szakpolitikai

stratégiákba és fejlesztési koncepciókba, beleértve a zöld beruházások lehetséges megvalósítását a városias településeken.
Kulcsszavak: városi árvíz, vízelvezetés, ökoszisztéma, lefolyás, többcélú alkalmazás, adaptáció

Balog Fatime

The Role of the Unified Digital Radio System (URS) in Disaster Management

The more and more frequent and more and more intensive natural and civilizational disasters have set newer and newer challenges to organisations involved in heading off disasters. Their previously used communication systems were no longer able to meet the increased information requirements, thus a new solution was necessary which could effectively support the public safety organisations during cooperation. This solution was realised by building and using the Unified Digital Radio System (UDRS). The purpose of the article is to demonstrate how effective this TETRA-based network structure has been in practice in disaster management over the past decade.

Keywords: EDR, TETRA, disaster, emergency communications, disaster management, communication

Introduction

On 1 January 2001, in order to increase the effectiveness of disaster control, a new law enforcement agency was established: the National Directorate General for Disaster Management of the Home Office (NDGDM) where civil defence and the national and county fire departments were integrated and later the state fire department system and the agency of security industry also joined. While it is the NDGDM's responsibility to plan, organise, control and coordinate disaster management activities, disaster management is generally a national affair and the central control of defence is a state affair. The participants in disaster management are civil protection organisations, business organisations, the Hungarian Defence Forces, the law enforcement agencies, the Hungarian Meteorological Service, the National Ambulance Service, the local governments, other organisations and all Hungarian citizens. [1] The NDGDM, as the central body, is responsible for establishing the communication channels which are necessary to achieve effective cooperation. The complex communication system of disaster management includes both the public and the within-organisational and the cross-organisational platforms. Thus the decisive element of the cooperation is the within-organisational and the cross-organisational communication as it is needed to provide the necessary information

in connection with the expected behaviour and the control of their activities not only for the public but it is also vital to continuously keep contact between the participating organisations and the leading, controlling persons in case of an intervention.

Before the introduction of the UDRS most of the communication systems serving the needs of the public safety organisations had long been considered outdated and there was no reason for maintaining and developing them. The different organisations used completely different systems and there was no solution to effectively connect them which made it more difficult to coordinate the defence tasks. Building up the UDRS as a national network offered a solution to unblock this anomaly, and since its transmission, it has been providing a unified communication platform for the more effective cooperation of the organisations affected in defence. Beside the several advantages of the system based on modern technologies, during the practical application, recurrent problems occurred which made the work of the users more difficult. The purpose of the article is – beside highlighting the advantageous features – to contrast the possibilities hiding in the system and the negative experience of the applications and it also reveals how these can affect the performance of the tasks in certain cases.

Circumstances of the UDRS Establishment

Before the introduction of UDRS communication inside the organisations at both the national and the local level was provided with an open single-channel analogue half-duplex VHF and HF radio systems. As a consequence, there was a significant danger of the overload of the available frequency band and the monitoring of the transmitted communication. The nationwide radio communication network applied by the NDGDM for civil protection tasks was modern but it was not interoperable with any other standby radio systems. As part of the disaster management, the fire brigades used other channels which, in addition, could not even provide a countrywide coverage. All in all, the radio systems of the separate organisations did not provide interoperability and often the different systems used in a given organisation made the cooperation even more difficult. The cooperative communication was largely based on public wired and mobile telephone network in accordance with the general and public service conditions and rules.

Naturally in these systems – with certain technical solutions – "closed circuit" networks can be formed and by using these necessary communication channels can be created in a secure manner with the expected standards and quality; there are other, alternative solutions to meet communication requirements, [2] but creating a primary platform became essential to ensure the conditions of emergency communication. Therefore, there was a decree issued to build up a countrywide system which is suitable for both the communication inside the organisations and – if necessary – between the organisations.

The UDRS Government Commissioner of the Prime Minister's Office signed the contract with the winner T-Mobile Hungary Corporation – Hungarian Telecom consortium at the end of 2005. It states that the consortium constructs the countrywide system from its own resources and would ensure its operation for 10 years.

UDRS is a closed circuit radio communication system at a high service which has been fully operational since the trial operation, 1 February 2007. The radio system, which is operating according to the standards of the European Telecommunications Standards Institute, digital, trunked, created for government purposes and corresponding to the Schengen criteria given by the European Union, can be made capable of cooperating with the standby radio systems of other EU member states. UDRS terminals, hand terminals, fix installed versions, the car-based mobile radio versions or the aircraft-based mobile radio versions were available pro rata according to the contract, at the same time as the network. [3]

Figure 1. UDRS terminals (Source: www.ativizig.hu/projektek/keop/keop1103f2.aspx [16.09.2017.])

Three years before the operation contract was due to expire, the radio telecommunication system was owned by the state and the reason of this was the intention to integrate it in the telecommunication service providers of the state. According to this, by the repeal of the Government Regulation 109/2007. (V.15.) about the unified digital radio telecommunication system, the government-purpose networks 346/2010. (XII. 28.) government regulation has decreed about the specific rules of the unified digital radio telecommunication systems. According to the regulation the users are including, not limited to the law enforcement agencies, the disaster management organisations, the Hungarian Defence Forces, the National Ambulance Service, the National Water Directorate-General, the

National Atomic Emergency Agency, the National Media and Communications Authority and the National Tax and Customs Office. [4]

UDRS Services

UDRS is based on TETRA technology (Figure 2.) which is a cellular mobile telecommunications system with selective and group communication speech and data services. While in case of a disaster the public mobile telephone networks may become overwhelmed for the public, the UDRS system, due to the independent TETRA network provides a stable communication within the supply area helping the continuous cooperation of the public safety organisations. The groups of UDRS users share a common infrastructure; however, each organisation is able to form and use its own network structure independently of the others, without interfering with each other (organisations, speaking groups, permissions). This solution is called VPN, Virtual Private Network. TETRA technology allows to form a small or a large network or even an infrastructure covering the whole country, within which the virtual networks can be connected in any way and any time.

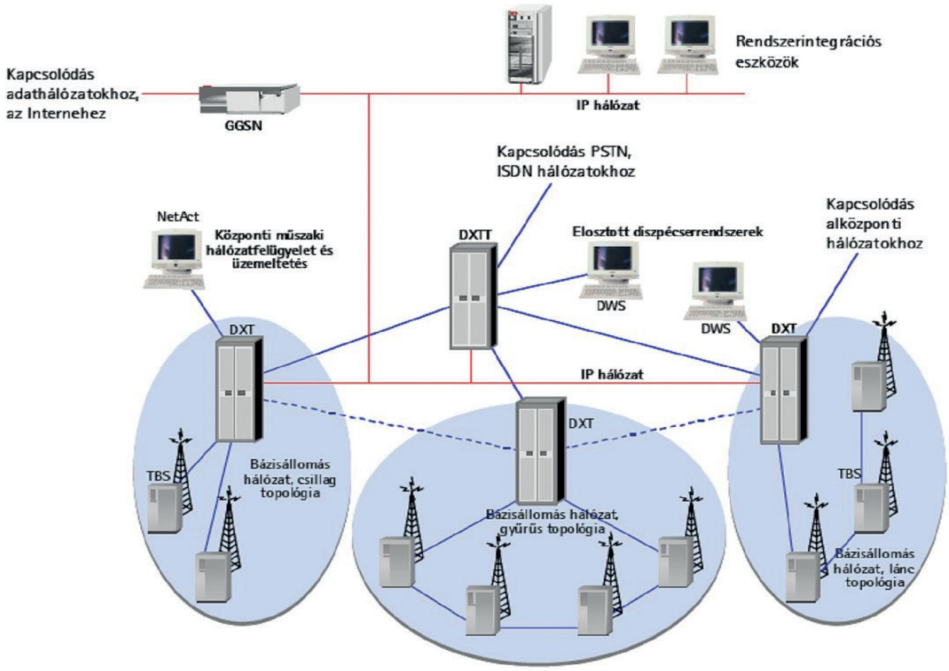


Figure 2. The architecture and network elements of TETRA network [6]

In each standby organisation the VPN manager performs the organisational hierarchy within VPNs, the group training, handling the permissions, the managing of the features of the appliances, the creating conversation groups but they cannot access other VPN's data. Conversation groups can be pre-programmed in the appliances or temporarily formed according to the requirements. In the latter case the system sends the configuration to the affected terminals through radio waves. Forming such groups this way, takes only a few minutes. Managing by the central dispatcher makes it possible – depending on the nature of the calls – to monitor the communication of the police, the army, the ambulance, the fire brigade or the public safety units of the disaster management, or to create mixed work groups.

As a matter of fact, while UDRS is working, it provides connections on request among the deployment staff on the spot, the commanders and the dispatchers.

For the operation of the system the followings are needed: base station transceivers to provide connection, switching centres to handle calls, data bases to identify users, network surveillance centre for monitoring and controlling the network and gates to ensure the connection to other telecommunication networks. As a cell mobile telephone network, the TETRA system supports within cross-organisational communication. The appliances do not work isolated, all of them know the location of the neighbouring stations and in case of a cell switching they apply to another station. [2: 25–26] By 2017 the entire system in Hungary has operated with more than 200 base stations and 4 switching centres which can be found in Budapest, Székesfehérvár, Szolnok and Kecskemét.

One part of the UDRS services is the speaking-type services. Communication can be achieved by a pre-defined relationship within the traffic group or by the direct connection of two subscribers. UDRS can be connected to other closed circuit or public networks via the interconnected PBX, as well as emergency calls. In normal network operation the connection is made with the help of the switching centres and base stations. Each base station is connected to the TETRA network control centre. In the absence of network coverage, the appliances are able to communicate with each other directly. This is the so-called DMO mode; after selecting the channel the appliances can directly communicate with each other in the usual way within their range. The range of a hand terminal is about 1 km depending on the terrain, the weather and the electromagnetic environment, the range of a fix installed or a built-in appliance in a vehicle is 5–10 km.

Other services include data transfer services such as short data messages or the group of pre-defined messages.

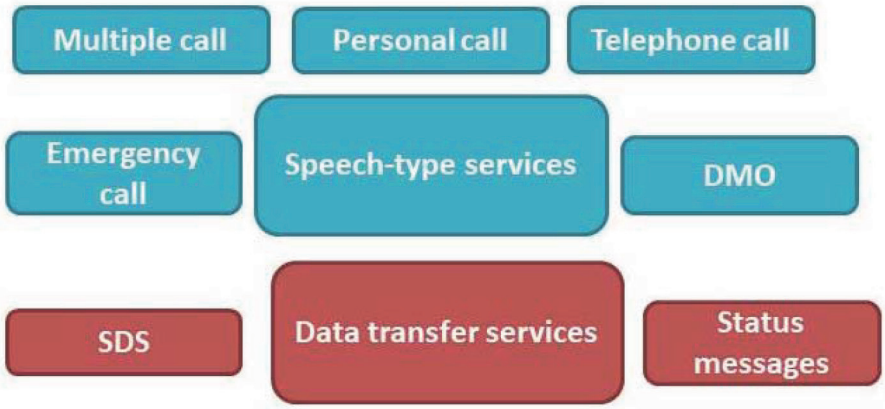


Figure 3. UDRS services [Chart compiled by the author.]

Apart from the standard network mode and DMO, among the special services of UDRS, DMO repeater can also be found, which is a mobile radio capable of functioning as a repeater station allowing remote devices to communicate with each other in uncovered areas.

The so-called gateway serves as an extension of the covered area picking the DMO users into the system. Activating the island mode is a solution if one or more base stations are disconnected from the system, meanwhile in their area the system keeps on providing the possibility of the connection.

If necessary, to reduce supply problems, mobile base stations can also be connected to the system. Thus a wide range of services provide the most suitable communication form for the needs, so that the possible connection is available even in extreme cases, the system can function properly and the effective flow of information can occur between the organisations and the individuals.

Regarding safety, unlike previous networks, UDRS can completely ensure closed communications between users. The system prevents the earlier experienced unauthorised access, wire-tapping, illegal use of information and data. [5]

The Practical Experience of the Operation of UDRS

When delivering the UDRS, the system met the quantitative and qualitative requirements that were defined during the design but there have been significant changes in the

operation and management of the using public safety organisations and TETRA technology progress over the past decade, which requires further expansion of the system. With the modernization of switching centres, the receiving traffic capacity is increasing, enabling the integration of new base stations. [6] The aim of the expansion is to improve the coverage of the UDRS network in Hungary and to improve traffic capacity according to user needs. Network coverage can be increased by installing new base stations. During the installation, the terrain conditions, landmarks, legal and other regulations must be considered. When installing base stations, the propagation characteristics of radio frequency waves should be taken into account when determining their position. In addition to optical visibility, the status of the so-called Flesnel zones should be calculated. Complex geospatial systems are used to carefully design and optimize settlement locations. Uncovered, service-accessed "shaded" areas can be plugged into the system via two-station repeater stations.

I would like to illustrate the problem through the example of Zala county, whose terrain conditions are varied, mostly hilly, wavy surface areas. The landscape of the county is basically determined by two regions, the Keszthely Mountains and the Zala hills. Zala County belongs to the Székesfehérvár switching centre for UDRS and currently operates 9 base stations. According to the needs of county-level users, more base stations would be needed, as environmental conditions prevent access to services in many areas. There was also a problem with the establishment of a public mobile phone network (GSM) to determine the location of the base stations, and the use of VHF radio systems used by the disaster management also had a number of problems due to the terrain conditions. At the county level, primarily the use of standard network mode, group communication service is mandatory. However, due to the aforementioned reception problems, in many cases, the devices need to be switched to a DMO mode or to widen the distances in both cases repeater stations are necessary. In larger cities such as Zalaegerszeg, the signalling problem is less common, but settlements such as Zalakaros or other small settlements may be affected on the whole area by the problem. During the 10 years of existence of the system, based on the experience of the users, the Zala County Disaster Management Directorate has an accurate database of uncovered areas (Table 1). In future designs, the data stored there may provide a good basis for defining the proper installation site for new base stations.

Table 1. UDRS coverage problems in Zala County [Table compiled by the author.]

Office	Settlement	Description	Mobile	Hand
Zalaegerszeg	Söjtör	Petőfi street	–	–
	Pusztaszentlászló	Kossuth street	–	–

Office	Settlement	Description	Mobile	Hand
	Zalaegerszeg	Bypassing section of Road 74 in the branching area of Nagypál	OK	–
	Zalaegerszeg	Bands at Csács Botanic Garden, Road 76	OK	–
	Szentpéterfölde	On the whole territory of the settlement	–	–
Nagykanizsa				
	Zalakaros	On the whole territory of the settlement	–	–
	Zalamerenye	On the whole territory of the settlement	–	–
	Zalaszabar	On the whole territory of the settlement	–	–
	Valkonya	On the whole territory of the settlement	–	–
	Rinyác	On the whole territory of the settlement	–	–

The promised enlargements, however, were lagging behind, due to financial problems. Still, it is a fact that, since 2015, the start of the migration crisis, the base station installation in the border areas has been given priority. Another major problem is that, although the system has many additional functions compared with previous VHF systems, due to strict county user regulations, they are still unused up to now.

On the whole, however, the development projects have made significant changes in the years 2014–2015 compared to 2007. The capacity of the network has increased and the coverage has improved considerably, especially along the Schengen border. Since the introduction of the system, around two hundred base stations have risen to around 300 at national level. At present, the rate of the national coverage of the car-based mobile radios is up to 99.2%, while the handheld radios used outdoors increased to 88.0%. [7]

Summary

The complexity of organizational and task system management of emergencies caused by disasters requires the establishment of communication systems to facilitate coordination. When building a communications system, the necessary periodic maintenance, user needs, organizational structure, and technology changes have to be considered. 21st century technology developments provide the right technical background to improve existing functions to enable these systems to function effectively in the future. The UDRS

network has undergone more technical upgrades over the past 10 years and has an expanded capacity, but as a result, it has not necessarily evolved in parallel with user needs.

In the future, remarks of the users of the system should be considerably more taken into account, as developments taking practical experience into account can maximally further increase the system's resistance, applicability, reliability and provide adequate infrastructure to allow users to access the network services as much as possible without interfering with each other.

Bibliography

[1] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény.

[2] Németh A.: *A mobil szolgáltatók hálózatainak felhasználása, fejlesztési lehetőségei és alternatív megoldások a katasztrófavédelmi kommunikáció területén.* Doktori (PhD) értekezés, Budapest, 2007. http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2008/nemeth_andras.pdf (16.09.2017.)

[3] EDR, www.frekvencia.hu/lexikon/e/edr.htm (16. 09. 2017.)

[4] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról.

[5] Kuris Z.: Az Egységes Digitális Távközlő Rendszer (EDR) alkalmazásának lehetőségei a rendészeti szerveknél. *Hadmérnök*, 5. évf. 2. szám, 2010. http://hadmernok.hu/2010_2_kuris.pdf (16.09.2017.)

[6] Egységes Digitális Rádiótávközlő rendszer (EDR) fejlesztése. http://kifu.gov.hu/kifu/hu/projektek/projektekleirasa/edr (16.09.2017.)

[7] Lezárult az EDR projekt megvalósítása. 2015. http://hirlevel.egov.hu/2015/09/09/lezarult-az-edr-projekt-megvalositasa/ (16. 09. 2017.)

Az Egységes Digitális Távközlő Rendszer (EDR) szerepe a katasztrófakezelésben

Fatime Balog

Az egyre gyakoribb és növekvő intenzitással jelentkező természeti és civilizációs eredetű katasztrófák az elmúlt évtizedekben újabb és újabb kihívások elé állították az elhárításba bevont beavatkozó szervezeteket. A korábban használt kommunikációs rendszereik már nem tudták kielégíteni a megnövekedett információs igényeket, ezért egy olyan megoldás bevezetése vált szükségessé, amely hatékonyan képes támogatni a készenléti szervezeteket az együttműködés során. Ez a megoldás az Egységes Digitális Távközlő Rendszer (EDR) kiépítésével és használatba vételével valósult meg. A közlemény célja, hogy bemutassa, hogy ez a TETRA-alapú hálózati struktúra mennyire volt eredményes a gyakorlatban a katasztrófák kezelése során az elmúlt évtizedben.
Kulcsszavak: EDR, TETRA, katasztrófahelyzet, veszélyhelyzeti hírközlés, katasztrófavédelmi kommunikáció