HADMÉRNÖK

Kiemelt közlemények

17. évf. (2022)
3. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9–11.
Postacím: 1581 Budapest, Pf. 15.
„A" épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000/29-289/ Fax: +36-1-432-9025
E-mail: hadmernok@uni-nke.hu
Web: https://folyoirat.ludovika.hu/index.php/hadmernok

Kiadó
Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes

Tartalom

Fórum

HADMÉRNÖK
HADITECHNIKA
17. évfolyam (2022) 3. szám 5–34.
DOI: 10.32567/hm.2022.3.1

Sándor Béres,[1] Árpád Kovács[2]

Quality Requirements for Front and Rear Support in Relation to the Precision of a Bolt Action, Big Calibre Precision Rifle

The aim of our study was to identify which support conditions result in producing the best accuracy with a bolt action, large calibre firearm, even over long distances. Precision is the feature that shows how closely impact points are grouped relative to each other.[3] According to Litz, precision is primarily determined by non-deterministic coefficients. He also states that the choice of the right equipment is primarily aimed at reducing the uncertainties of the shooter as much as possible. He says: "The challenge is if the shooter wants to use the same equipment for different purposes, because then the shooter has to make compromises."

In our study, a total of 11 different front and rear support combinations were tested. For each method, we varied weapon support strategies and surfaces. We fired five shots with each method and investigated the precision, weapon displacement characteristics, and the group of shots as a putative determinant of precision. The data obtained showed significant variation in the precision of each method. There was also a significant difference in the values of the recoil length and the post-firing backward slide of the shot. The rear support was a combination of a rice bag and a gripped monopod, or a rear eared shooting bag. In terms of retention, both sliding and controlled handling were effective as compared with a pinched grip.

Keywords: **precision shooting, long-range shooting, precision, bolt action rifle, support methods**

[1] Hungarian University of Sports Science, Department of Athletics, e-mail: odd0@protonmail.com
[2] Hungarian University of Agricultural and Life Sciences, Institute for Business Regulation and Information Management, Department of Information Management, e-mail: kovacs.arpad.endre@gmail.com
[3] Bryan Litz: Scope Tracking: Tall Target Test. Applied Ballistics with Bryan Litz. *YouTube,* 12 June 2015.

1. Literature review

The main aim of group-shot shooting in F-Class competitions is precision, i.e. to achieve the narrowest possible groups of hits. In this type of competition, shooters shoot in prone position, usually at distances of 300 m, 600 m and 1,000 m. As Simonyi writes: "In this style, excellent individual shooting technique, excellent wind-reading ability, good quality rifle, ammunition and scope are very important."[4] Of course, it is also important that the group is as close as possible to the centre of the target area. In addition to the above said, precision is a basic requirement for tactical sniping competitions. These competitions, however, lay down rules for the use of support equipment.

To support their weapons, shooters can use front, rear and centre support variations. Single-point support is not very effective for high accuracy, and therefore, the methods of fixation used on tripods are not utilised in such competitions and will thus not be addressed in this study. In most competitions, the use of two-point support is a permitted method, with bipods at the front and shooting bags at the rear being the most common. In some competitions, the use of monopods at the rear is allowed, but this may result in a reclassification. Precision is part of the so-called "monopod" PRS *(Precision Rifle Series)* competitions, but not as much as in the F-Class competition series. PRS competitions are, by their nature, more liberal in their approach to support, as the aim in this series is primarily to hit metal targets in different time frames, positions and from various objects at known and unknown distances. Competitors may use two or one support, gun straps, shooting bags, etc. However, precision is not as important in PRS competitions. Instead, the ability to read the elements (mainly the wind) or the speed and stability of the shooting position are more crucial.

2. Methods

2.1. Protocol

In this study, we will look at the most common double (front and rear) supports used in most competition situations. As the main objective is to understand the mechanism of operation and features of these devices, we will try to minimise all other influencing factors. There are two main groups of factors to be considered that can significantly influence the final result. The *weather factors* and the so-called shooting errors *that the shooter can make*.

Of all the weather factors, *wind has* the greatest impact on the projectile. This effect was minimised by conducting the tests at a wind-protected firing range. Additionally,

[4] Ottó Simonyi: *A mesterlövész. Vadászatról és sportlövészetről* [The Sniper. About Hunting and Sport Shooting]. Vác, Cyberkinetic Kft., 2021.

we tried to minimise shooting error by utilising an experienced shooter, who worked out each shot and executed the shot to the best of his or her ability. During the execution, the shooter payed great attention to the best possible "natural point of aim", i.e. where the crosshairs of the scope end up when the shooter is in a relaxed state in his/her shooting position. It is the place where the crosshairs will rest for a short period in his/her natural respiratory pause.[5] In general, this is an important firing rule because if the shooter applies force to the barrel or grip with the shoulder or the palm of the firing hand in order to keep the centre of the crosshairs on the target, the barrel of the gun will be off the target at the moment of firing and the bullet will no longer be pointing at the target during its stay in the barrel and at the moment of exit. The other important criterion was the firing process established by the shooter. In the firing process, the shooter pressed the two-stage trigger (having a resistance of ~0.6–0.7 kg) which was pulled in a gentle manner, with a long forward stroke, until the action was smooth and even. The accuracy of the firing process was taken high level by the shooter using a pre-test, post-test method of checking that the crosshairs did not move off target during dry firing.

To ensure the most harmonious and accurate interaction between ammunition and barrel, we used loaded ammunition (with carefully selected and grouped components) rather than factory ammunition for the greatest consistency as described in the literature. The primary parameter for this consistency was to minimise muzzle velocity dispersion and optimise tube vibration harmony. Therefore, a precisely measured, bullet seating depth, the so-called "jam point", i.e. the rise point where the projectile touches the rifling, was set at minus 0.002 inch, or 0.05 mm, of the total L6 ammunition length (by C.I.P. regulations).[6] The Hornady 147 grains (9.52 g) projectile (2.64 inch – 6.71 mm diameter), which has one of the highest ballistic coefficients (BC: G7 = 0.697) in its category, was designed to achieve the factory-specified velocity at 15 °C (822 m/s). The projectiles were grouped by weight in hundredths of milligrains and the brasses were categorised by H_2O, grain cubic content for maximum accuracy. For consistent extraction force, we used "fire-formed" Hornady Creedmoor brasses already fired, i.e. formed to the chamber, the case neck was *annealed* by an induction annealer machine, the length was adjusted (trimmed to uniformity), and the neck was lined. The primer hole was cleaned, standardised, and *large primary* ignition was applied using CCI 250 *boxer* primers.

In the evaluation, we sought economy, accuracy and applicability. Using predefined and pre-set support variations, we shoot 5–5 bullets at circular paper targets. Fewer shots than this, are not suitable for determining accuracy.[7]

[5] See www.longrangeshooting.org/articles/natural-point-of-aim

[6] Gunmakers' Company and The Guardians of the Birmingham Proof House: *Rules, Regulations and Scales Applicable to the Proof of Small Arms.* London, 2006.

[7] RocketmanOU: *Statistics, Shooting and the Myth of the Three Shot Group.* 2020.

2.2. Target cards, precision assessment

The main objective was to assess precision, so we did not focus on ballistic deviations. We used targets with a white centre made by Swiss Arms, in the classic size of 14 × 14 cm, compatible with a classic catcher. These targets are made of thicker paper for better stability in the catcher. The diameter of the white centre is 17 mm. We fired with a predefined elevation value, set by loading and fixing the tactical turrets of the scopes. The scope's tactical turret "ladder test" *(Tall Target Test),*[8] which is used to verify the accuracy of the clicks or elevation showed that the accuracy of the 300 m ballistic elevation of the turret was 100%.

Aiming at the centre of the circular target, the main objective was "group shooting". The sizes of the groups were measured in "Minutes of Angle" or MOA, the most commonly used angle measuring unit in precision shooting. The so-called "Extreme Spread" (ES) value evaluation method, which calculates precision based on the distance between the farthest hits of a given group of hits, was disregarded[9] although this evaluation is also presented, as it is the most commonly used evaluation method in shooting circles.

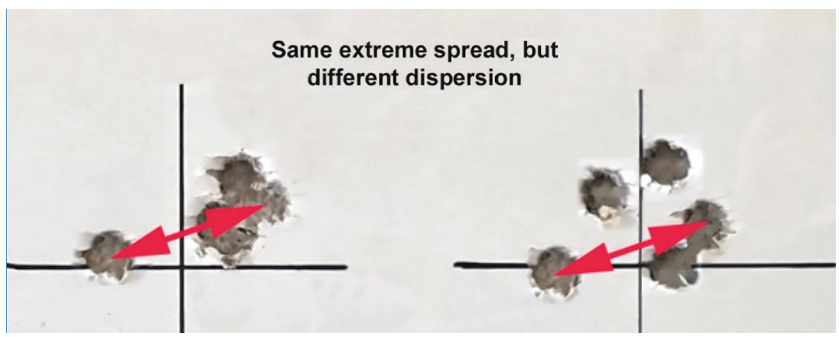


Figure 1: We have disregarded the so-called "Extreme Spread" (ES) value evaluation method, which calculates precision based on the distance between the furthest hits in a given hit group
Source: Compiled by the author.

A valid evaluation method for precision is the "Mean Radius" or "Average to Centre" method, which not only calculates the accuracy based on the distance between two points, but also uses the information contained in all the points in the group to determine the accuracy of the rifle, ammunition or support used. The average radius gives the possibility to determine the quality of dispersion with fewer shots.[10]

[8] Litz (2015): op. cit.
[9] Cal Zant: Works Cited for Statistics for Shooters Articles. *Precision Rifle Blog,* 2020.
[10] Guns and Ammo: *Long Range Shooting: Understanding Extreme Spread and Standard Deviation.* 05 September 2018.

2.3. Post-shot target assessment

An effective way to assess possible shooting errors, as well as the supports and surfaces is to analyse the evaluation shot after shot.

The two components of this are the direction of the bounce of the crosshair's centre and the distance (position) of its impact relative to the centre of the target.

After each shot, the direction and distance (described in the study as the displacement "force") were recorded. The direction was given by marking whole clock directions, and the displacement force was defined on a scale of 0–20 where one unit represented an angular displacement of approximately 0.2 MOA (~0.06 mil), which is a displacement of 1.75 cm relative to the midpoint over the 300 m distance.

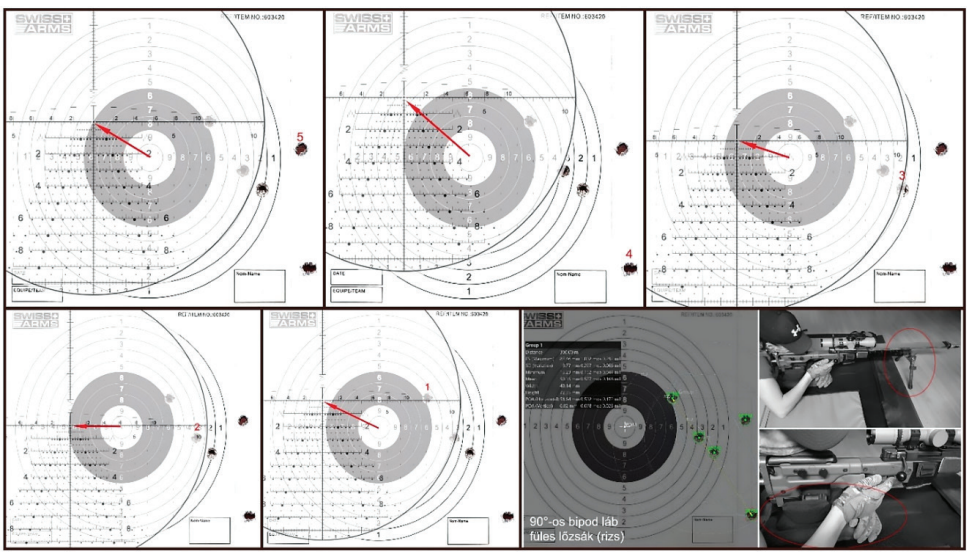


Figure 2: Evolution of the shot image after each shot in relation with the centre of the crosshairs and the centre of the target area – calculation method (1 unit of displacement = 1.75 cm at 300 m, or 0.2 MOA, or ~0.06 mil)

Note: The size of the crosshairs is only an illustration, slightly reduced compared to the size of the target.

Source: Compiled by the author.

2.4. Tools used

The study focuses on the use of a single calibre, the 6.5 Creedmoor. With other calibres the recoil force may be different. The recoil forces are accurately given by the Gordon Reloading Tool (GRT) in Joules for ammunition loaded with the given components. In our case, the recoil energy was 7 Joules. The weight of the weapon was 8 kg.

The first support was an Atlas style LRA Light Tactical Bipod. Dimensions: leg length: 21–29 cm, support span: 30–37.5 cm, tilt angles: 0°, 22°, 45°, 90°, weight: 0.8 kg.

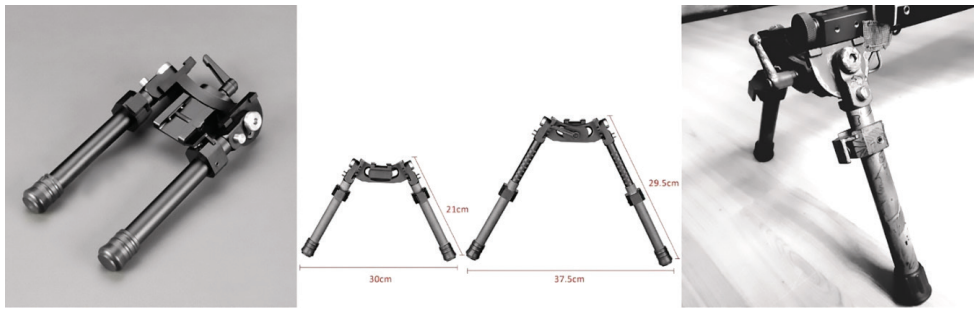


Figure 3: Atlas style LRA Light Tactical Bipod front support – hard rubber foot end plug (dimensions: leg length: 21–29cm, support span: 30–37.5cm, tilt angles: 0°, 22°, 45°, 90°, weight: 0.8kg)
Source: Compiled by the author.

The tools used for the back support included: rice-filled standard shooting bag (dimensions: 15 × 15 × 5 cm, weight: 0.5 kg), PET granulate filled rear eared bag (dimensions: 18 × 11 × 11 cm, weight 1.25 kg), Accu-Shot Accuracy International AT Monopod BT57-QK, lifting height 7.5–10.5 cm.

Figure 4: Cser Industries rear ear bag (PET granulate filled), standard rice shooting bag, BT57-QK: Accu-Shot Accuracy International AT Monopod (from left to right)
Source: Compiled by the author.

The adjustable butt plate used in the study was an Accuracy International rubber butt end combined with a Canadian made 4-way-adjustable butt end bracket with original AI rubber butt plate.

Figure 5: Adjustable butt plate – Accuracy International rubber butt end and a 4-way-adjustable butt plate bracket from a Canadian manufacturer
Source: Compiled by the author.

The footage was recorded with a high-speed video camera at 960 frames per second in 1080p quality, triggered by motion detection software and stopped after 0.4 seconds. The camera used was the high performance camera of a Samsung 9 Plus phone. This recording speed allows for a time of 0.00104 s, which is suitable for recording the movement of the barrel while the bullet is in the bore.

Camera placement took into account a slight wide angle of view, which was corrected in software. Regardless of this, the camera was placed as far away from the barrel of the gun as possible, so that it was in the same place and at the same height. A reference frame with mm-precision scale was placed behind the barrel, fixed firmly so that it would not be displaced by the shock wave generated by the muzzle break. From the resulting images, we were able to determine the horizontal and vertical displacements to an accuracy of 0.5 mm.

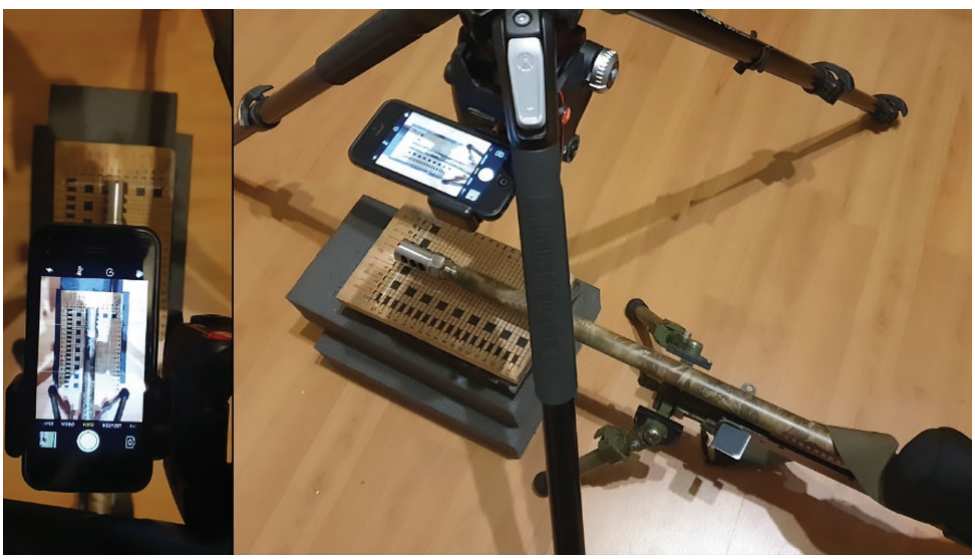


Figure 6: Measuring the recoil distance with a high-speed camera
Source: Compiled by the author.

For lateral displacements towards the barrel mouth or muzzle break, a camera with a vertically oriented downward field of view mounted on a tripod was placed with the aforementioned parameters and reference grid.

The projectile velocities were measured with a Magnetospeed magnetic projectile velocity meter, which was not mounted on the barrel but on the forestock, so as not to affect the barrel vibrations in the swinging barrel design. The system software of Magnetospeed software version number 3.0.3.

The shots were fired at 5 °C with 5 °C gunpowder.

The time of the projectile in the barrel at the above mentioned loading values – *Optimal Barrel Time (OBT)* was 1.3084 ms (0.001308s).

Table 1: The weapon system

Make of weapon	Accuracy International Arctic Warfare 2012 English made sniper rifle (England, Portsmouth)
Tube and calibre	Proof Barrel, 6.5 Creedmoor, 24" inch long, for Accuracy International
Chamber	Factory CIP Chamber
Riflescope	Schmidt & Bender, Ultra Short 5–20 × 50, Tremor 2 reticle
Trigger force	7N (0.7kg)
Ammunition used	loaded, jam point –0.002 inch long L6 value, fire formed, standardised Hornady case, Hornady 147 grn ELD Match bullet
Applied gunpowder	Vihtavouri 555, 42.2 grn
Applied primers	CCI 250 large

Source: Compiled by the author.

Figure 7: Accuracy International Arctic Warfare 2012 English sniper rifle (England, Portsmouth)
Source: Compiled by the author.

Figure 8: Hornady 147grn ELD Match projectile
Source: https://proshooting.hu/termekkepek/800/hornady-eld-match-65-mm-147-gr-lovedek15430990370.jpg

Table 2: Environmental conditions

Distance	300 m
Objective	circular paper target
Target area zones	target area diameter 17 mm, target sphere 0.05 mil (15 mm with 15 mm masking)
Wind	0 m/s
Air pressure	1001 hPa
Moisture content	52%
Firing direction	131 degrees
Altitude above sea level	129 m

Source: Compiled by the author.

Theoretical values: The theoretical data was obtained using the Gordon Reloading Tool (Patreon Nightly ver. 18.55) software for loading ammunition.

Shooting conditions, supports, surfaces used: The support, gun grip and recoil damping parameters that were varied as a part of the experimental methods were divided into the following categories:

Support forms

- Front supports
  - conventional bipod with rubber bung feet with variable foot angles
  - rice filled barricade bag
- Rear supports
  - a rice filled standard rear bag
  - plastic (PET) granulate filled rear eared bag
  - tilting monopod (forward tilting system)
- Weapon holding
  - gripped
  - controlled
  - permissive (way giving)
- Supporting base surface
  - hard
  - absorbing
- Recoil absorption
  - compensated with muzzle break
  - non-compensated

Detailed description

- Methods of weapon holding
  - In the so-called "gripped" method of weapon holding, the shooter pulls the weapon into the shoulder and applies pressure through the butt end. The grip is held either by a full grip (with the thumb wrapped around it) or by extending the thumb forward on the side of the gun, with the other fingers holding the grip firmly. The cheekbone rests on the cheekpiece, supporting all or part of the weight of the head, ensuring a consistent cheekbone

position that returns to the same position, creating the identity of the sighting in the scope. The recoil exerts an immediate or near-instant force on the shoulder, stopping the glide.
  - The case of "controlled" gun grip is similar to the gripped method, but in this case the shooter allows the gun to move slightly, but keeps it under control with the grip hand. The thumb is extended forward above the trigger guard to support and "control" the pre-firing position of the weapon as well as the glide during recoil. The shoulder is not pressed firmly against the butt.
  - The "permissive" handling of weapons. In this method, the shooter does not apply any pressure to the butt end of the rifle, thus ensures vibration-free aiming and the possibility of the weapon sliding backwards. The cheekbone is not pressed against the adjustable cheekpiece, which also reduces any vibration that may occur during aiming, but reduces the possibility of consistent head aligning and target view development. With this method, a complete "clear" sight picture ensures targeting identity. The pistol grip is not tightly held.
- Methods used for the support surface of the weapon
  - *Support on hard surfaces.* In this study, the bipod was supported on concrete for hard surfaces. In one case, the monopod was used as a back support on Orca fabric placed on concrete for its retained shape, which was treated as a solid surface given the thinness of the material. The solid wood base was not used in the study.
  - *Support on a vibration absorbing surface.* In this study, vibration absorbing surfaces were used under the front support in two cases. In the first test, a 4 kg Cser Barricade Bag filled with plastic PET granules was utilised. In the second test, a 12 × 6 × 1.5 cm bag filled with sand integrated into a 30 × 60 × 3 cm recortan sheet was placed under the bipod feet (Figure 9). In one rear support test, as mentioned in Figure 2, no vibration absorbing support was used. The rear bag was filled with plastic PET granules and the conventional bag was filled with rice.

Figure 9: Bipod feet placed on sand bags integrated in a recortan sheet
Source: Compiled by the author.

- Gun recoil absorption methods
  - With muzzle break. The recoil damping was solved with the Gen 2 Little B* Self Timing Muzzle Break (Figure 10) developed by American Precision Arms, which provides world-leading damping and target return for the calibre.[11] According to Simonyi, a muzzle brake is suitable for a given calibre if it has a positive effect on the gun's rate of displacement and the amount of projectile dispersion. He describes the advantages of using a muzzle brake as "useful because it reduces recoil, improves the scatter pattern and makes the hit observable in the scope".[12]
  - Without muzzle break.
  - A tilt-absorbed backward-sliding force, whereby the bipod moves backward around the anchor points of the legs as axes of the weapon system. This tilt is bipod dependent. Bipod legs left loose will tilt or "slacken" during the recoil while legs turned with tight tolerances will allow little tilt and will compensate by sliding the legs. Bipod legs tilted at 90° are more likely to compensate by tipping, due to the longer lever arm, than bipod legs tilted at 45°. 45° tilted bipod legs compensate for both pitching and sliding. Also by tilting, the recoil force is reduced for rear supports by angled, hand-held monopods. These have the advantage of holding the target quickly, but the tilting makes it more likely that the end of the barrel will be off target during the shot while the projectile is in the barrel.
  - Slip-absorbed forces are released by the recoil of the weapon system, giving the barrel a better chance of staying level. Such methods include the sled-solved base of F-Class bipods, or the heavier F-Class rest, which allow the front part of the stock to slide in the U shape top of the rest, resulting in frontal upsets. As for the rear supports, the various bunny-ear rear bags and brackets, of differing effects depending on the design, serve the same purpose. Their efficiency can be increased by using the so-called "bumper brackets". The effectiveness of these devices can be increased by the use of "bag riders", which are tubes or rails mounted on the bottom of the gun butt and which fit precisely into the cavity provided by the eared bag, thus facilitating the retention of the rider's position. The AIAW system allows the folded, fixed monopod (Accu-Shot Accuracy International BT57-QK) to function as a "bag rider" when using an eared bag (Figure 2).

Figure 10: Gen 2 Little B Self Timing Muzzle Break developed by American Precision Arms*
Source: www.americanprecisionarms.com/products/gen-2-little-bastard-muzzle-brake

[11] Cal Zant: Muzzle Brake: Summary of Field Test Results. *Precision Rifle Blog,* 21 August 2015.
[12] Simonyi (2021): op. cit.

Combined methods used

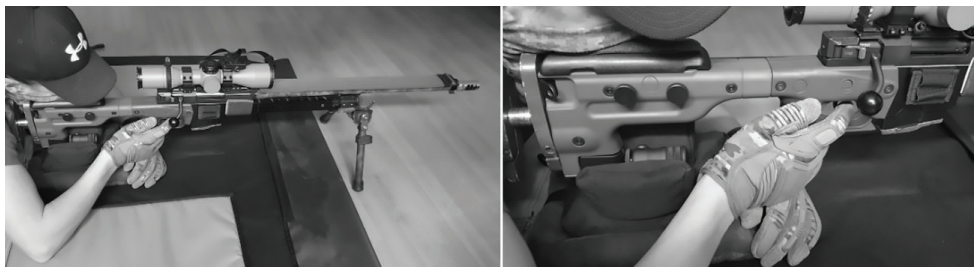


Figure 11: Method No. 1 – Front support (standard tactical bipod, 90°, resting on concrete surface – hard rubber foot end plug). Rear support (horizontal monopod resting on a tabbed rice bag – passive, support hand for gripping and regulating the eared rearbag).
Source: Compiled by the author.

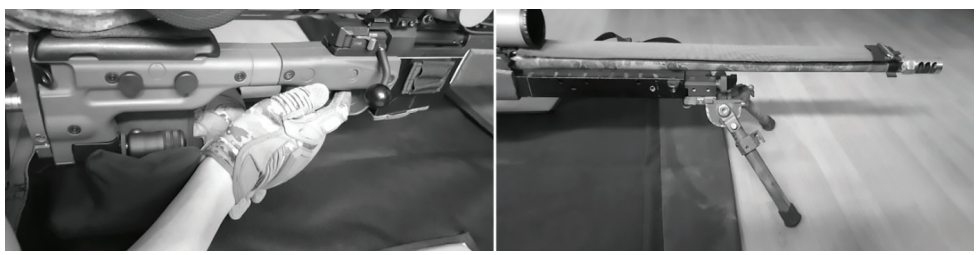


Figure 12: Methods No. 2 – No. 3 – The second and third shooting positions and support conditions are identical. Two control strategies. No. 2: Gun left in slide (shooter leaves recoil, does not support against the shoulder). No. 3: Controlled supported weapon (shooter, with the butt slightly rotated and elevated, adjusted to his/her shoulder, supports the recoil with his/her shoulder, tracing the recoil, transforming its energy to his/her shoulder). Front support (standard tactical bipod 45° foot, resting on concrete surface – hard rubber leg end plug). Rear support (horizontal monopod resting on an eared bag – support adjusted by hand).
Source: Compiled by the author.

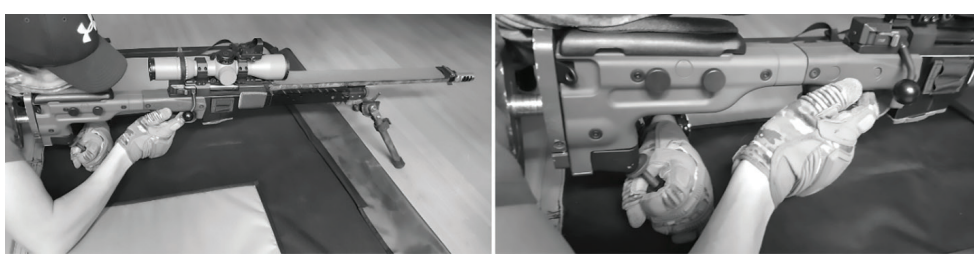


Figure 13: Method No. 4 – Front support (standard tactical bipod, 45° leg angle, resting on concrete surface – hard rubber leg end plug). Rear support (tilted, passive support resting on wooden surface, manually gripped and controlled monopod – recoil force absorbed by tilting).
Source: Compiled by the author.

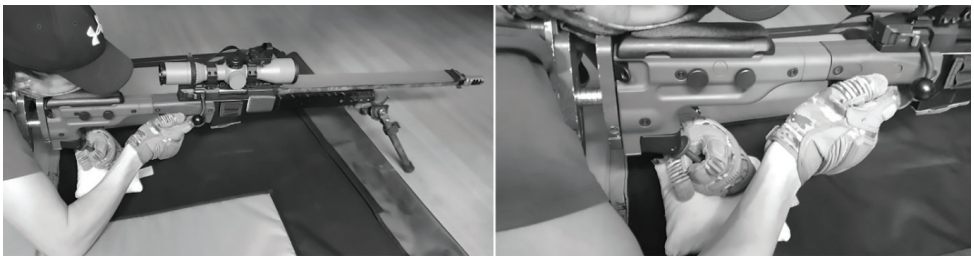


Figure 14: Method No. 5 – Front support (standard tactical bipod, 45° leg angle, resting on concrete surface – hard rubber leg end plug). Rear support (tilted, passive support resting on rice filled rear bag, manually gripped and controlled monopod – recoil force absorbed by tilting).
Source: Compiled by the author.

Figure 15: Method No. 6 – Front support (Barricade Bag [~4kg] filled with plastic granules from Cser Ind.). Rear support (eared bag).
Source: Compiled by the author.

Figure 16: Method No. 7 – Front support (standard tactical bipod, 45° leg angle, resting on concrete surface – hard rubber leg end plug). Rear support (rice filled standard rear bag).
Source: Compiled by the author.

Figure 17: Method No. 8 – Without muzzle break. Front support (standard tactical bipod, 45° leg angle resting on concrete surface – hard rubber leg end plug). Rear support (tilted, passive support resting on a rice-filled rear eared bag, hand-controlled monopod).
Source: Compiled by the author.

Figure 18: Method No. 9 – Without muzzle break. Front support (standard tactical bipod, 45° leg angle, legs resting on sand-filled neoprene bags). Rear support (tilted, passive support resting on eared bag, hand-controlled monopod).
Source: Compiled by the author.

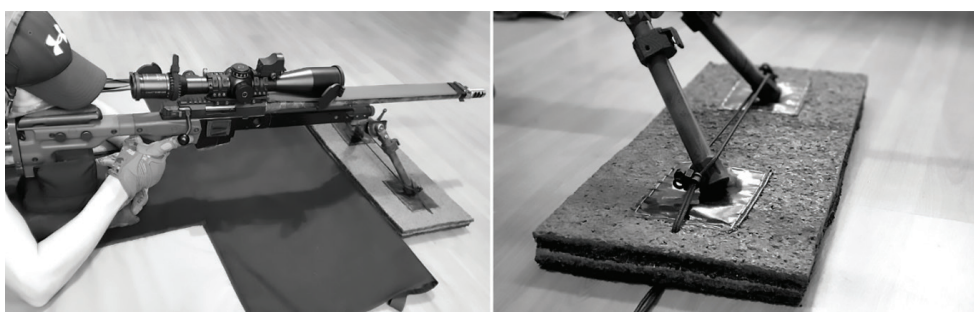


Figure 19: Methods No. 10 and No. 11 – The tenth and eleventh shooting positions and supporting conditions are identical. Two control strategies. No. 10: Gun left in slide (shooter leaves recoil, does not support against the shooter). No. 11: Controlled supported weapon (shooter, with the butt end slightly rotated and elevated, adjusted to his/her shoulder, supports the recoil with his/her shoulder, tracing the recoil, catching its energy with his/her shoulder). Front support (standard tactical bipod, 45° leg angle, feet cut and fitted into recortan base, resting on 2 cm deep sand pads). Rear support (rear eared bag).
Source: Compiled by the author.

Statistical procedures used: The results were analysed using Statistica 8.0 software.

Comparisons were made using one-sample T-tests and Pearson correlation. The probability coefficient was set at $p < 0.05$.

3. Hypothesis

1. We hypothesise that shots fired with one calibre using different supports and different gun grip methods will show significant variation in accuracy when fired by one shooter.
2. rom the methods chosen, those that give the most accurate spread patterns are those that ensure the smallest barrel movements in all directions during the time the projectile is in the barrel. We hypothesise that the support methods that best meet this criterion are those that absorb the recoil force by back-slip rather than by tilting.
3. We assume that the follow up view after the shot is a good indicator of accuracy. The shorter the distance of the jump from the target and the more uniform the direction, the smaller the spread of hits will be.
4. We hypothesise that the second most accurate results will be obtained by firing a bipod on a vibration absorbing surface, with the possibility of the bipod legs slipping during displacement.
5. It is assumed that the least accurate results are obtained by firing a bipod on solid ground with a tilting bipod.

4. Results

4.1. Evaluation of precision and accuracy

All tests resulted in two measurable parameters. First, the mean radius of group shots, which represented the *precision,* in other words the distance of the hits to each other, i.e. the spread. We also calculated the diameter of the resulting pattern for better clarity. This data is more important for the evaluation of the supports or the shooting errors. We also examined the ES, or extreme spread (MOA, [minutes of *angle*], degrees). This data measured the distance between the two hits furthest apart for a given image. This data set does not always characterise the group, since this data can include anomalies due to a single miss or a target hit that may be far from the shot group due to a defective projectile or charge or a change in bullet velocity. In the English literature, these anomalies are called a "flyer", which degrades the characteristics of the group, even though the shooter does not make a shooting error.[13]

The second measurement determined in this study is *accuracy,* which is the closeness of the average shot of the group to the target centre. This feature is

[13] Cal Zant: Works Cited for Statistics for Shooters Articles. *Precision Rifle Blog,* 2020.

characterised by two parameters. The first was the number of scores scored and the second was the distance (mm) from the target centre of the group.

Table 3: Determination of the precision by spread images, with applied supporting methods, using extreme spread ES, standard variations SD, Mean Radius MR, Mean Radius × 2 MR2, and extreme spread vs mean radius2× ES vs MR × 2 methods in MOA
*Note: *** best value, ** second best, * third best value*

No.	Description of methods	Front support style-tilting (b), sliding (cs)	Rear support style tilting (b), sliding (cs)	ES Extreme Spread	SD variation	Mean Radius	Mean Radius × 2	ES vs MR × 2
				(MOA)	(MOA)	(MOA)	(MOA)	(MOA)
1	90° bipod, ear bag	b	cs	1.002	0.227	0.294*	0.588*	0.41
2	45° bipod, ear bag, permissive handling	b/cs	cs	0.753**	0.178	0.302	0.604	0.146*
3	45° bipod, eared bag controlled	b/cs	cs	0.933	0.22	0.288**	0.576**	0.356
4	45° bipod, monopod resting on wooden surface	b/cs	b	0.924	0.127***	0.393	0.786	0.137***
5	45° bipod, monopod on rice bag	b/cs	b	0.697***	0.17*	0.252***	0.504***	0.193
6	barricade bag, ear bag	cs	cs	1.007	0.283	0.378	0.756	0.248
7	45° bipod, rice bag	b/cs	cs	1.134	0.313	*0.416*	0.832	0.301
8	45° bipod, without muzzle brake, eared bag	b/cs	cs	*1.329*	0.286	0.378	0.756	0.563
9	45° bipod on sand bag without muzzle brake, eared bag	b/cs	cs	1.183	0.278	0.322	0.644	0.538
10	45° bipod, recortan base, ear bag permissive holding	b/cs	cs	0.866	0.172	0.3	0.6	0.268
11	45° bipod, recortan base, ear bag, gripped holding	b/cs	cs	0.759*	0.158**	0.311	0.622	0.138**

Source: Compiled by the author.

According to the results, the support variation with the best effect on precision, based on Extreme Spread (ES) calculations, was a 45° bipod and monopod on standard rice bag support combination which resulted in a 0.697 MOA spread (Table 3). The second best support variation was the 45° bipod combined with an ear bag, with permissive handling (weapon left sliding [not shouldered]). This combination resulted in a slightly better ES value compared to the third best variation which consisted of the ear bag with gripped handling (weapon shouldered), combined with the 45° bipod on sandbags integrated into a recortan base. All three support variations had a 45° tilted leg bipod as the first elevation. The highest ES value was shown by the 45° bipod, no pipe mouth support variation with a value of 0.1329 MOA.

The way of measurement that best indicates precision[14] is the Mean Radius (MR) method. With this evaluation method, the best support variation was the 45° bipod combined with a monopod on rice bags which resulted in a spread of 0.252 MOA (Table 3). The second best support combination was a 45° bipod with an ear bag and controlled handling. The third best method, based on MR measurements, was a 90° bipod combined with an ear bag. The highest MR value was obtained using a 45° bipod, rice bag combination with a MOA value of 0.476.

4.2. Evaluation of the image displacement force, direction and back kick values

Table 4: Muzzle velocity (m/s), recoil value (mm), round score (points), view displacement (mil) and displacement direction (hr) data measured at the applied supports
*Note: *** minimum value, ** second minimum, * third minimum*

No.	Description of methods	Projectile muzzle velocity (m/s) avg., SD	Horizontal recoil value (mm) avg., SD	Avg. and SD of round scores (points)	View displacement rate (mil) avg., SD	View displacement directions (in hours) avg., SD
1	90° bipod, eared bag	810.4	29*	2.4	3.2***	9.7
		2.302	*4.796*	*2.608*	*0.447*	*0.671*
2	45° bipod, eared bag, permissive handling	813	26.2	5.8**	3.5*	10.9
		2.915	*3.768*	*2.280*	*0.500*	*0.652*
3	45° bipod, eared bag controlled	811.4	17.4	6.6***	3.8	11.9
		2.408	*0.548*	*2.702*	*0.758*	*0.894*
4	45° bipod, monopod resting on wooden surface	813.2	27	5.2*	8.2	12.2
		4.658	*2.449*	*2.049*	*1.789*	*0.447*
5	45° bipod, monopod on rice bag	810	21.2	5.8**	8.8	12.3
		1.871	*0.837*	*1.789*	*1.304*	*0.274*

[14] Cal Zant: Works Cited for Statistics for Shooters Articles. *Precision Rifle Blog,* 2020.

No.	Description of methods	Projectile muzzle velocity (m/s) avg., SD	Horizontal recoil value (mm) avg., SD	Avg. and SD of round scores (points)	View displacement rate (mil) avg., SD	View displacement directions (in hours) avg., SD
6	barricade bag, eared bag	815.2	12.75*	5	7.4	10.8
		2.950	*0.500*	*2.915*	*0.418*	*0.447*
7	45° bipod, rice bag	812.8	18.6	2	10.2	11.3
		3.421	*1.140*	*2.345*	*1.789*	*0.758*
8	45° bipod, without muzzle brake, eared bag	812.6	29.6**	5	12.5	10.7
		1.949	*3.130*	*3.742*	*3.317*	*2.683*
9	45° bipod on sand bag without muzzle brake, eared bag	812.2	32.2***	3	13.2	11.2
		3.701	*3.421*	*2.236*	*2.280*	*1.037*
10	45° bipod, recortan base, eared bag permissive holding	786	16.4	3.8	3.6	11
		4.528	*1.817*	*1.304*	*0.894*	*1.000*
11	45° bipod, recortan base, eared bag, gripped holding	788.4	14.2	4.2	3.4**	10.9
		5.128	*1.304*	*4.025*	*0.894*	*0.418*

Source: Compiled by the author.

4.3. Recoil values

The recoil value is mainly generated by the resistive force at the moment of firing, which depends on the weight of the rifle, on the bullet velocity, weight, friction force and gas pressure. The smaller this force, the less likely the end of the barrel is to jump off the target during the time the projectile is in the barrel, thus creating the possibility of a more accurate hit, with a well-defined ballistic calculation. The recoil force as a function of the accuracy of the hit is accompanied by the support conditions that actually "control" the recoil. The results obtained for the combination of support methods and methods to reduce recoil are shown in Figure 20.

The lowest recoil value, 12.6 mm, was obtained using a combination of barricade bag and ear bag. This value can be evaluated in relation to the extent to which the weapon system modulates in other directions during the recoil, which we determined by the position of the sight after the shot. Ultimately, the results of the shooting and the two parameters mentioned above can characterise the effectiveness of the support methods.

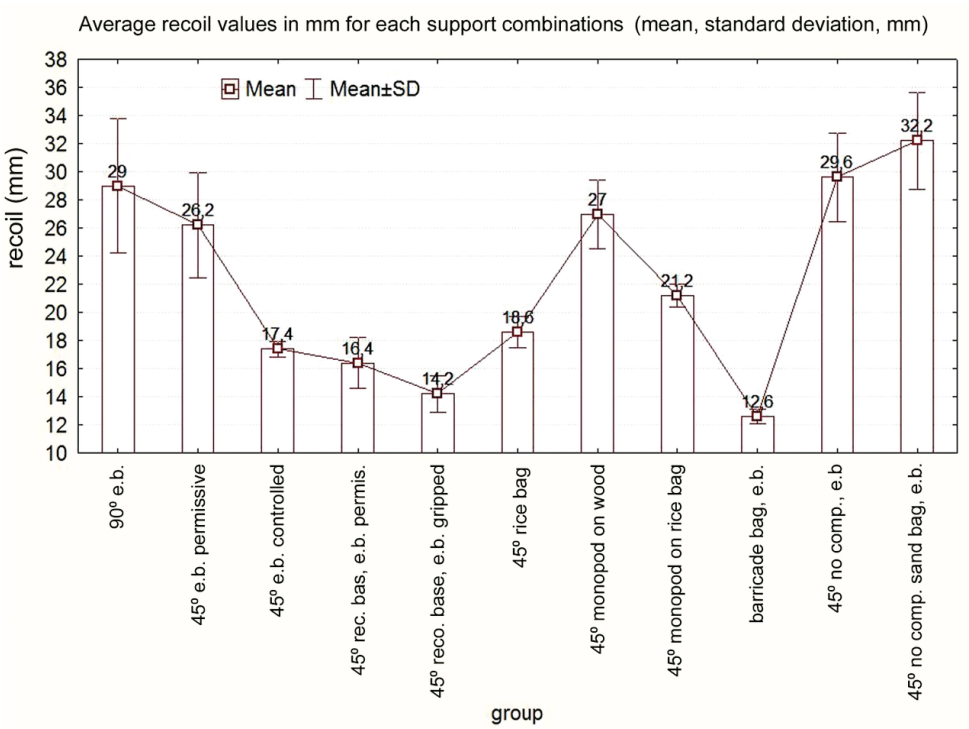


Figure 20: Average recoil values in mm for each support combination (mean, standard deviation, mm)
Source: Compiled by the author.

The mean of the total recoil values was 22.21 mm (N = 55, SD = 6.97), indicated by the red line in Figure 21. In terms of recoil, we can talk about support methods with recoil values below and above the average.

As expected, the two methods that did not use a muzzle break, the 90° bipod – ear bag combination and the 45° bipod – ear bag left in the slide combined with a monopod on a wooden surface, resulted in high backsliding. For the 90° bipod – ear bag combination, the possibility of the bipod being fixed under the barrel as an axis, as well as the relative height and the bipod moving backwards around the axis of rotation due to the larger lever of force, was also assumed. With the weapon left in the slide, the shoulder does not form an obstacle behind the backward moving weapon and a longer backward movement was expected. The rear support left on a wooden surface, movement around the axis of rotation of the monopod, and the slight sliding on the wooden surface all combined to cause the greater recoil. The slippage is eliminated when the monopod is placed on a rice bag, a change that caused a significant reduction in the recoil value ($t = 5.0104$, $p = 0.001039$).

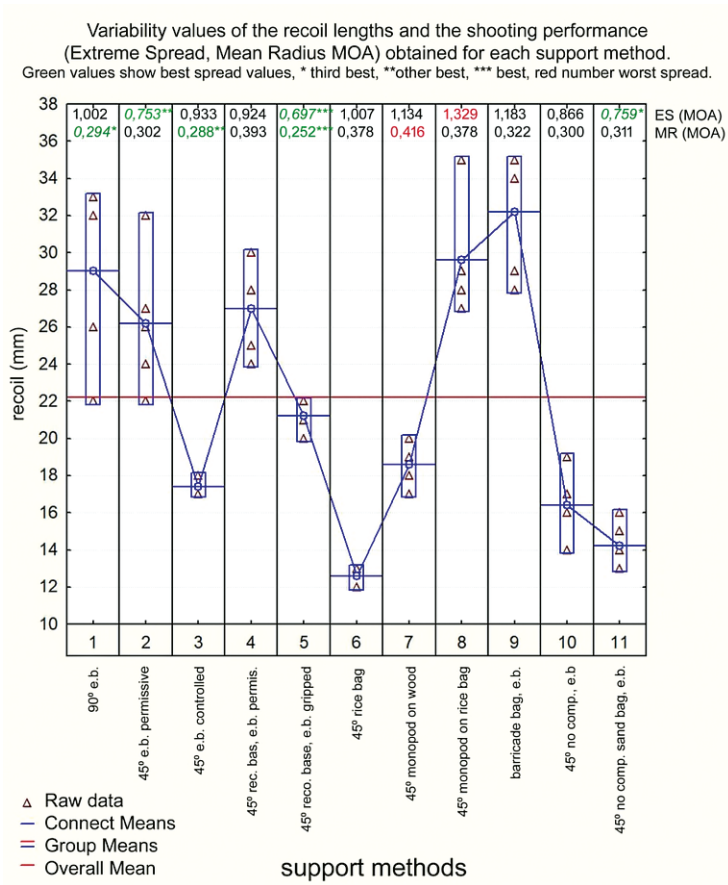


Figure 21: Variability values of the recoil lengths and the shooting performance (Extreme Spread, Mean Radius MOA) obtained for each support method

*Note: Green values show best spread values, * third best, ** other best, *** best, red number worst spread.*

Source: Compiled by the author.

The magnitude of the recoil showed no correlation with the magnitude of the view displacement, except in one case. The combination of a 45° bipod on a flat bag filled with sand with an ear bag and without a muzzle brake was only correlated in two cases. The smaller the backward displacement, the smaller the displacement of the bipod ($r = 0.9231$; $p = 0.0253$). This implies that the amount of backward displacement is not responsible for the amount of displacement of the image.

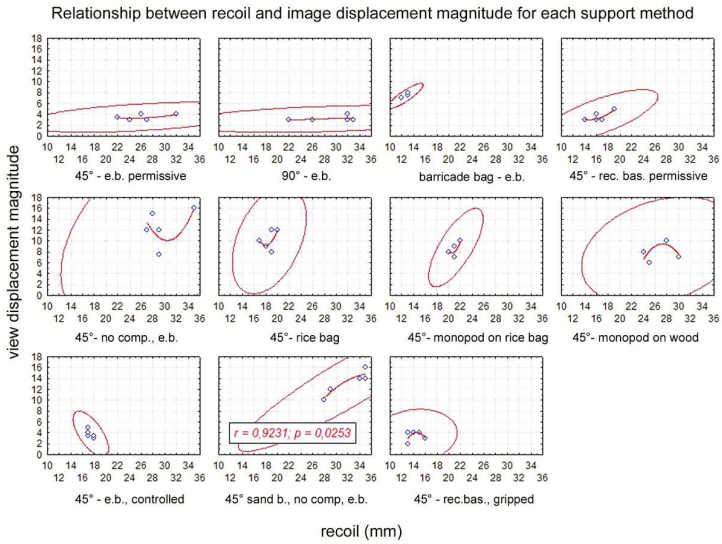


Figure 22: Relationship between recoil and view displacement magnitude for each support method

Note: A correlation was obtained only for the case of the combination of 45° bipod, eared bag, without compensator, placed on a sand-filled flat bag (r = 0.9231; p = 0.0253).

Source: Compiled by the author.

The strength of the recoil did not show any correlation with the scores achieved. That could mean that the success of the competitions are not determined by the magnitude of the recoil.

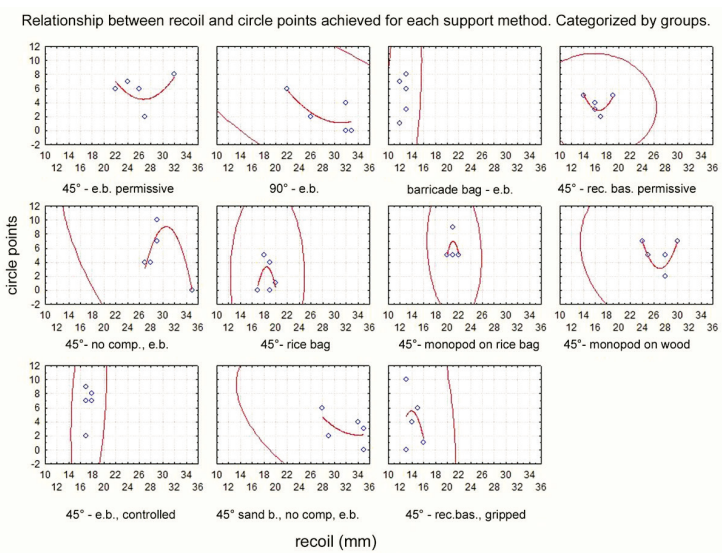


Figure 23: Relationship between recoil and circle points achieved for each support method (categorised by groups)

Source: Compiled by the author.

The rate of recoil and the direction of view displacements also showed no correlation except in one case. A correlation was found between the mentioned parameters in case of method barricade bag and eared bag ($r = -0.9186$; $p = 0.0276$). It was concluded that the length of the recoil does not influence the direction of the shot displacement (Figure 24).

In summary, the results obtained show that the length of recoil observed in the different front and rear support variations does not affect the direction of the developing reticle view, the length of its displacement, or the effectiveness in terms of circle points, except in one case. From this we concluded that there is no use in studying the rate of recoil in terms of these parameters, i.e. indirect accuracy. In the future, research should focus on changes that are happening during the time when the projectile is in the barrel. It should be noted that the above statement is for each separate case and the 5–5 shots should be treated with caveats due to the smaller number of elements.

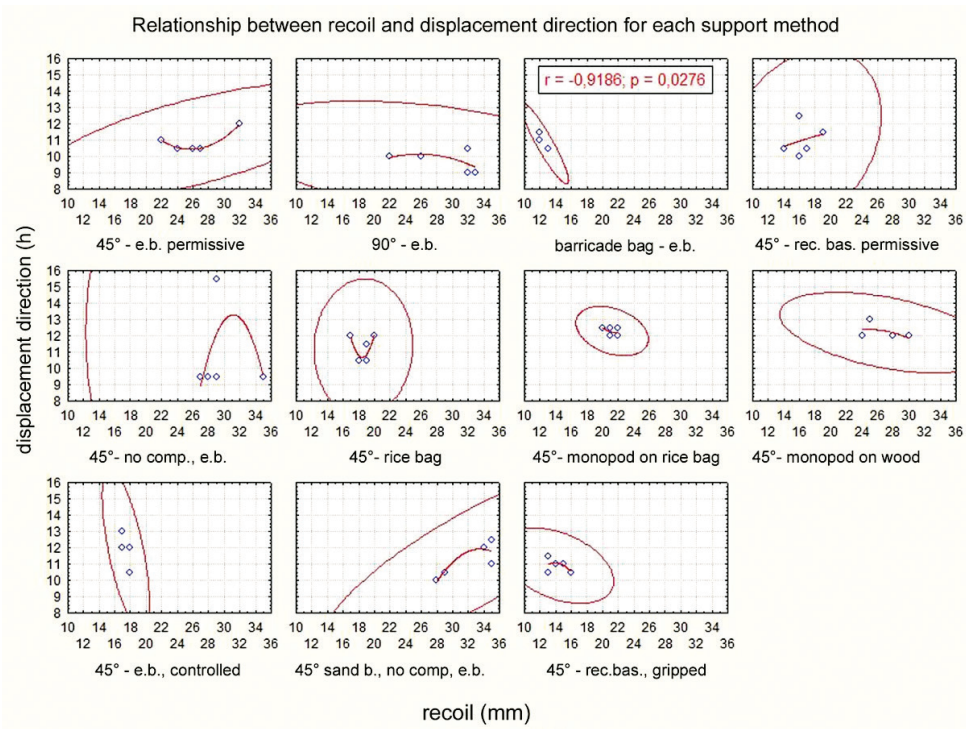


Figure 24: Relationship between recoil and displacement direction for each support method
Note: A correlation was obtained for the combination of barricade bag, eared bag ($r = -0.9186$; $p = 0.0276$).
Source: Compiled by the author.

4.4. Post-shot reticle centre vs. target centre view assessment

The target image observed after firing shows the relationship between the centre of the crosshairs and the centre of the target in units of 0.2 MOA (1.75 cm, or 0.06 mil). This post-fire view was a good characterisation of the jump-off from the target. In PRS competitions, the possibility of correction only becomes an option if the shooter can see the impact, i.e. the "jump-off" is small. Based on our hypothesis, this feature may also be an indicator of accuracy.

As shown in Figure 25, three groups could be distinguished. A small, medium and large jump group from the given support methods.

The smallest jumps were typically characterised by a jump unit of 3.2–3.6, with a jump of 0.64–0.76 MOA (5.6–6.6 cm, 0.196–0.228 mil). The difference between the small and medium groups was significant ($t = -14.429$, $p < 0.001$, F-ratio variances $= 3.761$, $p = 0.00432$).

- 90° bipod, eared bag
- 45° bipod, eared bag, permissive handling
- 45° bipod, eared bag controlled
- 45° bipod, recortan base, eared bag, permissive
- 45° bipod recortan base, eared bag, gripped holding

The medium group had a jump of 7.4–8.8 units, which translates to 1.48–1.76 MOA, (12.95–15.4 cm, 0.444–0.528 mil). The difference between the overall results of the medium and large groups was significant ($t = -4.9202$, $p < 0.001$, F-ratio variances $= 4.0515$, $p = 0.0132$).

- 45° bipod, monopod resting on wooden surface
- 45° bipod, monopod on rice bags
- barricade bag, eared bag

The large jump group was 10.2–13.2 leap units, which was 2.04–2.64 MOA (17.85–23.1 cm, 0.612–0.792 mil).

- 45° bipod, rice bag
- 45° bipod, without muzzle brake, eared bag
- 45° bipod without muzzle brake, on sand support bag

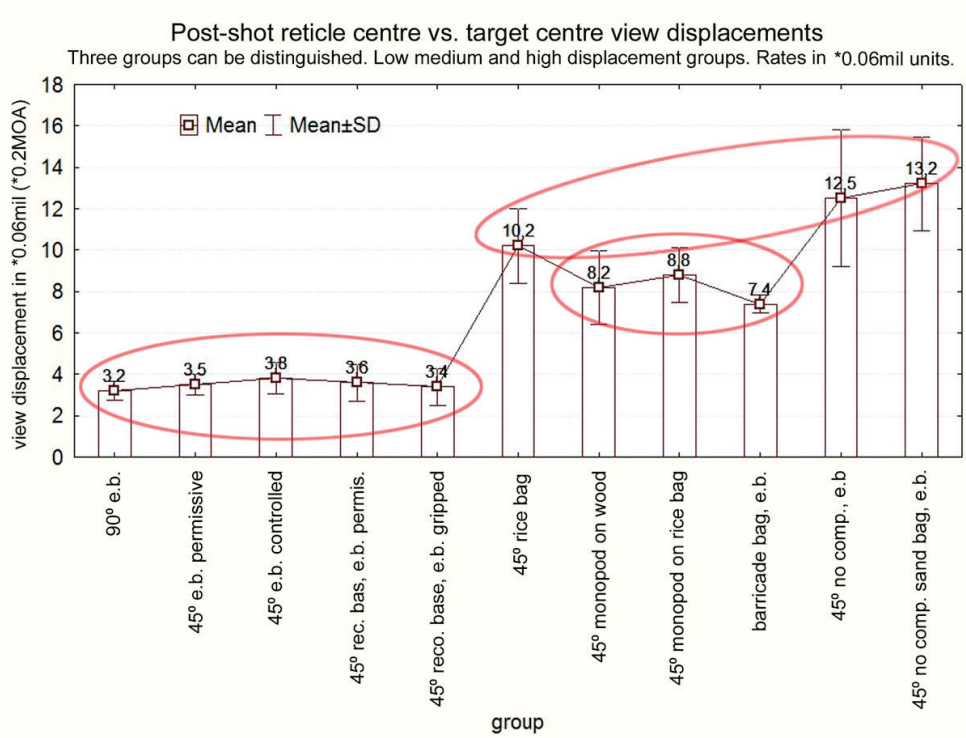


Figure 25: Post-shot reticle centre vs. target centre view displacements
Note: Three groups can be distinguished: low medium and high displacement groups (rates in 0.06 mil [0.2MOA] units).
Source: Compiled by the author.

The most stable support methods that stayed on target were those that could be described as "traditional". In national level competitions, the regulations state that a tactical bipod and a single rear bag may be used. In point of view, the eared bag is more advantageous because the ears, properly filled with sand or other material, provide greater stability in the lateral directions. During Hungarian precision competitions (big calibre, optical sighting), most competitors use a bipod and a shooting bag tilted at some angle, or a shooting bag with ears. During site placement to support the weapon, it would be essential to place the bipod on soil or sand, in other words, on a stable but not hard surface. Beginners often make the mistake of placing the bipod on a sponge or polyfoam surface (onto the shooting mat), thus reducing stability. Another potential issue is a surface that is too hard, such as concrete, on which rubber-tipped bipods can bounce. This is why the first five supports in Figure 25 can be called conventional. The sandbags integrated into the recortan base were designed to model the vibration absorbing properties of the bipod foot placed on sand. The higher degree of bounce caused by the 45 degree bipod foot plus rice bag combination can be attributed to the properties of the rice bag; however, this combination had the best spread results.

4.5. Displacement directions

After the moment of the shot, the movement direction of the crosshairs were determined by the dial of the clock. After each shot, the position of the arrival of the centre of the crosshairs and the centre of the target were compared and determined in 0.5 o'clock directions, and the results were averaged. This way, we obtained the direction in which the rifle started and arrived during the shots. Overall, we can say that the rifle was displaced from left to right and upwards, but that the different support variations did have an impact on this crosshair movement.

As shown in Figure 26, the 45° bipod-monopod method of trajectory displacement direction (mean: monopod end resting on tree: 12:15 h; monopod end resting on rice bag: 12:20 h) showed a significant difference from the 90° bipod-eared bag (mean: 9:45 h) support combination ($p = 0.00143$).

We are unable to accurately determine the causes of the trends in the image displacement data, as this may depend on several parameters, either individually or in combination, which we detail below:

- the direction of firing force transmission by the trigger
- the lateral movement of the weapon on the rear support due to the softness, hardness and fullness of the support materials
- the displacement effect of the force of the shooter's cheekbone on the muzzle
- structural failure of the first support (minimum probability, due to the quality of the first support)
- unevenness of the surface under the first support (minimum probability, due to its thorough inspection)
- inadequate water levelling (minimum probability because we tried to minimise it with a water level indicator before each shot – uniform implementation)
- the actual coincidence of muzzle vibration harmony and the ammunition powder charge and L6 length and NOD points

The two support methods that clearly showed upward displacements were the 45° bipod and the two rear monopod supports, which are logical and well defined influencers of displacement direction.

The monopod was held in such a way that the non-firing, i.e. back or passive, hand gripping the monopod by the handhold was angling the monopod (monopod pointing downwards relative to the pivot point on the stock) such that we could point to the centre of the target by leaning on the monopod. Retaining the weapon moving backwards at the moment of firing is relatively difficult at this point, as the monopod resting on the fulcrum will swing backwards along the axis of rotation, causing the weapon system, i.e. the barrel, to move upwards. In this case, the crosshairs are forced upwards away from the target and the rate of jumping from the target is very high.

In terms of accuracy (hitting spread), the largest deviations were obtained for shots without muzzle brake, where muzzle brake did not affect the target retention (SD = 2.28 hours for 45° – bipod on sandbag – muzzle brake, SD = 1.037 hours for 45° – bipod on sandbag – muzzle brake).

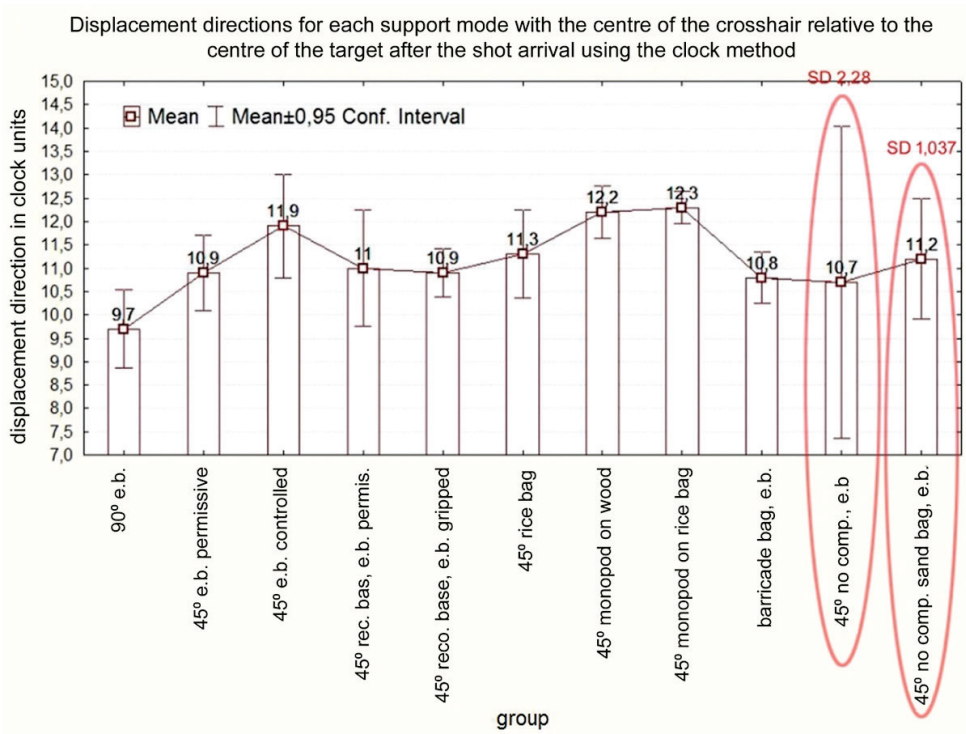


Figure 26: Displacement directions for each support mode with the centre of the crosshair relative to the centre of the target after the shot arrival using the clock method (clock)

Source: Compiled by the author.

4.6. Comparisons

By comparing the Pearson correlation of each parameter, we sought to determine the context in which any significant correlation can be interpreted in terms of the accuracy and precision of the shooting events in relation to each other for each support combination.

The recoil distance showed a significant correlation with the magnitude of the perceived displacement of the view after the shot ($r = 0.4381$, $p < 0.001$). This phenomenon can be considered natural and confirms the justification of the post-shot target image check in order to allow the shooter to control for possible errors that may occur during the shot. These errors include both the shooter's error and the error caused by overpressure from overloaded ammunition that produces a more pronounced recoil.

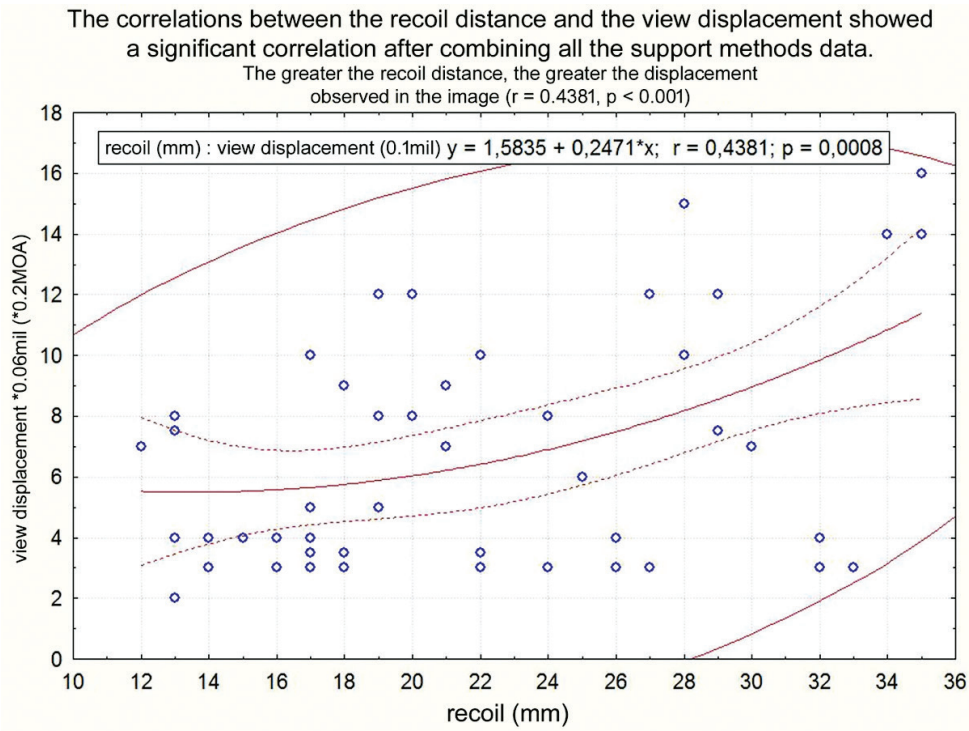


Figure 27: The correlations between the recoil distance and the view displacement showed a significant correlation after combining all the support methods data – the greater the recoil distance, the greater the displacement observed in the image (r = 0.4381, p < 0.001)

Source: Compiled by the author.

No significant correlations were found between the accuracy indices (ES, SD, MR, points) of the shooting series and the shooting and recoil data. We also found standard deviation values between support methods with both above-average and below-average recoil values for the first three accuracy values (Figure 21).

The relationship between precision and accuracy data is clear. The inverse proportionality of the correlation of the race performance score values with the horizontal group centre distance and the target centre distance values is also understandable ($r = -0.7503$, $p < 0.02$), as is the correlation with the group centre distance and target centre distance values ($r = -0.8501$, $p < 0.001$). This means that the smaller the horizontal or overall distance of the groups from the target centre, the higher the score achieved. However, no correlation was found between the distance between the vertical group and the target centre and the score ($r = -0.4635$, $p = 0.111$).

5. Conclusion

From the support variations, the best method in terms of precision, based on *Extreme Spread* (ES) and *Mean Radius* (MR) calculations, was to use a 45° bipod with a monopod and rear rice bag support combination, resulting in ES = 0.697 MOA and MR = 0.252 MOA. The second best variation was the 45° bipod and eared bag combination with permissive method (the weapon left sliding, and not shouldered), which measured at 0.753 MOA. However, the values from this support combination were similar to the values of the 45° bipod on recortan integrated sandbags and eared bag combined with the gripped rifle method (weapon shouldered).

The lowest recoil value was obtained with the combination of barricade bag and eared bag, which had an average recoil value of 12.6 mm for the five shots.

The length of recoil developed during the different front and rear support methods did not affect the direction of the view image, the length of its displacement, or the effectiveness in terms of circle points, except in one case. In other words, there is no benefit to studying the extent of recoil in terms of these parameters, i.e. indirect accuracy.

The methods that were best at staying on target were those that could be described as "traditional".

Overall, we found that the weapon moved left to right and upwards during the shots, but that different support combinations affected this movement. Two support methods that clearly produced upward displacements were the 45° bipod, rear monopod combinations.

Correlation tests showed that recoil distance was significantly correlated with the magnitude of the view displacement ($r = 0.4381$, $p < 0.001$).

No significant correlations were found between the precision indicators (ES, SD, MR, points), displacement view, and recoil data. However, the correlation with precision data is clear. The inverse proportionality of the correlation of the point values (indicators of competition performance) with the horizontal group centre and target centre distance values is also clear ($r = –0.7503$, $p < 0.02$), as is the correlation with the group centre and target centre distance values ($r = –0.8501$, $p < 0.001$).

Our first hypothesis proved to be correct, that there is a significant difference in precision between the different types of rest combinations, i.e. it does not matter which front and rear rests are used in sport shooting competitions and how the shooter handles the gun during the shoot.

Our second hypothesis regarding the degree of recoil in each support scenario was not proven correct since we found no correlation between the degree of recoil and accuracy in individual cases of different support methods. A comparison of all the data, however, showed that the degree of recoil was significantly related to precision. The other part of our hypothesis, that the support methods that absorbs gun recoil movements during firing is more accurate, was not confirmed. However, this assumption is compounded by the fact that the we did not apply one specific support method which used the "only recoil" method, utilised by the traditional F-Class or other precision competitions, (for example ski-mounted wide F-Class bipod or special shooting "base" or "benchrest"). We used a barricade bag implemented mainly in

PRS competitions, which, although it provided the lowest recoil value, but was not among the methods that provided the highest accuracy.

Our hypothesis that the magnitude of the displacement of the image after the shot is related to accuracy was confirmed (magnitude of image displacement vs. ES: $r = 0.6922$, $p = 0.018$), but it was not related to the more narrowly defined value of accuracy (MR) (magnitude of image displacement vs. MR: $r = 0.4946$, $p = 0.122$).

It was also assumed that the first support method (Figures 9, 10, 20) placed on three vibration absorbing surfaces – where the bipod was placed on a bed of sand or bags – would give the second most accurate results was only partially fulfilled. The method without a muzzle break was not accurate despite the sand bed. From the two other methods, the vibration absorbing front support produced narrow spread only when firing with a tight, gripped gun.

Finally, our hypothesis that the least accurate results would be obtained with a bipod on solid ground, which is based on the principle of tipping, was not clearly determined because the accuracy did not depend primarily on the front support alone, but on the combined properties of the front and rear supports.

In the study, the tilting-sliding method was mixed for the front and rear supports. No method was investigated that was clearly and explicitly a sliding support for the front and rear cases. These are part of the F-Class applications we already mentioned. These do not allow lateral movement deviations in a well-defined way. The initiation and deceleration of the gun slide is easy and does not cause any jump during the time the projectile is in the barrel that would adversely affect accuracy. In future research, we will focus on this aspect.

6. Summary

The aim of our study was to find under which support conditions bolt action, high-calibre firearms produce the best accuracy at long range.

In this study, we chose 11 different front and rear support methods that are most commonly used in domestic, precision competitions. In these methods, we used a tactical bipod and barricade bag as front supports combined with an eared bag, rice bag or a monopod as rear supports. Muzzle breaks were used in most of the methods, but in two cases we fired without it. During the shooting we used: a) permissive (way giving or untensioned) method, where the shooter lets the gun slide freely backwards; b) gripped method, where the gun is pulled tightly into the shoulder; c) controlled handling method, where we applied support but the gun could move in a controlled way. Accuracy was determined by the spread (ES, MR) and circle values (circle units) generated by bullet on paper target area by MOA and point parameters. During firing, we examined the length of the weapon recoil, the direction and extent of view displacement relative to the target centre, and the velocity of the projectile.

As expected, the data obtained showed significant variation in precision between each support combination. There was also a significant difference in the values of the recoil length and the shot bounce after the shot. The directions of barrel displacement were essentially in the quarter between the 9 and 12 o'clock positions.

All of the most precise trial results were obtained using a muzzle break with a 45° bipod as the first support. For the rear support, a combination of a rice bag and a gripped monopod, or an eared bag was optimal. Regarding the method of retention, both permissive (sliding) and controlled handling were effective compared to the gripped method. Less optimal spread was obtained with: no muzzle brake, barricade bag as front, and rice bag lifted and controlled as rear support.

The correlation studies showed that the length of recoil developed had no effect on the view directions, the length of the view displacement, nor the effectiveness counted in circle points, except in one-one case when recovery methods were examined separately. However, when all the data were pooled, recoil distance showed a significant correlation with the amount of post-shooting displacement of view in relation of crosshair centre and target centre ($r = 0.4381$, $p < 0.001$).

In future studies we will be analysing the front and rear supports used in F-Class competitions and comparing these data with the present results to see which methods allow for the best precision.

References

Guns and Ammo: *Long Range Shooting: Understanding Extreme Spread and Standard Deviation.* 05 September 2018. Online: www.gunsandammo.com/editorial/long-range-shooting-understanding-extreme-spread-and-standard-deviation/247510

Gunmakers' Company and The Guardians of the Birmingham Proof House: *Rules, Regulations and Scales Applicable to the Proof of Small Arms.* London, 2006. Online: www.gunproof.com/downloads/rules-proofing

Litz, Bryan: Scope Tracking: Tall Target Test. Applied Ballistics with Bryan Litz. *YouTube,* 12 June 2015.

RocketmanOU: *Statistics, Shooting and the Myth of the Three Shot Group.* 2020. Online: www.bealeinnovations.com/stats-3shotgroup.pdf

Simonyi, Ottó: *A mesterlövész. Vadászatról és sportlövészetről* [The Sniper. About Hunting and Sport Shooting]. Vác, Cyberkinetic Kft., 2021. Online: https://doi.org/10.38146/BSZ.2022.7.13

Zant, Cal: Muzzle Brakes: Ability to Stay on Target. *Precision Rifle Blog,* 25 July 2015. Online: https://precisionrifleblog.com/2015/07/25/muzzle-brakes-ability-to-stay-on-target/

Zant, Cal: Muzzle Brake: Summary of Field Test Results. *Precision Rifle Blog,* 21 August 2015. Online: https://precisionrifleblog.com/2015/08/21/muzzle-brake-summary-of-field-test-results/

Zant, Cal: Works Cited for Statistics for Shooters Articles. *Precision Rifle Blog,* 2020. Online: https://precisionrifleblog.com/works-cited-for-statistics-for-shooters-articles/

Zant, Cal: Statistics for Shooters – Executive Summary. *Precision Rifle Blog,* 16 December 2020. Online: https://precisionrifleblog.com/2020/12/16/statistics-for-shooters-executive-summary/

HADMÉRNÖK
HADITECHNIKA

17. évfolyam (2022) 3. szám 35–44.
DOI: 10.32567/hm.2022.3.2

Ember István,[1] Ádám Balázs[2]

Kumulatív töltetházak 3D nyomtatása

Shaped Charge Body Producing with 3D Printer

A kumulatív töltetek alkalmazása az ipari és katonai robbantások során esetenként jelentős előnyöket hordozhat. A különböző rombolások és tűzszerészek által végzett hatástalanítások meghatározó módszereihez szükségesek ezek a töltetek. A feladatok jelentősen eltérhetnek, ami eltérő típusok alkalmazását teszi szükségessé. Tanulmányunkban megvizsgáljuk a lehetőségeit a töltetházak 3D nyomtatásának, ezzel bemutatva egy 21. századi lehetőséget. A vizsgált nyomtatási lehetőségek megmutatták, hogy az alkatelemek megfelelő minőségű tervezéséhez jártasságszintű tervezőprogram-ismeret szükséges. A nyomtatások során több esetben nehézségekbe ütköztünk, de sikerült elérni a kitűzött célokat és kinyomtatni több változatban kumulatívtöltet-házat. A gyártás idő- és anyagigénye igazolja, hogy ennek a módszernek van létjogosultsága a hadi és ipari alkalmazás során.

Kulcsszavak: **kumulatív töltet, 3D nyomtatás, robbantás, PLA**

The use of shaped charges during industrial and military blasting process may provide significant benefits. The different destructions and disarming tasks accomplished by sappers or explosive disposal operators demand special methods with shaped charges. There may be some notable difference among those tasks which determine the engagement of different types of charges. We examine the possibilities of 3D printed shaped charge bodies in our study presenting an up-to-date solution. These examined possibilities showed that it is necessary to know well a sketcher software to execute a proper planning process. During the printing procedures we faced with several problems, however, we managed to achieve our goals and multiple types of charge body were printed. The claim of time and material certifies that this method is applicable in industrial and military blasting processes too.

Keywords: **shaped charge, 3D printing, blasting, PLA**

[1] Egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék; doktorandusz, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, e-mail: Ember.Istvan@uni-nke.hu

[2] Honvédtisztjelölt, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: Adam.Balazs@uni-nke.hu

1. Bevezetés

Korunk fejlett technológiai szintje lehetőséget biztosít rengeteg területen, hogy egyedi eszközöket, alkatelemeket használjunk hétköznapjaink vagy munkánk során. Nincs ez máshogy a robbantástechnikában sem. A különböző speciális eszközök, töltetek kialakítása – alapszintű számítógépes tervezési ismerettel és némi jártassággal a 3D nyomatás világában – gyakorlatilag egy irodában is lehetséges a szakemberek számára. Természetesen a robbanóanyag-töltet és a gyújtószer ezekben az esetekben csak az alkalmazás helyszínén kerülhet bele a kinyomtatott alkatelemekbe.

A műszaki támogatás[3] keretében végrehajtott robbantások sokfélék lehetnek, és helye van köztük a kumulatív tölteteknek. Helye lehet a különböző rombolási feladatok során és a tűzszerész szakfeladatok végrehajtásakor egyaránt. Az előző két terület alapján meghatározható, hogy vizsgálatunk kiterjed a Magyar Honvédség (MH) által kijelölt több fő kutatási irányba is, mint a terrorizmus elleni harc, egyes nemzetközi feladatok és az országvédelem.[4] Ez azt is mutatja, hogy a lehetséges eredmények több vonatkozásban segíthetik majd a szakemberek munkáját.

Feltételezésünk szerint lehetséges olyan töltetházat kialakítani ezekkel a modern eszközökkel, amely alkalmas lehet a kumulatív töltetek többi elemének hordozására, valamint a helyszíni vagy alkalmazás előtti készre szerelés feltételeit is biztosítja.

A fenti feltételezések igazolásán túl célkitűzésünk, hogy a katonai felsőoktatásban műszaki specializáción tanuló honvédtisztjelöltek képzésébe is integrálható eljárást alakítsunk ki, ezzel emelve a felkészítés egyébként is magas színvonalát.

2. A 3D nyomtatás technológiái

Napjainkban a 3D nyomtatás különböző technológiáival már nemcsak műanyagokat, hanem fémeket és egyéb építőanyagokat is lehet nyomtatni. 2021-ben Németországban már egy kétszintes családi házat is sikeresen kinyomtattak, speciális betonkeverék segítségével. Az új technológia alkalmazásához csupán két kezelőre volt szükség, és a normál építési feladatok időtartamához képest annak töredék ideje alatt sikerült elkészíteni az épületet, amelynek minden egyes betonrétege 2 cm vastag volt. Alapvetően viszont a 3D nyomtatást először műanyagok nyomtatására fejlesztették ki. Csak később váltak vele nyomtathatóvá más anyagok, mint például a fémek vagy a fent említett beton.

Mivel a műanyagokat kezdték el legelőször 3D nyomtatásra felhasználni, így napjainkra már számos nyomtatási mechanizmus vált ismertté. Mivelhogy a töltetház anyagának kiválasztása megtörtént, így már csak az alkalmazott nyomtatási eljárást kellett kiválasztani. Minden nyomtatási technológiának megvannak a maga előnyei és hátrányai, így több technológia összehasonlításának eredményeként született meg

[3] Kovács Zoltán: Gondolatok a műszaki támogatás és a műszaki zárás alapjairól. *Nemzetvédelmi Egyetemi Közlemények,* 6. (2002), 1. 30–46.

[4] Boda József et al.: A hadtudományi kutatási irányok, prioritások és témakörök. *Államtudományi Műhelytanulmányok,* (2016), 16. 1–23.

a döntés a szálhúzásos (FDM[5]-) módszer mellett. A vizsgált típusok között voltak még a poralapú (SLS[6]-) és folyadékalapú (SLA[7]-) technológiák. Minden kétséget kizáróan a műanyagok nyomtatása jár a legkisebb költségekkel, valamint az eltérő műanyagtípusok alkalmazását is a konkrét feladathoz lehet igazítani. Viszont fontos leszögezni, hogy ennek költségei még így is jelentősen nagyobbak, mint a műanyag fröccsöntésé, ezért a 3D nyomtatást csak a tesztelések és prototípusok előállítására, továbbá egyedi geometriák kialakítására érdemes használni korlátozott mennyiségben. Azt nagyipari termelésre sem a munkaidő, sem az előállítási költségek nem teszik alkalmassá.

Az SLS-technológia lényege, hogy egy fúvóka zárt térben 50–200 mikron[8] vastagságú porréteget képez, amelyet egy meghatározott pályán mozgó lézer pontonként kiéget. Ahol a lézer kiégette a műanyag alapú port, ott az megszilárdul, ahol nem, ott továbbra is por halmazállapotú marad. Mivel a port rétegenként viszi fel, így a legkülönfélébb geometriai alakzatok nyomtatásához sincsen szükség támasztékok beépítésére a 3D modellbe. Viszont pontosan ennek köszönhetően a nyomtatás befejezésekor a tárgyak előhívásához utómunkaként el kell a felesleges (nem megszilárdult) pormennyiséget távolítani, ami az egészségre rendkívül káros, így csak fokozott munkavédelmi előírások betartása mellett történhet. SLS-technológiával csak nylon anyagok nyomtathatók különböző változatokban, ezeknek színe leginkább szürkés barnás, ezáltal rendkívül könnyen felismerhetők az ilyen típusú nyomtatók termékei. Alapvető tulajdonságai a törésmentesség, szakadásmentesség és a rugalmasság, ezért rendkívül jól használható kis terhelésű mozgóalkatrészek gyártására.

Az SLA-technológia alkalmazása során a lézer fényre érzékeny folyadékba sugároz, ahol a 3D nyomtatott modell megfelelő pontjain a fényérzékeny műanyag folyadék megszilárdul. A megszilárdult pontokból rétegről rétegre jön létre a 3D modell. Alapvetően a folyadék miatt itt sincs szükség statikai támasztékokra, viszont a folyadékból való kiemeléshez a tárgynak a megfelelő pontokon kapcsolódnia kell az azt mozgató tálcához, ezért vannak beépítve támasztékok, viszont ezek könnyen és egyszerűen eltávolíthatók. A nyomtatási eljárások közül a galvófejes lézer segítségével lehet a legpontosabban nyomtatni, ugyanis ennél a technológiánál mikronos pontosságról beszélhetünk. Éppen ezért rendkívül részletes, egymáshoz illeszkedő alkatrészeket lehet vele nyomtatni, így előszeretettel alkalmazzák a technológiát a fogászatban. Színes és átlátszó kivitelben is lehet kapni a nyomtatáshoz szükséges, fényre érzékeny folyadékot, amelyet színezékekkel a kívánt színűre lehet festeni. A folyadék kiszerelését tekintve általában 500 g vagy 1000 g,[9] illetve fontos, hogy megfelelő időközönként a gépben lévő tálcákat is – amelyek a folyadékokat felfogják – cserélni kell.

Az FDM- vagy szálhúzásos technológia segítségével lehet a legegyszerűbben és legolcsóbban előállítani 3D-s tárgyakat, ezért a nyomtatók e fajtája a legelterjedtebb. Legnagyobb választékban az FDM-típusú eszközök kaphatók, amely nyomtatók bekerülési értéke mellett a fenntartási és alapanyagköltségek is a legkisebbek a korábban említettekhez képest. Működése egyszerű. Egy filamentnek nevezett

[5] Angol elnevezése: *fused deposition modeling*.
[6] Angol elnevezése: *selective laser sintering*.
[7] Angol elnevezése: *stereolithography*.
[8] FreeDee: *SLS-nyomtatás (szelektív lézerszinterezés) útmutató*. (é. n.).
[9] Lásd: www.3djake.hu/resin

tekercselt műanyagot használ, amely műanyag típusa rendkívül változatos lehet. A filament egy fogaskerekes adagolóegységen megy keresztül, amely azt belenyomja a melegítő egységbe,[10] ahol a műanyag megolvad, folyékony halmazállapotúvá válik. Az adagolóegység által létrehozott nyomás hatására a „hotend" végén lévő fúvókán keresztül jut ki a műanyag a nyomtatófejből a fűtött asztalra vagy tálcára. Az eltérő filamenttípusok eltérő nyomtatástechnológiát kívánnak, így mind a „hotend", mind a fűtött tálca hőmérséklete szabályozható. A feladathoz mért megfelelő részletességű nyomtatáshoz ki kell választani a megfelelő méretű fúvókát, amelyből számtalan méret létezik. Rendelkezésünkre állt több változat: 0,25 mm, 0,4 mm és 0,8 mm. Ezekből alapvetően a legnagyobbat használtuk ennél a vizsgálatnál. A fúvóka átmérőjének megfelelő kiválasztása azért is fontos, mivel a nagyobb átmérővel felére vagy harmadára lehet csökkenteni a nyomtatási időt. Éppen ezért, ha nem kívánt a modell tökéletes és részletgazdag nyomtatása, nagyobb fúvókaátmérővel érdemes nyomtatni. A filamenteknek rendkívül sok változata ismert. Találhatunk farostokkal vagy rézzel, illetve olyan gipsszel dúsítottakat is, amelyeket makettezőknek fejlesztettek ki, hogy azokat festéssel lehessen színezni.

Mivel a kutatás során az egyik fő feladat a kumulatív töltetházak nyomtatása volt, így a feladathoz legjobban illeszkedő nyomtatótípus kiválasztása volt a feladatunk. A követelményeket a viszonylagosan nagyszámú nyomtatás, a költséghatékony fenntarthatóság és a pontosság mérésének nem a pár tíz mikronos, hanem az annál jóval nagyobb mértékek használata jellemezte. Így a feladathoz legjobban illeszkedő technológiát és nyomtatót, egy Craftbot 3 típusú FDM-nyomtatót választottunk a feladathoz.

3. A töltetházzal szemben támasztott követelmények

Mivel egy robbantási feladathoz tervezett eszközről van szó, az esztétikai szempontokat minden esetben jelentéktelennek tekinthetjük. A kialakítás során az alkalmazhatóság és a töltet hatékonyságának növelése a meghatározó. Mindezeken túl a kész alkatelemeknek minimális utómunkálattal (sorják eltávolítása) egymásba illeszkedőnek kell lenniük, és pillanatragasztóval megbízhatóan kell rögzülni a részegységeknek. A gazdaságosság szintén meghatározó szempont, valamint az, hogy képes legyen elviselni a készre szerelés erőhatásait.

A ház falának kialakítása az alkalmazott anyagok és az észszerűen méretezett vastagság miatt nincs hatással a hatékonyságra. Készíthető olyan töltetház, amely kibírja a robbanás dinamikus terheit és ezáltal a fellépő energiákat tovább erősíti, de ezek alkalmazása nem praktikus. Nem is igazán fellelhető ilyen a piacon, inkább mint elvi lehetőség említettük meg. Az viszont nem kérdés, hogy kellően erős töltetházra van szükség a helyszíni, kézi készre szerelés végrehajtásához.

Az anyag tekintetében a hadi felhasználás a tartós, időjárásálló és vegyszerálló alapanyagokat részesíti előnyben. Ezek jelentősége vitán felül áll. Azonban egy prototípus gyártásakor meg kell találni a legolcsóbb, de használható anyagokat. A PLA

[10] Angol és szakmai elnevezése: „hotend".

ilyennek bizonyult annak ellenére, hogy korlátozott ideig eltartható. Mivel a gyártás vagy nyomtatás esetén ilyen tölteteknél nem telik el hosszú idő (technikailag 1–2 nap), valamint a helyszíni alkalmazás és készre szerelés sem időigényes (néhány óra), úgy gondoljuk a hadi alkalmazása is megfontolandó. Mindezeken túl nagyon stabilan ragaszthatók[11] a PLA-alapanyagok egymáshoz és fémekhez egyaránt. A későbbiekben természetesen lehetőség van a kész terveket más alapanyagokkal is reprodukálni.

Mivel az ilyen töltetek a különböző robbantási feladatoknál különböző ipari robbanóanyagokkal,[12] bináris robbanóanyag-keverékekkel[13] és katonai robbanóanyagokkal[14] egyaránt készülhetnek, a végleges alapanyagot meghatározza majd azok összeférhetősége egymással. Várhatóan a hadi alkalmazás miatt valamilyen plasztikus robbanóanyag lesz majd a fő töltet, mint például a Semtex.

4. Kumulatív töltetházak 3D-modellezése

A végső változatok „FreeCAD" program alkalmazásával készültek el. Ez a szoftver lehetőséget biztosít, hogy professzionális módszerrel alakítsuk ki az alkatelemeket. Kifejezetten ez utóbbira optimalizált felülettel is rendelkezik, de klasszikus tervezési lehetőségeket is biztosít. Az elkészült 3D-modellt exportálni kell és „.stl" formátumban elmenteni, amit a továbbiakban a nyomtatás előkészítése során, az alkatelem modelljének úgynevezett „szeletekre" bontásánál használni tudunk.

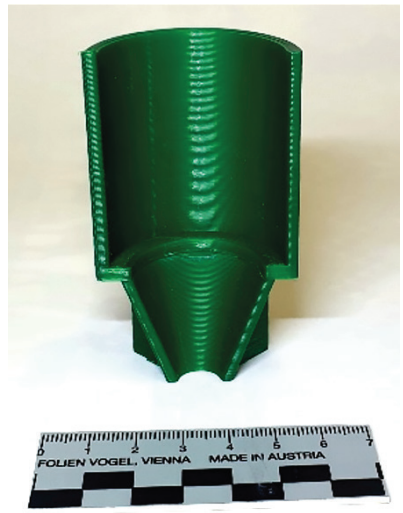
A kumulatív töltetházak több méretben készültek, ezeket a bennük elhelyezett kumulatív béléstestek belső átmérője alapján neveztük el. Az elnevezésük nem fedi a tényleges paraméterüket, de ragaszkodnunk kellett ehhez a változathoz, mert a béléstest átmérője alapján lehetett könnyen azonosítani az egymáshoz megfelelő méretű alkatelemeket. A kinyomtatott változatok a fent jelzett elnevezések mentén készültek 40 mm-es, 35 mm-es, 30 mm-es, 25 mm-es és 20 mm-es béléstestekhez. Ahogy az 1. ábrán látszik, a töltetházak felső része henger alakú volt, amely feladata a kumulatív béléstest, illetve a robbanóanyag pontos rögzítése. Ez alatt egy belső átmérőjében és vastagságában kisebb henger helyezkedett el, amely támaszt biztosított és pozicionálta is a béléstestet. A töltetház aljára egy, a töltet alja felé szűkülő, üreges csonkakúp visszaáramlásgát került, amelynek feladata a kumulatív sugár kialakulásának optimalizálása, ezzel az elvi penetrációs képesség növelése. A töltetházak két típusú eltartással készültek. Ez azt jelenti, hogy a kumulatív béléstest alsó síkja, illetve a céltárgy között a béléstest belső átmérőjének egyszeres vagy kétszeres távolsága van. E köré négy téglatest került, amelyek a töltetház stabil és megbízható feltámaszkodását és rögzítését biztosítják a céltárgyon.

[11] Loctite Power Flex és Loctite Super Bond termékek alkalmazásával vizsgálva.

[12] Daruka Norbert: Robbanóanyag-ipari alapanyagok és termékek osztályozásának lehetőségei. *Műszaki Katonai Közlöny,* 26. (2016), 1. 26–43.

[13] Kugyela Lóránd: A többkomponensű robbanóanyagok múltja, jelene és jövője. *Katonai Logisztika,* 28. (2020), 4. 58–75.

[14] Lukács László: *Szemelvények a magyar robbantástechnika fejlődéstörténetéből. Különös tekintettel a továbbfejlesztés várható irányaira és a kor új kihívásaira.* Budapest, Dialóg Campus Kiadó, 2017. 26. 1. ábra.



1. ábra: Töltetház metszete
Forrás: a szerzők szerkesztése

A töltetházakhoz készült egy gyutacsfészek készítésére alkalmazható kupak. A kupak középső részén 1 cm magas, 0,8 cm átmérőjű henger van, amely a gyutacs pontos elhelyezését szolgálja a robbanóanyagban. Így a gyutacs a kör közepén való, megfelelő mélységű elhelyezésével egyenletes iniciálás érhető el plasztikus robbanóanyagok alkalmazása esetén. A későbbiekben egy gyutacstartó kupakot is kialakítottunk. Ennek a középső hengeres részében 8 mm-es furat található, valamint a furat felett 1 cm magas henger, amelyben szintén megegyező 8 mm-es furat van. A kupakot és a hengert külön alkatelemként nyomtattuk ki és pillanatragasztóval rögzítettük véglegesen egymáshoz.

5. 3D-modellek szeletelése és a G-kód előállítása

A töltetházak nyomtatásának legfontosabb követelményei a strapabíró, erős kialakítás és a minél gyorsabb előállíthatóság volt. A strapabíróságot a filament anyagának és a töltetház falvastagságának változtatásával lehet módosítani. Mivel a töltetházakat tárolásból kivétel után egyből felhasználják, nem kitétel a környezeti hatásoknak ellenálló anyag, mint az ABS[15]-filament használata, ezáltal a legazdaságosabb filamentből, a PLA-ból[16] dolgoztunk a házak gyártása során. Mivel a lehető legrövidebb nyomtatási időt szerettük volna elérni, a 0,8 mm-es fúvókaátmérőt használtuk nyomtatás során.

A 3D-modellek szeleteléséhez, a G-kód előállításához több felhő- és nem felhőalapú szoftver is használható. Jelen feladathoz a „Craftbot" cég által fejlesztett

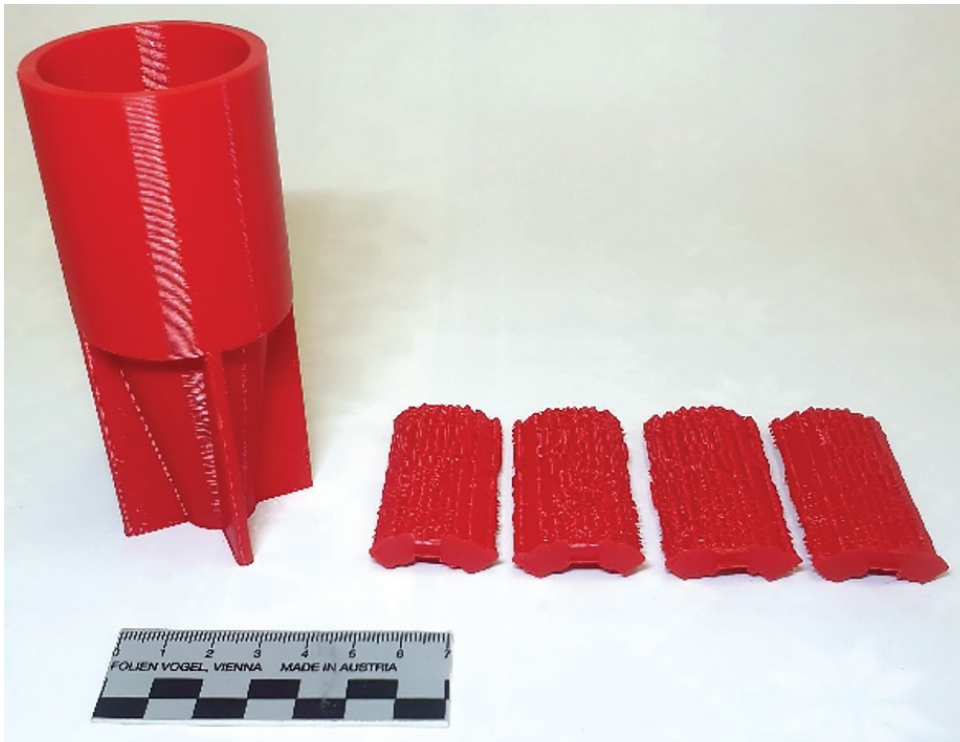
[15] Angolul: *acrylonitrile butadiene styrene,* magyarul: akrilnitril-butadién-sztirol.
[16] Angolul: *polylactic acid,* magyarul: politejsav.

CraftWare alkalmazást használtuk. A gyorsabb nyomtatás érdekében párhuzamos, tehát egyszerre két fejjel való eljárást választottunk. Ekkor a két fej egymással szinkronban mozog, így megegyező idő alatt két test is kinyomtatható, viszont hiba esetén könnyen mindkettő test hulladékká válhat.

2. ábra: Töltetház a nyomtatási támasztékokkal
Forrás: a szerzők szerkesztése

A töltetházak nyomtatásához szükség volt támasztékok generálására is a béléstest felfekvését biztosító henger alá (2. ábra), mivel ellenkező esetben ezek a levegőben szabadon lógtak volna. Ennek kiküszöbölésére szóba került a 180°-os „fejjel lefelé" nyomtatás is, viszont így is kellett volna támasztékokat generálni, csak azok a testen belülre kerültek volna, ami nehezítené azok eltávolítását. A támasztékok eltávolítását megkönnyítette volna, ha azokat vízben oldódó filamentből (PVA)[17] készítjük, viszont így egy tárgy nyomtatásához két nyomtatófejet kellett volna használni, továbbá a felhasznált anyagok sokkal költségesebbek lettek volna. Ezért inkább a támaszoszlopok méretét kellett megfelelően kiválasztani úgy, hogy a PLA-anyagú támasztékokat egyszerűen, fizikai erővel is ki lehessen törni a töltetházból (3. ábra).

[17] Angolul: *polyvinyl acetate,* magyarul: polivinil-acetát.



3. ábra: Töltetház az eltávolított nyomtatási támasztékokkal
Forrás: a szerzők szerkesztése

A különböző gyártók eltérő hőmérsékletértékeket határoznak meg a PLA-anyagok felhasználásához, de mi ezektől függetlenül általános értékeket, tehát 215 °C-os „hotend" és 60 °C-os tálcahőmérsékletet alkalmaztunk minden nyomtatásnál. A töltetház belső kitöltését a lehető legnagyobb szilárdság elérése érdekében párhuzamos vonalakból álló 100%-os kitöltésre állítottuk. Célszerű karima használata a test körül, amely nyomtatása során a nyomtatófej valamennyire kalibrálja magát, valamint ezáltal az esetleges kezdeti hibák is hamar kiderülhetnek.

6. Kumulatív töltetházak nyomtatásának sajátosságai

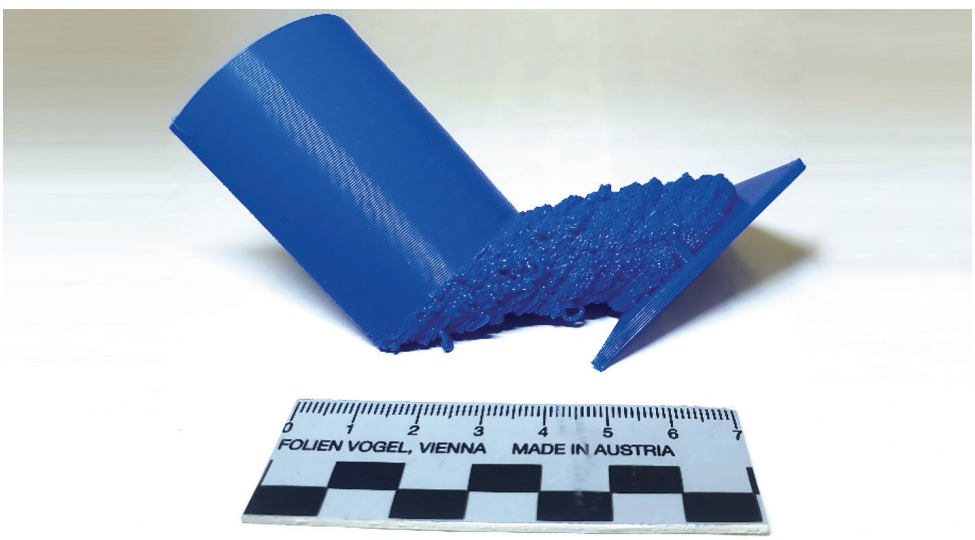
A töltetházak nyomtatásához két darab Craftbot 3 nyomtatót használtunk. Bár a CraftWare alkalmazás a „szeletelés" során ad egy hozzávetőleges nettó értéket a nyomtatás időtartamát illetően, ezt a tapasztalatok alapján 15–20%-kal növelve kapjuk csak meg a tényleges időtartamot. Viszont ez függ a nyomtatófejek és a tálca hőmérsékletétől, a szünetektől és a G-kódtól is, így az erről szóló táblázatban (1. táblázat) a CraftWare által megadott nettó értékek szerepelnek.

1. táblázat: Töltetházak nettó nyomtatási ideje

Fsz.	Töltettípus	Átmérő	Magasság	Nyomtatási idő
1.	20 mm-es béléstesthez	36 mm	61 mm	40 perc
2.		36 mm	81 mm	59 perc
3.	25 mm-es béléstesthez	41 mm	70 mm	54 perc
4.		41 mm	95 mm	92 perc
5.	30 mm-es béléstesthez	46 mm	80 mm	71 perc
6.		46 mm	110 mm	108 perc
7.	35 mm-es béléstesthez	51 mm	90 mm	90 perc
8.		51 mm	125 mm	139 perc
9.	40 mm-es béléstesthez	60 mm	100 mm	131 perc
10.		60 mm	140 mm	207 perc

Forrás: a szerzők szerkesztése

A töltetházak nyomtatása során kevés hibát tapasztaltunk. Leginkább annak köszönhetően, hogy a nyomtatófej körkörösen tudott dolgozni a 3D-modell szerkezete miatt, így nem kellett a nyomtatás irányát folyamatosan változtatnia. Néhányszor a tálca szennyeződése miatt nem volt megfelelő a tapadás, valamint előfordult, hogy a támaszoszlopok helytelen méretezése miatt a visszaáramlást gátló rész teljesen elferdült a nyomtatás során (4. ábra). De ezeket leszámítva kis hibaaránnyal készültek el az alkatelemek.



4. ábra: Hibás nyomtatás eredménye
Forrás: a szerzők szerkesztése

7. Összegzés

A nyomtatások eredményei bebizonyították, hogy az alkalmazott nyomtatótípussal lehetséges elkészíteni ezeket a töltetházakat. Az elkészült változatok felülete ugyan nem esztétikus, de egy felrobbantásra tervezett alkatelem esetében ez nem lehet szempont. Az alkalmazhatóság azonban már sokkal fontosabb tényező, és mivel a különböző alkatelemek egymásba illeszthetők lettek, valamint kellően erősek szerkezetileg, véleményünk szerint megfelelnek a kitűzött elvárásoknak.

Érdemes lehet a terület további vizsgálata más anyagokkal is, amelyek ellenállnak a vegyi hatásoknak és az időjárásnak. Egy-egy ilyen típus akár hosszú tárolási időt is elviselhet szerkezeti károsodás nélkül.

Más tekintetben lehetőség van a töltetházak kialakításában további alkatelemek beillesztésére, mint az úgynevezett inert lencse. Ennek a szakszerű pozicionálása komoly technológiai feladat, de a töltet hatékonyságában jelentős szerepe lehet. Továbbá érdemes megvizsgálni a zárókupak rögzítése csavarmenetes vagy bajonettzáras kialakításának lehetőségeit is.

Véleményünk szerint a fenti tapasztalatok jó alapot biztosítanak az eljárás beemelésére a katonai felsőoktatásba, amennyiben a technikai lehetőségek széles körben adottak lesznek a feladathoz.

Felhasznált irodalom

Boda József – Boldizsár Gábor – Kovács László – Orosz Zoltán – Padányi József – Resperger István – Szenes Zoltán: A hadtudományi kutatási irányok, prioritások és témakörök. *Államtudományi Műhelytanulmányok,* (2016), 16. 1–23. Online: www.med.u-szeged.hu/download.php?docID=90702

Daruka Norbert: Robbanóanyag-ipari alapanyagok és termékek osztályozásának lehetőségei. *Műszaki Katonai Közlöny,* 26. (2016), 1. 26–43. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2016_1_03_Robbanoanyag-ipari%20alapanyagok.pdf

FreeDee: *SLS nyomtatás (szelektív lézerszinterezés) útmutató*. (é. n.) Online: www.freedee.hu/sls-nyomtatas-szelektiv-lezerszinterezes-utmutato/

Kovács Zoltán: Gondolatok a műszaki támogatás és a műszaki zárás alapjairól. *Nemzetvédelmi Egyetemi Közlemények,* 6. (2002), 1. 30–46.

Kugyela Lóránd: A többkomponensű robbanóanyagok múltja, jelene és jövője. *Katonai Logisztika,* 28. (2020), 4. 58–75. Online: https://doi.org/10.30583/2020.4.058

Lukács László: *Szemelvények a magyar robbantástechnika fejlődéstörténetéből. Különös tekintettel a továbbfejlesztés várható irányaira és a kor új kihívásaira.* Budapest, Dialóg Campus Kiadó, 2017.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

17. évfolyam (2022) 3. szám 45–57.
DOI: 10.32567/hm.2022.3.3

Almási Csaba,[1] Cimer Zsolt[2]

Szénhidrogén-gázkeveréket küldeménydarabban szállító közúti jármű biztonsági kockázatának értékelése

Security Risk Assessment of a Road Vehicle Carrying a Hydrocarbon Gas Mixture in a Package

A veszélyesáru-szállítás szigorú, nemzetközi szabályokhoz kötött. A veszélyes áru közúti szállításának szigorú szabályozása több szempontból is kiemelt jelentőségű, mivel egy esetleges közúti baleset során a veszélyes anyag szabadba kerülésével jelentős méretű veszélyeztetett terület alakulhat ki. Másrészt a veszélyes áru tulajdonságait kihasználva, a lakott területeken áthaladó veszélyesáru-szállítmány potenciális célpontja lehet egy esetleges terrorcselekménynek. Az ilyen típusú kockázat csökkentésére a veszélyesáru-szállítási szabályzatokban külön rendelkezések vonatkoznak, azonban előfordulhat, hogy ezeket az intézkedéseket a szűkebb gazdasági, társadalmi és biztonsági környezet sajátosságaihoz érdemes igazítani. A publikációban a szerzők küldeménydarabban való szállítás esetén a visszaélés elleni rendelkezések hatálya alól mentesülő, propán-bután gázszállítmány elleni szándékos cselekmény következményeit vizsgálják meg szoftveres kockázatelemzés segítségével.

Kulcsszavak: **ADR, iparbiztonság, közúti veszélyesáru-szállítás, közbiztonsági előírások, terrorcselekmény, küldeménydarab, UN 1965 szénhidrogén-gázkeverék, cseppfolyósított, m.n.n. (A1 keverék)**

Transport of dangerous goods is committed to strict, international regulations. The strict regulation of transport of dangerous goods by road has a high importance, since

[1] Doktorandusz, tanársegéd, Nemzeti Közszolgálati Egyetem, e-mail: almasi.csaba@uni-nke.hu
[2] PhD, egyetemi docens, oktatási dékánhelyettes, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

by releasing hazardous materials during a road accident could create a potentially large area of risk. On the other hand, the dangerous shipment passing through inhabited areas can be a potential target of a terrorist attack by utilising the properties of dangerous goods. There are specific provisions in the dangerous goods transport regulations to reduce this type of risk, but these measures may need to be adapted to the specificities of the narrower economic, social and safety context. In this publication, the authors examine the consequences of an intentional act against a packaged shipment of propane-butane gas exempted from security provisions, by using software risk analysis.

Keywords: **ADR, industrial safety, transport of dangerous goods by road, security provisions, terrorist attack, package, UN 1965 hydrocarbon gas mixture (A1 mixture), liquefied, n. o.s.**

1. Bevezetés

A közúti veszélyesáru-szállítás a *Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás*, közismert néven az ADR (*Agreement Concerning the International Carriage of Dangerous Goods by Road,* ADR) szerint történik. Az ADR Megállapodást 1957. szeptember 30-án Genfben kötötték, 1968. január 29-én lépett hatályba, s Magyarország 1979-ben csatlakozott hozzá.

A 2001. szeptember 11-i terrortámadások rávilágítottak arra, hogy a közlekedési eszközök terrorcselekmény során potenciális fegyverként alkalmazhatók. A biztonsági kihívásra válaszul, az ENSZ Gazdasági és Szociális Tanácsa az ENSZ modellszabályozásokba épített olyan rendelkezéseket, amelyek terrorista cselekmények megelőzését segítik elő. Az előírások 2005-től, az ENSZ modellszabályozások, más néven a *Narancssárga könyv* alapján az ADR 1.10 fejezetként is megjelenik, *Közbiztonsági előírások* fejezetcímmel. A közbiztonsági előírások célja a veszélyes áru jogosulatlan birtokba kerülésének, a visszaélés, különös tekintettel a terrorcselekmény során való alkalmazhatóság megakadályozása.

A szigorú szabályozás ellenére az elmúlt évtizedben bekövetkezett terrorcselekmények rávilágítanak a témakör jelentőségére.

Megítélésünk szerint a kockázat nem csökkent, a közbiztonsági előírásokat folyamatosan vizsgálni és értékelni kell. A továbbiakban megvizsgáljuk a cseppfolyós szénhidrogén-gázkeverék (propán-bután gáz) küldeménydarabos szállítási módban való kiszabadulásának következményeit. A fenti gyúlékony gáznak ezt a szállítási módját jelenleg nem kell figyelembe venni a közbiztonsági tervezés szempontjából, ebben a formában mentesül az előírások alól. Az ilyen szállítmányok azonban igen gyakoriak hazánkban, ezért rá kívánjuk irányítani a figyelmet, hogy indokolt lehet a szabályozást a szűkebb gazdasági, társadalmi és biztonsági környezet sajátosságaihoz igazítani.

2. A közbiztonsági tervezés elhelyezkedése a nemzetközi és hazai jogi normarendszerben

Az Európai Parlament és a Tanács 2008/68/EK irányelve (2008. szeptember 24.) a veszélyes áruk szárazföldi szállításáról a veszélyes áruk uniós országokon belüli és azok közötti, biztonságos közúti, vasúti vagy belvízi szállítására vonatkozó közös szabályokat állapít meg. A szabályozás kitér a be- és kirakodás folyamatára, a más szállítóeszközről és a más szállítóeszközre való átrakásra, a szállítás során szükségessé váló egy helyben tartózkodásra. Az irányelv mellékleteiben található hivatkozás utal a veszélyesáru-szállítás alapszabályzóira, többek között az ADR-re.[3]

Annak érdekében, hogy a veszélyesáru-szállítás az Európai Unión belül azonos feltételekkel valósuljon meg, a jogszabály hatálya az országhatárokon belüli szállításra is kiterjed, azzal a kitétellel, hogy az uniós országok jogosultak arra is, hogy saját területükre vonatkozóan különös biztonsági követelményeket írjanak elő a veszélyes áruk országhatáron belüli és nemzetközi szállítására. Ilyen különös biztonsági szabály lehet például az útvonalak, tartózkodási helyek kijelölése.[4]

Az ADR naprakészen tartása folyamatos, ami azt jelenti, hogy a tudományos, illetve a technológiai fejlődés eredményei, az új környezeti kihívások beépülnek a kétévente frissülő szabályozásba.

A terrorizmus általi fenyegetettséggel, a veszélyes áru erőszakos cselekedetre való felhasználási lehetőségével mint új környezeti kihívással az ADR a 2000-es évek közepén kezdett el foglalkozni. 2005-től a veszélyesáru-szállítás nemzetközi szabályzatok kiegészültek közbiztonsági előírásokkal, amelyek célja, hogy lehetetlenné tegyék veszélyes áru jogosulatlan birtokba kerülését és terrorcselekményekben való felhasználhatóságát.[5]

Az ENSZ modellszabályozások alapján, 2005-től az ADR-ben is megjelenő 1.10 fejezet fogalommeghatározása szerint: „A nagy közbiztonsági kockázattal járó veszélyes áruk azok, amelyekkel terrorista cselekmények során vissza lehet élni, ami súlyos következményekkel járhat, pl. tömeges balesetet vagy tömegpusztítást idézhet elő, vagy – különösen a 7 osztály estében – súlyos társadalmi-gazdasági zavart okozhat."[6]

Az ADR 1.10 fejezet meghatározza azoknak az áruknak és szállítási módoknak a körét, amelyek közbiztonsági terv készítésére kötelezettek. A 1.10.3.2.1 pont szerint a nagy közbiztonsági kockázattal járó veszélyes áruk, vagy radioaktív anyagok szállításában részt vevő szállítóknak, fuvarozóknak, feladóknak és többi résztvevőnek közbiztonsági tervet kell készíteniük, bevezetniük és annak megfelelően eljárniuk.

[3] Veszélyes áruk szárazföldi szállítása. 2008/68/EK irányelv a veszélyes áruk szárazföldi szállításáról.
[4] 2008/68/EK irányelv a veszélyes áruk szárazföldi szállításáról.
[5] Kátai-Urbán Lajos – Vass Gyula: Veszélyes üzemek és szállítmányok biztonsága Magyarországon. *Védelem Tudomány,* 4. (2019), 1. 45–82.
[6] ADR 1.10.3.1.1 pont, A nagy közbiztonsági kockázattal járó veszélyes áruk meghatározása, 387/2021. (VI. 30.) Korm. rendelet a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről, 1. melléklet.

A közbiztonsági előírások gyakorlati bevezetésére és alkalmazására 11 szervezetet tömörítő, ipari szakértői munkacsoport dolgozott ki iránymutatást „Veszélyes áruk közúti szállításának közbiztonsági előírásaira vonatkozó ipari irányelvek"[7] *(Industry Guidelines for the Security of the Transport of Dangerous Goods by Road)* címen. A műszaki ajánlás első kiadása 2005 áprilisában jelent meg, az utolsó felülvizsgálat időpontja 2016. Az ajánlás az ADR-ben folyamatosan bekövetkező változásokhoz nem teljeskörűen illeszkedik, a harmonizáción az ipari szakértői munkacsoport folyamatosan dolgozik.

Magyarországon az ADR végrehajtásáról ma a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről szóló 387/2021. (VI. 30.) Korm. rendelet van hatályban. További kiegészítéseket tartalmaz a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás (ADR) „A" és „B" Mellékletének belföldi alkalmazásáról szóló 39/2021. (VII. 30.) ITM rendelet.

3. Közbiztonsági előírások veszélyes áru közúti szállítása során

Az ADR tartalmaz a veszélyes áru biztonságos közúti szállítása érdekében általános érvényű előírásokat. Ezek az előírások kiterjednek a szállítást végző személy azonosítására, képzettségére, valamint az átmeneti tárolással szembeni elvárásokra. A szállítási folyamatban részt vevő egyes szereplők – feladó, címzett, csomagoló, töltő stb. – más-más tevékenységet végeznek, más-más felelősségük van, így a közbiztonsági követelményeknek is eltérően kell jelentkezniük.

Az ADR külön szakasza foglalkozik az úgynevezett nagy közbiztonsági kockázattal járó veszélyes áruk meghatározásával. Az ADR alapján nagy közbiztonsági kockázattal járó veszélyes áruk azok, amelyekkel terrorista cselekmények során vissza lehet élni, ami súlyos következményekkel járhat, például tömeges balesetet vagy tömegpusztítást idézhet elő, vagy – különösen a 7 osztály estében – súlyos társadalmi-gazdasági zavart okozhat.[8] A nagy közbiztonsági kockázattal járó veszélyes árukat és a hozzájuk rendelt mennyiségeket az 1. táblázat mutatja be. Gyúlékony, nem mérgező gázok esetében, amely csoportba tartozik jelen vizsgálat tárgyát képező propán-bután gázkeverék is, az ADR 1.10.3.1.2 „b"-megjegyzés értelmében az 1.10.3 szakasz előírásait nem kell alkalmazni, a szállított mennyiségtől függetlenül.

[7] Almási Csaba ford. Az angol „security" szót a magyar nyelvű ADR 1.10 „közbiztonság"-ként, mint terminust alkalmazza. Az „Ipari irányelvek veszélyes áruk biztonságos közúti szállítására" nem tükrözné kellően a szöveg témáját, és nem állna összhangban az alapterminológiával.

[8] ADR 1.10.3.1.1 pont, A nagy közbiztonsági kockázattal járó veszélyes áruk meghatározása, 387/2021. (VI. 30.) Korm. rendelet a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről, 1. melléklet.

1. táblázat: A nagy közbiztonsági kockázattal járó veszélyes áruk

Osztály	Alosztály	Anyag vagy tárgy	Mennyiség		
			Tartányban (l)[c)]	Ömlesztve (kg)[d)]	Küldemény-darabban (kg)
1	1.1	Robbanóanyagok és -tárgyak	a)	a)	0
	1.2	Robbanóanyagok és -tárgyak	a)	a)	0
	1.3	Összeférhetőségi csoportba tartozó robbanóanyagok és -tárgyak	a)	a)	0
	1.4	UN 0104, 0237, 0255, 0267, 0289, 0361, 0365,0366,0440, 0441,0455,0456,0500, 0512 és 0513 alá tartozó robbanótárgyak	a)	a)	0
	1.5	Robbanóanyagok	0	a)	0
	1.6	Robbanótárgyak	a)	a)	0
2		Gyúlékony, nem mérgező gázok (a csak F betűt vagy csak FC betűket tartalmazó osztályozási kódok)	3000	a)	b)
		Mérgező gázok (T, TF, TC, TO, TFC vagy TOC betűket tartalmazó osztályozási kódok), az aeroszolok kivételével	0	a)	0
3		I és II csomagolasi csoportba tartozó gyúlékony folyékony anyagok	3000	a)	b)
		Érzéketlenített robbanóanyagok	0	a)	0
4.1		Érzéketlenített robbanóanyagok	a)	a)	0
4.2		I csomagolási csoportba tartozó anyagok	3000	a)	b)
4.3		I csomagolási csoportba tartozó anyagok	3000	a)	b)
5.1		I csomagolási csoportba tartozó, gyújtóhatású, folyékony anyagok	3000	a)	b)
		Perklorátok, ammónium-nitrát, ammónium-nitrát műtrágyák és ammónium-nitrát emulziók, szuszpenziók vagy gélek	3000	3000	b)
6.1		I csomagolási csoportba tartozó mérgező anyagok	0	a)	0
6.2		„A" kategóriába tartozó fertőző anyagok (UN 2814 es 2900, az állati eredetű anyagok kivételével) és ,,A" kategóriába tartozó gyógyászati hulladékok (UN 3549)	a)	0	0
7		I csomagolási csoportba tartozó maró anyagok	3000	a)	b)

Forrás: 387/2021. (VI. 30.) Korm. rendelet, 1. melléklet, 92.

A 7 osztályba tartozó veszélyes áruk közül nagy közbiztonsági kockázattal járó radioaktív anyagok azok, amelyeknél egy küldeménydarab aktivitása eléri vagy meghaladja a 3000A2 szállítási közbiztonsági küszöbértéket, kivéve az egyéb küszöbértékkel ellátott radionuklidokat. Az egyes radionuklidokra vonatkozó szállítási közbiztonsági küszöbértéket a 2. táblázat mutatja be:

2. táblázat: A nagy közbiztonsági kockázattal járó radioaktív anyagok

Elem	**Radionuklid**	**Szállítási, közbiztonsági küszöbérték (TBq)**
Americium	Am-241	0,6
Arany	Au-198	2
Kadmium	Cd-109	200
Kalifornium	Cf-252	0,2
Kürium	Cm-244	0,5
Kobalt	Co-57	7
Kobalt	Co-60	0,3
Cézium	Cs-137	1
Vas	Fe-55	8000
Germanium	Ge-68	7
Gadolinium	Gd-153	10
Iridium	lr-192	0,8
Nikkel	Ni-63	600
Palládium	Pd-103	900
Prometium	Pm-147	400
Polónium	Po-210	0,6
Plutónium	Pu-238	0,6
Plutónium	Pu-239	0,6
Rádium	Ra-226	0,4
Rutenium	Ru-106	3
Szelén	Se-75	2
Stroncium	Sr-90	10
Tallium	Tl-204	200
Tulium	Tm-170	200
ltterbium	Yb-169	3

Forrás: 387/2021. (VI. 30.) Korm. rendelet, 1. melléklet, 93.

A nagy közbiztonsági kockázattal járó veszélyes áruk szállításában érintett szereplőknek úgynevezett közbiztonsági tervet kell készíteniük és a szerint eljárniuk.[9] A közbiztonsági terv kötelező tartalmi elemei:

- a közbiztonsági rendszabályokért és óvintézkedésekért viselt felelősség részletes megosztása megfelelő hatáskörrel és képesítéssel rendelkező személyek között;

[9] Kátai-Urbán Lajos – Kozma Sándor – Vass Gyula: Veszélyes szállítmányok felügyeletével kapcsolatos jog- és intézményfejlesztési tapasztalatok értékelése. *Hadmérnök,* 10. (2015), 3. 92–108.

- az érintett veszélyes áruk, illetve veszélyesáru-fajták nyilvántartása;
- a folyamatban levő tevékenységek felülvizsgálata és a közbiztonsági kockázat értékelése, beleértve a szállítási műveletek szükség szerinti megszakítását, a veszélyes áruk járművön, tartányban vagy konténerben tartását a szállítás előtt, alatt és után, illetve a veszélyes áruk átmeneti tárolását az intermodális szállítás vagy az egységek közötti átrakás során;
- a résztvevők felelősségével és feladatával arányban álló intézkedések egyértelmű meghatározása, amelyeket a közbiztonsági kockázat csökkentéséhez meg kell tenni, beleértve:
  - a képzést;
  - a közbiztonsági eljárásokat (például teendők súlyos fenyegetettség esetén; új, illetve áthelyezett alkalmazottak ellenőrzése stb.);
  - az üzemi eljárásokat (például útvonalak kiválasztása/használata, ahol ismeretes; hozzáférés a veszélyes árukhoz az átmeneti tárolóhelyeken [mint azt a c) pont meghatározza]; érzékeny infrastruktúra közelsége stb.];
  - a közbiztonsági kockázat csökkentéséhez használandó eszközöket és forrásokat;
- hatékony, naprakész eljárások a közbiztonsági fenyegetettség, a közbiztonság megsértése, illetve a közbiztonságot érintő rendkívüli események kezelésére és jelentésére;
- a közbiztonsági terv értékelésére, ellenőrzésére, valamint a rendszeres felülvizsgálatára és korszerűsítésére vonatkozó eljárás;
- a közbiztonsági tervben szereplő szállítási információk fizikai védelmének biztosítására szolgáló intézkedések;
- intézkedések annak biztosítására, hogy a közbiztonsági tervben szereplő szállítási információkhoz csak az érdekeltek juthassanak hozzá. Ezek az intézkedések azonban nem akadályozhatják az ADR-ben máshol előírt információk megadását.[10]

A veszélyes áru szállítási baleset, egyéb rendkívüli események eredményeként a minősített csomaglóeszközben tárolt veszélyes anyag a szabadba kerülhet. A veszélyes anyag tulajdonságaitól függően különböző hatásokkal kell számolni, többek között mérgező felhő terjedésével, tűzzel, robbanással, egyéb környezeti veszélyeztetéssel, így amennyiben az esemény lakott területen történik, nem zárható ki a lakosság jelentős számú elhalálozása sem.[11]

4. Közbiztonsági előírások értékelése

Az ADR a közbiztonság megőrzésére vonatkozó általános előírásokkal, a nagy közbiztonsági kockázattal járó veszélyes áruk és radioaktív anyagok azonosításával, valamint a közbiztonsági terv készítésére és alkalmazására vonatkozó szabályozással a veszélyes

[10] A nagy közbiztonsági kockázattal járó veszélyes áruk meghatározása, 387/2021. (VI. 30.) Korm. rendelet, 1. melléklet.

[11] Kátai-Urbán Lajos: *Habilitációs Tézisek veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény- és eszközrendszer fejlesztése Magyarországon.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

áru illetéktelen, terrorcélú felhasználási lehetőségét jelentősen csökkentette. A nagy közbiztonsági kockázattal járó veszélyes árukhoz való illetéktelen hozzáférés nehezebbé vált, ahogy a lakott területre való bejuttatás is.

Ugyanakkor, megítélésünk szerint, a szabályozás, a nagy közbiztonsági kockázattal járó veszélyes áruk és a vonatkozó küszöbértékek újragondolása szükséges, amit az alábbi példán keresztül kívánunk bemutatni.

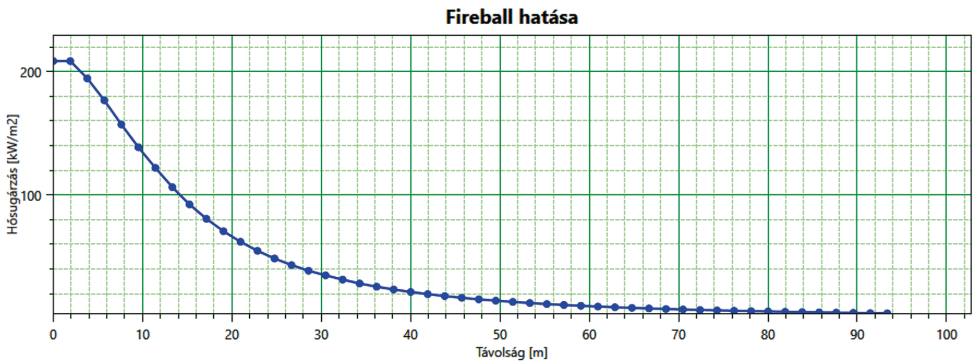
A propán-bután gázkeverék az ADR az UN 1965-tétel és 2F osztályozási kód alatt, a cseppfolyósított szénhidrogén-gázkeverékhez sorolja (A1 keverék), amely gyúlékony gáz. Az A01 gázkeverék gőznyomása 70 °C-on nem haladja meg az 1,6 MPa-t (16 bar-t), és sűrűsége 50 °C-on 0,516 kg/l-nél nem kisebb.[12] A propán-bután így az ADR szerint nagy közbiztonsági kockázattal járó – „gyúlékony, nem mérgező gázok" – veszélyes árunak minősül, ugyanakkor küldeménydarabos szállítás esetén a nagy közbiztonsági kockázattal járó veszélyes árukra vonatkozó előírásokat nem kell alkalmazni. A propán-bután küldeménydarabos szállítás jellemzően gázszállító palettában történik, amelyben általában 16 db palack van. A szállítását az 1. ábra szemlélteti.

1. ábra: Propán-bután gázkeverék küldeménydarabos szállítása
Forrás: https://adoc.pub/queue/hirlevel-december-2-oldal-kszto-3-oldal-kereskedelmi-hirek-.html

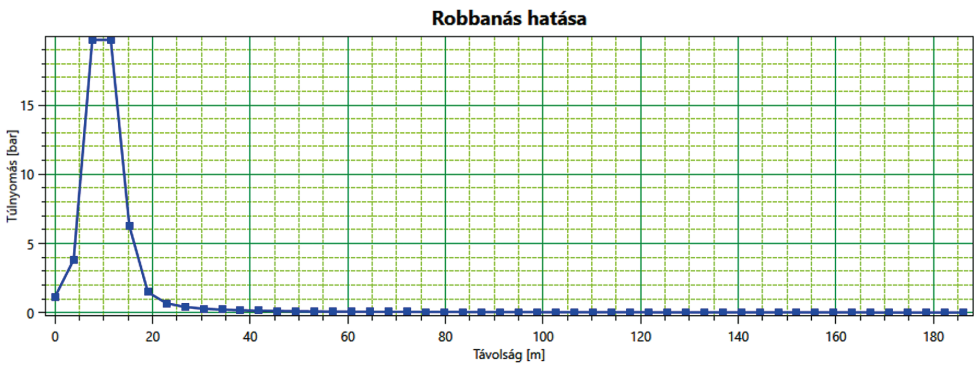
Bár a küldeménydarabos csomagolással egy esetleges rendkívüli esemény során a szabadba kerülhető veszélyes anyag mennyisége maximalizálva van, de jelen esetben nem zárható ki, hogy dominóhatás következtében, vagy egy külső inicializálás eredményeként a palettán lévő palackok közel azonos időben sérüljenek, így a hatások

[12] ADR 2.2.2.3 bekezdés, A gyűjtőmegnevezések felsorolása, 387/2021. (VI. 30.) Korm. rendelet, 1. melléklet.

nem eltolódva, hanem összegződve jelentkezhetnek. Feltételezve, hogy külső szándékos hatás következtében a 16 db 11,5 kg-os palack közel egy időben, pillanatszerűen sérül, elsősorban *fireball* és robbanás következhet be. A következmények a 2. ábra szerinti hősugárzás–távolság és a 3. ábra szerinti túlnyomás–távolság diagramokkal jellemezhetők.

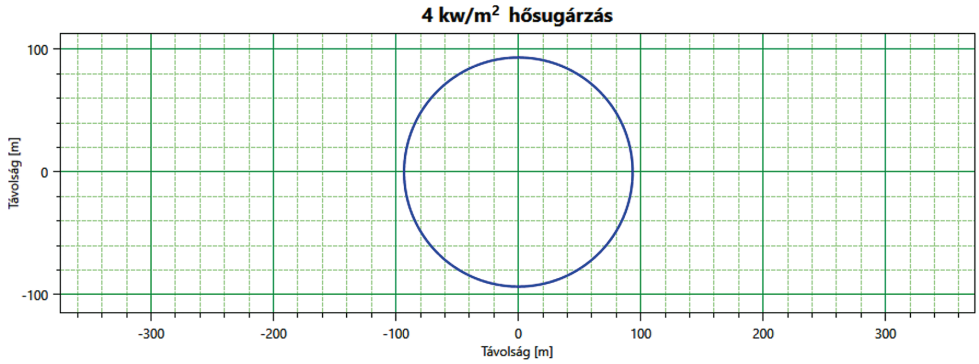


2. ábra: Fireball hatása
Forrás: a szerzők szerkesztése

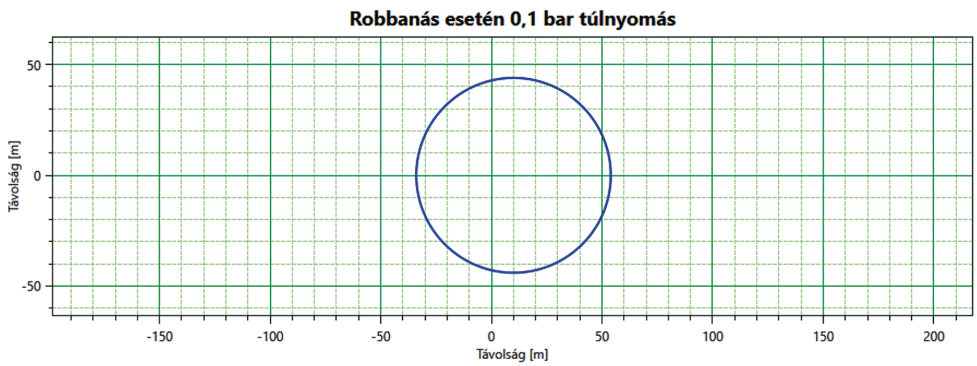


3. ábra: Robbanás hatása
Forrás: a szerzők szerkesztése

Amennyiben egy személy 20 másodpercig 4 kw/m^2 hősugárzásnak van kitéve, égési sérülésekkel, 0,1 bar értéknél nagyobb nyomásnál elhalálozással kell számolni. Fireball esetén – a 4. ábrának megfelelően – körülbelül 100 m sugarú övezeten belül kell sérüléssel számolni robbanáskor.

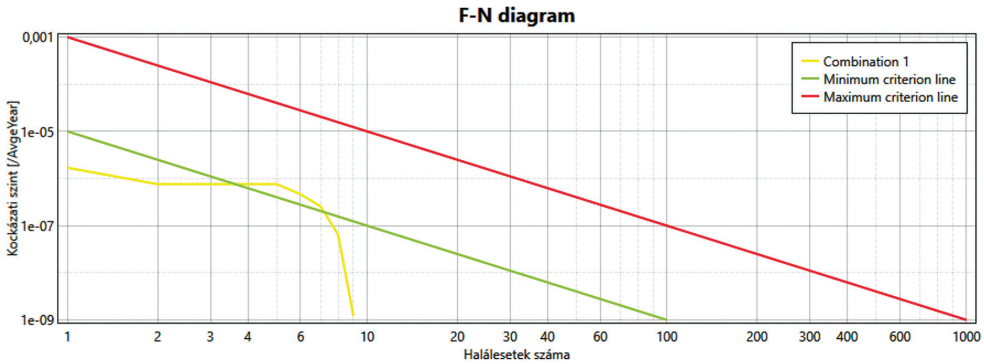


4. ábra: Fireball esetén 4 kw/m² hősugárzás övezete
Forrás: a szerzők szerkesztése



5. ábra: Robbanás esetén 0,1 bar túlnyomás övezete
Forrás: a szerzők szerkesztése

Amennyiben feltételezzük, hogy a szállítmány lakott területen belül volt, és a népesség sűrűsége 100 fő/ha, valamint az esemény gyakorisága 10^{-5} esemény/év értékű (egy atmoszférikus tartály sérülésének gyakoriságával közel egyenlő), akkor a társadalmi kockázat meghatározható. A társadalmi kockázatot ábrázoló diagram x tengelye a halálozások számát jelöli logaritmikus skálán, az y tengelye az N vagy annál több ember halálával járó balesetek összegzett gyakoriságát jelenti. A társadalmi kockázatot a 6. ábra mutatja be, ahol a sárga görbe a számított értéket, a zöld egyenes a feltételek nélküli elfogadhatóság, a piros egyenes a feltételekkel sem elfogadható kockázat határát jelöli.



6. ábra: Társadalmi kockázat
Forrás: a szerzők szerkesztése

A veszélyes üzemekre vonatkozó elfogadhatósági feltétel „a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről" szóló 219/2011. (X. 20.) Korm. rendelet szerint:

- A társadalmi kockázat feltétel nélkül elfogadható, ha F < (10 – 5xN – 2) 1/év, ahol N ≥ 1. (Zöld egyenes alatti terület.)
- A társadalmi kockázat feltétellel fogadható el, ha minden F < (10–3xN–2) 1/év, és F > (10–5xN–2) 1/év tartomány közé esik, ahol N ≥ 1. Ebben az esetben a tevékenység kockázatának csökkentése érdekében a hatóság kötelezi az üzemeltetőt, hogy gondoskodjon olyan üzemen belüli megelőző biztonsági intézkedésekről (riasztás, egyéni védelem, elzárkózás stb.), amelyek a kockázat szintjét csökkentik. (Zöld és piros egyenes közötti terület.)
- Nem elfogadható szintű a veszélyeztetettség, ha F > (10–3xN–2) 1/év, ahol N ≥ 1. Ebben az esetben, ha a kockázat más eszközökkel nem csökkenthető, a hatóság kötelezi az üzemeltetőt a tevékenység korlátozására vagy megszüntetésére. (Piros egyenes feletti terület.)

A számított társadalmi kockázat – sárga görbe – átnyúlik a feltétellel fogadható el tartományba, ezért kockázatcsökkentő intézkedés megtétele szükséges. A számítás eredményeit súlyosbítja, hogy a halálozást okozható repeszhatást a modellezésnél nem vették figyelembe. A feltételezett esemény reálisnak tekinthető, hiszen egy benzinkútra való PB-palack-szállítás, a szállítmány ideiglenes parkoltatása lakott területen senkinek sem tűnik fel.

A társadalmi kockázatot csökkentő intézkedés lehet többek között a közbiztonsági terv kidolgozása és az abban foglaltak alkalmazása, vagy útvonal-kijelölés alkalmazása.

5. Következtetések, összegzés

Veszélyes áruk szállítása valamennyi közlekedési ágazatban többletveszélyt jelent, azonban a statisztikák és az egyes közlekedési ágak baleseti kockázatának értékeléséből az a következtetés vonható le, hogy a legnagyobb veszélyeztetést a közúti árutovábbítás jelenti.[13]

A katasztrófavédelmi iparbiztonsági szakterület egyik fő feladata a veszélyesáru-szállítási tevékenység lehető legmagasabb fokú biztonságának garantálása is.[14]

A veszélyes áruk szállításának szabályozása során külön figyelmet kell fordítani a szállítmány terrorcselekményekként való alkalmazhatóságának megelőzésére, amelyre már kialakult a jó gyakorlat. Ugyanakkor a szabályozás nem teljes körű, megítélésünk szerint újragondolás szükséges, amelyet példával is alátámasztottunk.

A közbiztonságra vonatkozó szabályozás újragondolásánál javasolt a nagy közbiztonsági kockázattal járó veszélyes áruk körének kiegészítése, illetve a kapcsolódó küszöbmennyiségek módosítása.

A lakosság védelme érdekében a közbiztonságra vonatkozó szabályozás újragondolásán túl indokolttá válhat a veszélyesáru-szállítmányok útvonal-kijelölésére vonatkozó nemzeti szintű metodika kidolgozása és alkalmazása.

Felhasznált irodalom

Hoffmann Imre – Kátai-Urbán Lajos – Lévai Zoltán – Vass Gyula: *Iparbiztonsági kockázatok Magyarországon.* Védelem Online, Tűz- és katasztrófavédelmi szakkönyvtár, 2015. Online: www.vedelem.hu/letoltes/anyagok/546-iparbiztonsagi-kockazatok-magyarorszagon.pdf

Industry Guidelines for the Security of the Transport of Dangerous Goods by Road (2016. december). Online: https://cefic.org/app/uploads/2018/12/Guidelines-for-the-security-of-the-transport-of-dangerous-goods-by-road-2016-GUIDELINES-ROAD.pdf

Kátai-Urbán Lajos: *Habilitációs Tézisek veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény- és eszközrendszer fejlesztése Magyarországon.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Kátai-Urbán Lajos – Kozma Sándor – Vass Gyula: Veszélyes szállítmányok felügyeletével kapcsolatos jog- és intézményfejlesztési tapasztalatok értékelése. *Hadmérnök,* 10. (2015), 3. 92–108. Online: http://hadmernok.hu/153_08_katayul_ks_vgy.pdf

Kátai-Urbán Lajos – Vass Gyula: Veszélyes üzemek és szállítmányok biztonsága Magyarországon. *Védelem Tudomány,* 4. (2019), 1. 45–82. Online: http://vedelemtudomany.hu/articles/03-katai-vass.pdf

[13] Hoffmann Imre et al.: *Iparbiztonsági kockázatok Magyarországon.* Védelem Online, Tűz- és katasztrófavédelmi szakkönyvtár, 2015.

[14] Német Alexandra – Kátai Urbán Lajos – Vass Gyula: Veszélyes tevékenységek biztonsága a fenntarthatóság jegyében. *Védelem Tudomány,* 5. (2020), 1. 137–152.

Német Alexandra – Kátai Urbán Lajos – Vass Gyula: Veszélyes tevékenységek biztonsága a fenntarthatóság jegyében. *Védelem Tudomány,* 5. (2020), 1. 137–152. Online: www.vedelemtudomany.hu/articles/09-nemet-katai-vass.pdf

Jogi források

387/2021. (VI. 30.) Korm. rendelet a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről, 1. melléklet. Online: https://njt.hu/jogszabaly/2021-387-20-22

Veszélyes áruk szárazföldi szállítása. 2008/68/EK irányelv a veszélyes áruk szárazföldi szállításáról. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=-LEGISSUM%3Atr0006

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

17. évfolyam (2022) 3. szám 59–69.
DOI: 10.32567/hm.2022.3.4

Horváth Lilla[1]

Tűzoltólaktanya munkavédelmi szemmel

Fire Station Barracks from an Occupational Health and Safety Perspective

A tűzoltólaktanyák kialakítása és fenntartása során a munkavédelmi szabályok betartása kiemelt jelentőségű. Központi kérdés az állomány biztonságának és munkavégző képességének megóvása, élet- és vagyonvédelmi szempontból is. A rendszeres munkavédelmi ellenőrzések alkalmával tárhatók fel a működőképességet veszélyeztető hiányosságok, így általuk a munkáltatónak lehetősége nyílik azok kijavítására, hogy egy esetleges baleset elkerülhető legyen. A szerző jelen cikkel, többéves tapasztalatait összegyűjtve, betekintést enged az olvasó számára a tűzoltólaktanyák munkavédelmi szempontú előírásait illetően, továbbá rövid kitérőt tesz az oktatás területére, mivel a munkavédelem szerves részét képezi az állomány rendszeres szakmai képzése is. Végül néhány javaslatot kínál a laktanyákon belül betartandó munkavédelmi szabályokról és kialakításokról.

Kulcsszavak: **munkavédelem, tűzoltólaktanya, prevenció, oktatás, biztonság**

Adherence to occupational safety regulations is of paramount importance in case of design and maintenance of fire station barracks. A key issue is the safe intervention and the preservation of the work capacity both in terms of protection of life and property. Regular safety inspections can reveal deficiencies that endanger functionality, so that the employer has the opportunity to correct them in order to avoid a possible accident. The author, gathering her many years of experience, gives the reader an insight into the occupational safety regulations of fire station barracks, and also makes a short detour in the field of education, as regular professional training of the staff is also an integral part of occupational safety and health. Finally, the author offers some suggestions on occupational safety rules and designs within fire departments.

Keywords: **occupational health and safety, fire station barracks, prevention, education, safety**

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: horvath.lilla@katved.gov.hu

1. Bevezetés

A „munkavédelem" fogalma sokak számára láthatatlan mindaddig, amíg baleset vagy tragédia nem történik. Ekkor válik világossá, hogy komplex szakterületről beszélhetünk, amelynek célja a prevenció, azaz a megelőzés. Ezt Magyarország Alaptörvénye is rögzíti a XVII. cikk (3) bekezdése szerint, azaz: „Minden munkavállalónak joga van az egészségét, biztonságát és méltóságát tiszteletben tartó munkafeltételekhez." A megelőzés során nemcsak a munkáltató vállal szerepet, hanem a munkavállaló is, így kialakítva egy kölcsönösségen alapuló rendszert.[2]

A beavatkozó tűzoltók úgynevezett 24/48 órás készenléti jellegű szolgálati beosztásban látják el szolgálati feladataikat. Ez azt jelenti, hogy 24 órában a szolgálati helyükön tartózkodnak, riasztás esetén pedig onnan közelítik meg egyéni védőfelszerelésben, tűzoltó gépjárműfecskendővel a kárhelyszínt. Ha nincs ilyen esemény, az nem azt jelenti, hogy semmittevéssel töltik a szolgálati idejüket. Ez idő alatt különböző foglalkozások, napi továbbképzések, tűzoltósági szakterület által tartandó gyakorlatok, például felkészítő gyakorlatok, ezen belül tűzoltótechnika-kezelő gyakorlatok,[3] kiképzési feladatok elé néznek, továbbá testi és lelki egészségük megőrzéséhez és fejlesztéséhez sportfoglalkozásokon vesznek részt.[4]

A biztonságos munkahely kialakítása során számos szempontot kell figyelembe venni, nem elhanyagolva azt, hogy egyes tényezők összefüggésben is vannak egymással. Az egészséget nem veszélyeztető és biztonságos munkavégzés feltételeinek megteremtéséhez szakmai álláspontom alapján az alábbi tényezők játszanak kulcsszerepet (a teljesség igénye nélkül):

- közlekedési és menekülési útvonalak;
- természetes és mesterséges szellőztetés, szellőzés;
- természetes és mesterséges világítás;
- hőmérséklet, páratartalom;
- ivóvíz, csatornázás;
- kémiai, biológiai tényezők.[5]

Mindezen körülmények biztosításához – még a használatbavétel előtt – a munkabiztonsági és munkaegészségügyi szakember elkészíti a kockázatértékelést, amelyben legalább az alábbiakat dokumentálják:

„a) a kockázatértékelés időpontja, helye és tárgya, az értékelést végző azonosító adatai;
b) a veszélyek azonosítása;
c) a veszélyeztetettek azonosítása, az érintettek száma;
d) a kockázatot súlyosbító tényezők;
e) a kockázatok minőségi, illetőleg mennyiségi értékelése, a fennálló helyzettel való összevetés alapján annak megállapítása, hogy a körülmények megfelelnek-e

[2] Varga László (szerk.): *A munkavédelmi törvény magyarázata.* Budapest, KJK-Kerszöv, 2005. 21–23.
[3] 53/2018. számú BM OKF főigazgatói intézkedés, 2. melléklet, 5.
[4] Hornyacsek Júlia – Vad Tibor. A tűzoltók fizikai, szellemi és pszichés terhelése. *Hadtudományi Szemle,* 4. (2011), 4. 145–146.
[5] 61/1999. (XII. 1.) EüM rendelet 2. § (1) *a)* pont értelmezése szerint.

a munkavédelemre vonatkozó szabályoknak, illetve biztosított-e a kockázatok megfelelően alacsony szinten tartása;
f) a szükséges megelőző intézkedések, a határidő és a felelősök megjelölése;
g) a kockázatértékelés elkészítésének tervezett következő időpontja;
h) az előző kockázatértékelés időpontja."[6]

A kockázatértékelésben manapság már kiemelt fontosságú a biológiai veszélyforrások és intézkedéseik felsorolása, hiszen a Covid–19 pandémiás veszélyhelyzet során nemcsak az adott laktanya állományát érintette a megbetegedés, hanem országszerte jelentett kihívást a helyzet kezelése. A már érvényben lévő kockázatértékelés bővítése során, az intézkedések meghozatalakor, közegészségügyi és járványügyi eljárásrendek és tájékoztatók alapján[7] az alábbi néhány kérdésre kellett megtalálni a szakszerű megoldást:

- Milyen eszközök és milyen összegben szükségesek a megelőzéshez, a higiénia fenntartásához (kéz- és felületfertőtlenítő, orrot és szájat elfedő maszk stb.)?
- Milyen módon és hogyan lehet kezelni a betegség (hiányzás) miatt kialakult humánerőforrás-hiányt?
- Milyen szervezési szabályokat kell hozni (például távolságtartás)?

Látható tehát, hogy a munkavédelem nem lineáris szakterület, hiszen sok más témakört is érintenie kell, hogy a munkáltatói és a munkavállalói oldalról egyaránt teljesüljenek a vonatkozó jogszabályi előírások és az ergonómiai feltételek.[8]

2. Munkavédelem

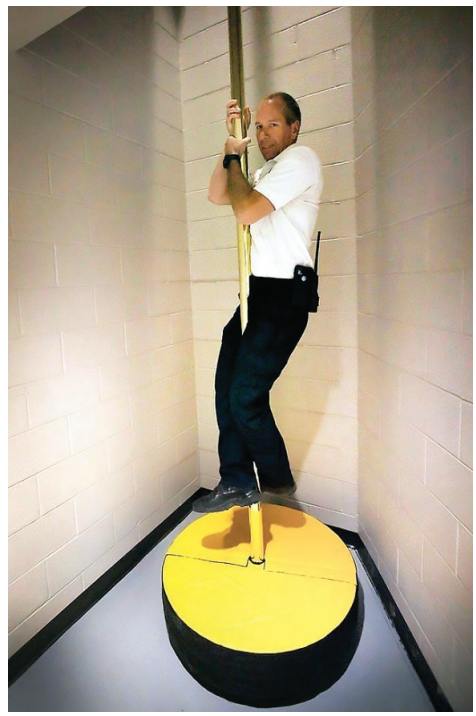
A tűzoltólaktanyák és a rendvédelmi objektumok esetén a munkavédelmi szempontú véleményezés már a tervezőasztalon megkezdődik. Erről a belügyminiszter irányítása alá tartozó rendvédelmi szervek munkavédelmi feladatai, valamint foglalkozás-egészségügyi tevékenysége ellátásának szabályairól szóló 70/2011. (XII. 30.) BM rendelet 5. § (1) *f)* és *k)* pontja rendelkezik.[9]

Bármely létesítmény, épület kialakításakor már a külső szakaszon szembesülhetünk a munkavédelmi szempontokkal. Így van ez egy tűzoltólaktanya esetén is. Ha az épület utcai homlokzata közvetlenül a közterületen lévő járda mellett van, akkor kiemelt figyelemmel kell lenni az esővíz-elvezetésre és a tetőről való hó megfogására (hófogók) a járókelők védelme érdekében. Természetesen ezt a szemléletet a laktanyához tartozó udvaron belül is szem előtt kell tartani a balesetek elkerülése végett. A téli, jegesedésre alkalmas időszakokban nem szabad elhanyagolni a különböző

[6] 1993. évi XCIII. törvény a munkavédelemről, 54. § (5) bekezdés.
[7] Nemzeti Népegészségügyi Központ: *Fertőződés elkerülése – Alapvető szabályok mindenki számára a Covid–19 vírusfertőzéssel kapcsolatban* (2020. március 16.).
[8] 1993. évi XCIII. törvény a munkavédelemről, 19. § (3) bekezdés.
[9] 70/2011. (XII. 30.) BM rendelet a belügyminiszter irányítása alá tartozó rendvédelmi szervek munkavédelmi feladatai, valamint foglalkozás-egészségügyi tevékenysége ellátásának szabályairól, 5. § (1) *f)* és *k)* pontjai.

csúszásmentesítésre alkalmas anyagok alkalmazását (homok, faforgács, környezetbarát sópótlékok stb.) az elcsúszás, elesés megakadályozásához.

A gépjárműfecskendőket és egyéb szereket tároló tűzoltószertárban található a csúszóakna, amelynek segítségével a beavatkozó tűzoltók a tűzoltóság legénységi szintjéről rövid időn belül a gépjárművekhez tudnak érkezni.[10] A csúszóakna alján, a padozaton helyezik el azt a szivacsot, amire biztonságosan megérkezhet az állomány (1. ábra).



1. ábra: Csúszóakna szivaccsal

Forrás: Mary Shinn: When Seconds Count, Durango Firefighters Hit the Brass Pole. The Durango Herald, 2019. november 3.

Lényeges, hogy ennek az anyaga olyan összetételű és keménységű legyen, ami az emberi váz- és izomrendszert sem rövid, sem pedig hosszú távon nem károsítja, eleget téve ezzel az ergonómiai szempontoknak. [11]

A hálókörletek kialakításakor számos szempontot kell figyelembe venni. A szerző álláspontja szerint javasolt az ablakok külső felületére szúnyogháló felhelyezése, hiszen az éjjeli órákban a szúnyogok, nappal pedig egyéb rovarok, például méh juthat be

[10] Alex Potter: How an Ingenious Fireman Brought a Pole Into the Firehouse. *Smithsonian Magazine,* 2020. július.

[11] 3/2002. (II. 8.) SzCsM-EüM együttes rendelet a munkahelyek munkavédelmi követelményeinek minimális szintjéről, 2. § (4) bekezdés.

a szobába, ami nemcsak a pihenéshez szükséges nyugalmat zavarhatja, hanem akár balesetveszélyes is lehet (csípés).

Az utóbbi években tapasztalható, éghajlatváltozás okozta szélsőséges időjárási események nemcsak beavatkozás közben, a káreseti környezetben hatnak a tűzoltókra. A laktanya belső tereiben, szobáiban lévő hőmérséklet az állomány teljesítőképességét, mentális állapotát, reakcióidejét nagymértékben befolyásolja.[12] Ha a laktanya homlokzata nem rendelkezik szigeteléssel, vagy nem megfelelő az árnyékolás az ablakok esetén, továbbá a mesterséges hűtés nem biztosított, akkor hosszú távon a tűzoltó nem képes magát oly mértékben kipihenni, hogy a következő beavatkozás során az elvárt teljesítményt nyújthassa. Ennek elkerülése érdekében a katasztrófavédelem minden évben korszerűsíti a meglévő laktanyáinak egy részét, az újakat pedig az energetikai követelményeknek megfelelően alakítja ki, például villamos áram egy részének biztosítása napelemek által (2. ábra).

2. ábra: Orosházi HTP megújulása

Forrás: Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság: Átépült és megújult az orosházi laktanya (2022. március 22.)

A helyiségek, kiemelten a vizesblokkok (fürdő és toalett) esetén problémát jelenthet a szellőzés hiánya, amely, ha huzamosabb ideig fennáll, akkor penészfoltok

[12] Padányi József: *Az éghajlatváltozás és a katonai erő viszonyrendszere a hazai és a nemzetközi kutatások tükrében.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 57.

megjelenéséhez vezethet, ami erősen allergén az emberi szervezetre nézve.[13] Az első generációs műanyag nyílászárók még nem rendelkeztek beépített szellőzőegységgel, így a szoba természetes szellőzése nem volt biztosított. A későbbiek során ennek megelőzése vagy megoldása érdekében kétféle megoldás adódott. Egyik esetben elszívó ventilátort építenek be, amely a páratartalom megemelkedésekor, vagy megfelelő időközönként bekapcsol, így csökkentve az adott helyiség levegőjének nedvességtartalmát. A másik esetben a műanyag ablakba utólag beépítenek egy légbevezetőt, így megvalósítva az egyenletes ablakszellőzést.

A beavatkozó állomány a tűzoltó bevetési védőruháját a laktanyán belül, ipari mosógéppel tisztítja, hiszen a személyi állomány egyéni védőeszközzel történő ellátásáról szóló 34/2021. számú Főigazgatói Intézkedés (Intézkedés) 12. pontja értelmében: „Az egyéni védőeszközöket a szerv területéről, azon kívüli munkaterületéről – a szervezett munkavégzés kivételével – csak a szerv vezetője által elrendelt, illetve engedélyezett munkavégzéshez szabad külön engedéllyel kivinni, amennyiben a közegészségügyi előírásokat nem sérti."[14]

Olyan beavatkozást követően, amely során humán vagy állati eredetű szennyeződéssel (például vér) érintkezik a tűzoltó védőruhája, nem elegendő a laktanyán belüli mosás. Az önfertőzés elkerülése végett az egyéni védőfelszereléseket úgy kell levenni, hogy a bőrfelület ne érintkezzen a ruházat külső felével. Ezt követően helyezhető el szakszerűen a bevetési védőruha speciális csomagolásba, majd azt így szállítják el a fertőtlenítőhelyre.

A védőruhák, ruhák tárolását illetően kétféle öltözőtípust lehet megkülönböztetni. Az úgynevezett fehér öltözőbe helyezik a tűzoltók az utcai, hétköznapi ruháikat. Az úgynevezett fekete öltözőbe kerülnek a beavatkozások idején használt (általában szennyezett) tűzoltó-védőruhák, amelyek minden esetben elkülönülten találhatók meg a fehér öltözőktől. Ezzel a jól bevált módszerrel az emberi szervezetet ért biológiai és kémiai veszélyforrások kockázata nagymértékben csökkenthető.

A laktanya teljes területén kiemelt fontosságú, hogy a padló burkolata ne rejtsen magában botlásveszélyt. Ha ez bekövetkezik, és a probléma azonnal nem orvosolható, első körben a terület elkerítése, megjelölése szükséges figyelemfelhívás végett. Szintkülönbségek esetén, ha az adott szakasz nem szabványos méretű (például régebbi pincelejárók), vagy az arra haladó személy akadályba ütközhet, akkor a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről szóló 2/1998. (I. 16.) MüM rendelet 11. § (1) bekezdése alapján fekete-sárga vagy vörös-fehér csíkozással szükséges megjelölni a kérdéses felületet.[15]

Az állomány egészségmegőrzése szempontjából hangsúlyos szerephez jut a kondicionálótermek állapota és felszereltsége. A helyiség bejáratához közel, jól látható helyen szükséges kihelyezni az úgynevezett „Kondicionáló terem házirendet", amelyben bármely, a terem eszközeit használó személy elolvashatja a biztonsági utasításokat és figyelmeztetéseket. Ezek közül az egyik legfontosabb, hogy minimum két embernek

[13] Ahmet Biler et al.: A Review of Performance Specifications and Studies of Trickle Vents. *Buildings,* 8. (2018), 11. 152.

[14] 34/2021. számú Főigazgatói Intézkedés a személyi állomány egyéni védőeszközzel történő ellátásáról, 12. pont.

[15] 2/1998. (I. 16.) MüM rendelet a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről, 11. § (1) bekezdés.

kell tartózkodnia egy időben a teremben, mivel egy esetlegesen bekövetkező baleset esetén a másik személy azonnal a sérült segítségére tud sietni elsősegélynyújtás okán, vagy a további sérülések elkerülése érdekében.

Ahogy otthonunkban, úgy a tűzoltólaktanyában is kellő figyelmet kell fordítani a takarító- és vegyszerek helyes tárolására, feliratozására. Általánosságban javasolt ezeket egy helyen, biztonságosan (összerendezve, elkerülendő a kiömlést) és elzárva tartani. A könnyebb felhasználás érdekében a folyékony vegyszert sok esetben nagyobb méretű kannából kisebb palackba töltik, viszont ez esetben kötelező a bárki számára jól olvasható és értelmezhető jelölés annak felületén. Ellenkező esetben előfordulhat, hogy az állomány egyik tagja összetéveszti a flakon tartalmát más iható folyadékkal, elfogyasztja, ami sérüléshez, vagy rosszabb esetben halálhoz vezethet. A vegyszerek tárolási helyén vagy ahhoz közel kell elhelyezni az úgynevezett biztonsági adatlapokat, amelyeken az esetleges baleset (például vegyszer véletlen lenyelése) bekövetkeztekor szükséges intézkedések olvashatók.[16]

A beavatkozó tűzoltók jellemzően nem képernyős munkakörben dolgoznak, a természetes és mesterséges megvilágítás mértéke számukra is meghatározó. Az újonnan átadott és felújított laktanyákban az energiatakarékossági szempontoknak megfelelő LED-fény-forrásokat szereltek be, amelyek kedvezőbb fényhatékonyságúak (lm/W), mint a hagyományos izzókkal rendelkezők.

A munkáltató kötelessége, hogy a munkavállalók munkavégzésük megkezdése előtt (előzetes), majd azt követően minden évben (ismétlő) munkavédelmi oktatásban részesüljenek. Az elméleti oktatás tananyagának többek között tartalmaznia kell (általános):

- munkahelyen előforduló veszélyek;
- munkakörrel összefüggő veszélyforrások;
- munkavállaló kötelességei és jogosultságai;
- baleset bekövetkeztekor szükséges intézkedések (például jelentési kötelezettség).

Amennyiben olyan baleset következik be a beavatkozó állomány körében, amely tanulságokkal szolgálhat, például áramütés beavatkozás során, akkor rendkívüli munkavédelmi oktatást kell tartani az esemény részletes leírásával, kielemezve, hogyan lehetett volna megelőzni az esetet. Az elméleti ismeretek elsajátítása mellett hangsúlyos szerephez jut természetesen a gyakorlati oktatás is.

A munkaeszközök használatuk során meghibásodnak, elhasználódnak, így meghatározott időközönként ellenőrizni, felülvizsgálni szükséges azokat a további biztonságos használat érdekében. Az időszakos biztonsági felülvizsgálatról a munkavédelemről szóló 1993. évi XCIII. törvény 23. § (1) bekezdése rendelkezik, amely szerint

„A biztonságos műszaki állapot megőrzése érdekében időszakos biztonsági felülvizsgálat alá kell vonni a veszélyes technológiát és a 21. § (2) bekezdésében meghatározott veszélyes munkaeszközt, továbbá azt a munkaeszközt, amelynek időszakos biztonsági felülvizsgálatát

[16] Occupational Safety and Health Administration: *Hazard Communication Standard: Safety Data Sheets.* OSHA Brief, 2012. 7.

jogszabály, szabvány, vagy a rendeltetésszerű és biztonságos üzemeltetésre, használatra vonatkozó dokumentáció előírja."[17]

A veszélyes gépeket felsoroló listát a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet 1/a. számú melléklete tartalmazza. Ezenfelül természetesen a munkáltató meghatározhat még egyéb – a cég profiljával összefüggő – speciális eszközöket is. Ezeket külön intézkedésben, szabályzatban rögzíti, majd az érintett munkavállalók számára oktatás keretében ismerteti. A katasztrófavédelem, tűzoltóság esetén veszélyes munkaeszköznek minősülnek a hidraulikus mentőeszközök is.

E felülvizsgálatok során feltárhatók azok az észrevétlen meghibásodások, sérülések, amelyek az eszköz használata közben okoznának sérülést vagy balesetet. Kiemelendő, hogy a rendszeres ellenőrzés, felülvizsgálat mellett az állomány számára elméleti és gyakorlati oktatás is szükséges, hogy minél nagyobb tapasztalattal, rutinnal legyenek képesek használni a beavatkozás során az adott gépet.

Az egyéni védőeszközök biztosítják azt a kiemelt szintű védelmet a beavatkozó tűzoltók számára széles körű feladataik ellátása során, ami elengedhetetlen munkavégzésük hatékonysága és egészségük védelme érdekében.[18] A katasztrófavédelem, a tűzoltóság vonatkozásában az Intézkedés Mellékletében találhatók meg tételesen felsorolva munkakörönként az egyéni védőeszközök. Így a készenléti szolgálatot ellátó hivatásos állomány számára az alábbiak olvashatók:

- tűzoltó-védőruha;
- tűzoltó-védősisak/nyak- és arcvédővel;
- tűzoltó-védőkámzsa;
- tűzoltó-védőcsizma;
- tűzoltó-védőkesztyű;
- munkavédelmi védőkesztyű;
- a magasból való leesés, vagy az esés hatásának megelőzésére szolgáló egyéni védőeszköz;
- zajvédő füldugó.[19]

Az egyéni védőeszközök rendeltetésszerű használatára, a szakfelszerelésekkel együtt viselés képzésére[20] nagy hangsúlyt kell fektetni, mivel egy káresemény során mindenképp szükséges és elvárható, hogy automatikusan hajtsa végre a tűzoltó az adott mozdulatokat. Az egyéni védőeszközöket minden használat előtt és után szemrevételezéssel ellenőrizni kell, hogy egy lehetséges sérülést vagy meghibásodást a laktanya területén vegyenek észre, ezzel megelőzve a kárt, balesetet.

[17] 1993. évi XCIII. törvény 23. § (1) bekezdés.
[18] Urbán Anett: A katasztrófavédelem tűzoltó egységeinél rendszeresített védőruházatok vizsgálata. *Műszaki Katonai Közlöny,* 27. (2017), 4. 103.
[19] 34/2021. számú Főigazgatói Intézkedés, Melléklet.
[20] Pántya Péter: A katasztrófavédelem beavatkozó hatékonyságának fejlesztése a tűzoltósági területen. *Hadmérnök,* 13. (2018), „KÖFOP" szám. 121.

3. Következtetések, javaslatok

A jelenlegi, technikai vívmányok adta világban a tűzoltólaktanyák tervezése és kialakítása már sokkal komplexebb szemléletet igényel. A laktanya funkciójának ellátása és az állomány biztonságos elhelyezése mellett megjelent a fenntartható fejlődés és a környezetvédelem fogalma is. Kiváló példaként szolgál e témakörön belül a napkollektorok, napelemek felhelyezése és használata. Fontos megemlíteni, hogy ez a technológia nem terjedt el olyan széleskörűen, mint például a hagyományos szén- vagy gázalapú fűtési rendszer, így mindenképp meg kell ismertetni az állománynyal a használatból eredő hibákat és veszélyeket (például áramütés). A jövőben nagy valószínűséggel számos technológiai korszerűsítés integrálása várható a laktanyákat illetően (például okosotthon technikai eszközei), így a képzést és továbbképzést mindenképp szükségesnek tartom ezen a területen is, mivel a helytelen kezelés felesleges karbantartáshoz, meghibásodáshoz vagy balesethez vezetne.

Emellett számba kell venni, hogy a sokak által is érezhető éghajlatváltozás következtében az eddig megszokott időjárási viszonyoktól eltérően szükséges megtervezni és megépíteni a jövő tűzoltólaktanyáit, például korszerűbb homlokzati hőszigetelési technológiával. Ez a módosítás várhatóan nemcsak az épület szerkezetét kell hogy érintse, hanem a belső terek kialakítását is, mivel a technológiai fejlődés adta modern eszközök, berendezések kihatnak egy adott helyiség elrendezésére is, például szerverhelyiség-hűtés (légkondicionáló berendezés) biztosításával.

Ezzel összefüggésben további fejlesztések várhatók a szakfelszerelések, egyéni védőeszközök tekintetében, hiszen ezen eszközöknek is követnie, igazodnia kell a megváltozott körülményekhez. A tűzoltólaktanya kialakítására, a helyiségeikre és az azokban található tárolóegységekre (például szekrény, doboz) hatással lehet mindez, hiszen ha egy adott felszerelés mérete megváltozik, akkor annak tárolását is más helyszínen vagy másképp kell megoldani. Amennyiben egy egyéni védőeszköz a közeljövőben kiegészítő egységet (például mesterséges külső váz/exoskeleton[21]) kap a megnövelt védelmi képesség érdekében, akkor ugyancsak nagyobb helyigényekkel kell számolni.

4. Összefoglalás

A tűzoltólaktanyák tervezésénél és kialakításánál a szakemberek számos különböző szakterület előírásait veszik figyelembe, amelyeknek egymással összhangban kell lenniük. A munkavédelemnek egészen a kezdetektől hangsúlyos szerepe van ebben, mivel az egészséget nem veszélyeztető és biztonságos munkavégzés feltételeit már a tervezőasztalon meg kell határozni.

A laktanya használatbavételét követően a rendszeres munkavédelmi szempontú ellenőrzések biztosítják, hogy folyamatosan és hosszú távon is megmaradjanak a balesetmentes munkakörülmények. Ezen túlmenően az állomány képzése munkavédelmi

[21] Arthur Osipov: Fire Exoskeleton to Facilitate the Work of the Fireman. *E3S Web of Conferences,* 126. (2019). 1–10.

és szakmai területen is kiemelten kezelendő, mivel ezek segítségével mélyíthető el az az ismeret, amelyet kellő magabiztossággal tudnak alkalmazni az érintett személyek.

Felhasznált irodalom

Ahmet Biler – Aslihan Unlu Tavil – Yuehong Su and Naghman Khan: A Review of Performance Specifications and Studies of Trickle Vents. *Buildings,* 8. (2018), 11. 152. Online: https://doi.org/10.3390/buildings8110152

Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság: *Átépült és megújult az orosházi laktanya* (2022. március 22.). Online: www.katasztrofavedelem.hu/29/hirek/262450/atepult-es-megujult-az-oroshazi-laktanya

Hornyacsek Júlia – Vad Tibor: A tűzoltók fizikai, szellemi és pszichés terhelése. *Hadtudományi Szemle,* 4. (2011), 4. 142–154. Online: http://epa.oszk.hu/02400/02463/00011/pdf/EPA02463_hadtudomanyi_szemle_2011_4_142-154.pdf

Nemzeti Népegészségügyi Központ: *Fertőződés elkerülése – Alapvető szabályok mindenki számára a Covid–19 vírusfertőzéssel kapcsolatban* (2020. március 16.). Online: www.nnk.gov.hu/index.php/koronavirus-tajekoztato/560-fertozodes-elkerulese-alapveto-szabalyok-mindenki-szamara

Occupational Safety and Health Administration: *Hazard Communication Standard: Safety Data Sheets.* OSHA Brief, 2012. Online: www.osha.gov/sites/default/files/publications/OSHA3514.pdf

Osipov, Arthur: Fire Exoskeleton to Facilitate the Work of the Fireman. *E3S Web of Conferences,* 126. (2019). 1–10. Online: https://doi.org/10.1051/e3sconf/201912600015

Padányi József: *Az éghajlatváltozás és a katonai erő viszonyrendszere a hazai és a nemzetközi kutatások tükrében.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Pántya Péter: A katasztrófavédelem beavatkozó hatékonyságának fejlesztése a tűzoltósági területen. *Hadmérnök,* 13. (2018), „KÖFOP" szám. 109–144.

Potter, Alex: How an Ingenious Fireman Brought a Pole Into the Firehouse. *Smithsonian Magazine,* 2020. július. Online: www.smithsonianmag.com/innovation/invention-firemans-pole-180975206/

Shinn, Mary: When Seconds Count, Durango Firefighters Hit the Brass Pole. *The Durango Herald,* 2019. november 3. Online: www.durangoherald.com/articles/when-seconds-count-durango-firefighters-hit-the-brass-pole/

Urbán Anett: A katasztrófavédelem tűzoltó egységeinél rendszeresített védőruházatok vizsgálata. *Műszaki Katonai Közlöny,* 27. (2017), 4. 103–122. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/1953/1239

Varga László (szerk.): *A munkavédelmi törvény magyarázata.* Budapest, KJK-Kerszöv, 2005.

Jogi források

1993. évi XCIII. törvény a munkavédelemről

70/2011. (XII. 30.) BM rendelet a belügyminiszter irányítása alá tartozó rendvédelmi szervek munkavédelmi feladatai, valamint foglalkozás-egészségügyi tevékenysége ellátásának szabályairól
2/1998. (I. 16.) MüM rendelet a munkahelyen alkalmazandó biztonsági és egészségvédelmi jelzésekről
61/1999. (XII. 1.) EüM rendelet a biológiai tényezők hatásának kitett munkavállalók egészségének védelméről
3/2002. (II. 8.) SzCsM-EüM együttes rendelet a munkahelyek munkavédelmi követelményeinek minimális szintjéről
53/2018. számú BM OKF főigazgatói intézkedés a tűzoltósági szakterület által tartandó gyakorlatok rendszerének szabályairól
34/2021. számú Főigazgatói Intézkedés a személyi állomány egyéni védőeszközzel történő ellátásáról

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

17. évfolyam (2022) 3. szám 71–80.
DOI: 10.32567/hm.2022.3.5

Benjámin Hózer[1]

The Safety Situation of Municipal Solid Waste Landfills in Hungary from a Disaster Management Perspective – Part 1

Today, nearly seventy municipal solid waste landfills in Hungary fully comply with European Union directives. Experience has shown that some sites have not yet been recultivated and that there are several illegal landfills. Waste fires are a special area within disaster management that have not yet been legally regulated nor intervention procedures have been established. In the first part of the series of articles I will present the key aspects that should be taken into account when defining a possible legal regulation. In addition, I plan to evaluate the prevention and response measures to hazards that are specific to landfills.

Keywords: **waste management, resource management, extinguishing water management, fire safety, industrial safety**

1. Introduction

The issue of fire safety and emergency planning of landfills in Hungary is a less scientifically researched topic. Waste is inherent in human life. No waste is generated in nature, as any residue is recovered in the form of food or humus. In some cases, it can also serve as a habitat for smaller organisms. However, mankind has been producing unusable materials since the beginning of his evolutionary development.

There are several definitions for waste. Among them, it is worth looking at Act CLXXXV of 2012 on Waste (hereinafter: the Waste Act), which is worded as follows in § 2 (23): "Waste: any substance or object which the holder discards or intends or is required to discard."

We must therefore take two official aspects into account when defining waste as a concept. On the one hand, it is a substance we want to get rid of, and on the

[1] PhD student, University of Public Service Doctoral School of Military Engineering, e-mail: hozer.benjamin@gmail.com

other hand, an unused residue. In addition to the comprehensive definition of waste, it is necessary to mention three subcategories.

The first group is *bio-waste,* which includes garden waste, also known as green waste, and food waste. During their natural decomposition, green waste forms, among other things, combustible and greenhouse gases.

The second category is *construction and demolition waste.* The vast majority of construction debris is inert waste. Inert wastes are non-combustible and do not oxidise. In addition, they do not emit environmentally hazardous compounds and do not undergo biodegradation.

The third group can be identified as *household waste,* which is commonly referred to as municipal or household waste. Thus, any waste that is generated in everyday life can also contain degradable, inert and small amounts of hazardous waste.

Based on the composition of municipal waste, it consists on average of 40–50% organic matter,[2] and the content of hazardous waste ranges from about 0.5 to 0.7%.[3]

In order to significantly reduce the amount of waste in our environment, in my opinion, it is necessary to change our approach to public waste management in the first place. Public education can play a key role in developing an environmentally conscious approach. For example, it is important to teach children that it is not only necessary to collect waste selectively, but also to understand the process that takes place with the recycled material during waste treatment. In addition to the selective collection of materials belonging to the already mentioned waste categories, information on the afterlife of waste can also be an important aspect. In the case of decomposing waste, recycling can take place as compost,[4] or biomass.[5] In addition, the utilisation of construction and demolition debris as a road base can reduce the amount of waste going to landfill.

One of the biggest problems regarding the safety of the environment[6] is waste that cannot be monitored by monitoring systems. For example the microplastics.[7]

Non-recyclable waste typically comes from a variety of packaging materials. Within the European Union, nation states use different methods to reduce landfilling and increase the spread of recyclable materials. An example is the deposit fee. Another method could be the banded garbage collection system prevalent in Germany.[8]

It can be seen from the above that waste that is neither reused nor recovered for energy is landfilled in a municipal landfill. A landfill is a facility with specific technical

[2] József Hajdú: *Biogáz üzemek működése és biogáz üzemi technológiák.* Gödöllő, Szent István Egyetemi Kiadó, 2009. 13.

[3] Lajos Kátai-Urbán: *Veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény- és eszközrendszer fejlesztése Magyarországon.* Budapest, Nemzeti Közszolgálati Egyetem, 2015. 34.

[4] Tamás Trenyik: *A települési hulladék begyűjtés és a kapcsolódó elválasztási láncok folyamatmodell bázisú értékelése.* PhD thesis, University of Kaposvár, Faculty of Economics, 2019. 3.

[5] Nemzeti Energia- és Klímaterv [National Energy and Climate Plan]. Ministry for Innovation and Technology, 2019. 41.

[6] Lajos Kátai-Urbán et al.: Veszélyes tevékenységek biztonsága a fenntarthatóság jegyében. *Védelem Tudomány,* 5, no. 1 (2020). 140.

[7] Lajos Kátai-Urbán – Tamás Parrag: *Szennyvizek mikroszennyező és mikroműanyag tartalma.* Iparbiztonsági és Hatósági Szakmai Nap, 2020. 104–113.

[8] Júlia Hornyacsek – Erika László: A hulladéklerakás adaptálható tapasztalatai Ausztriában és Németországban. *Bolyai Szemle,* 25, no. 3 (2016). 92.

protection where waste is stored on and off the surface for at least one year for non-recycling purposes.

The aim of this article is to present the general Hungarian safety regulatory environment, the most important safety factors, the sources of danger and the possible answers to the possible events of solid waste landfills in Hungary. In the course of my work, I used the sources of the European Union and domestic law as a basis. In addition, I analysed the scientific literature of both Hungary and abroad and compared it with a critical approach.

2. Evaluation of legislation

2.1. Examination of the international legal environment

The Council of the European Union, Directive 1999/31/EC on the landfill of waste lists, among the general requirements for action on landfills in point 5 of Annex I, an incident which has an adverse effect or a hazard on the installation.

It is unfortunate to note that the landfill regulations of the European Union basically set standards for the landfill and acceptance of waste, but this legislation does not deal with aspects of disaster prevention or fire protection.

2.2. Examination of the domestic legal environment

In Hungary, the general regulation of waste management is provided by the Waste Act, the authorising provision of which provides for the decree 20/2006 on certain rules and conditions related to landfilling (IV. 5.). The Ministry of Environment and Water defines the exact rules for the establishment and operation of the depository. That legislation does not deal with the safety aspects of the installations in a separate provision. However, Act CXXVIII of 2011 on Disaster Management Section 4 of the Act only establishes the *non-scope* of the Act in relation to waste landfills.

Decree 219/2011 (X. 20.) on the prevention of major accidents involving dangerous substances, formulates criteria only for hazardous waste, as solid hazardous waste is typically disposed of by incineration.[9] In addition, it is important to note that Decree 6/2016 (VI. 24.) on Firefighting Tactics Regulations and Technical Rescue Regulations BM OKF instruction does not contain any special provisions related to waste fires.

Establishment criteria are met only by Decree 54/2014 (XII. 5.) on National Fire Protection Regulations, introduced by the Decree of the Ministry of the Interior, § 72 (6), according to which "an extinguishing water intensity of 1,800 litres/minute shall be provided for one and a half hours in the open-air storage area of a municipal waste landfill". The law gives a free hand here as to whether this amount is provided

[9] Cintia Morvai: Veszélyes hulladékok keletkezésének és ártalmatlanításának vizsgálata. *Védelem Tudomány,* 2, no. 3 (2017). 136.

by the landfill operator from a hydrant or a firefighting reservoir. For most facilities, the plant has its own fire safety policy drawn up by its own or a qualified fire engineer. The instructions of which must be followed by the workers. These usually only provide instructions on how to place and keep fire extinguishers on standby.[10]

3. Assessment of the technical possibilities of waste management

3.1. Waste management activities in Hungary

Most of the waste generated by the population can be processed in three different ways:

- solid waste can be recycled or reused, as is the case with deposit products or paper
- energy use, i.e. the conversion of waste energy into thermal and electrical energy in incinerators, is also a significant form of recovery
- ultimately, depositing can be the right solution[11]

In terms of waste management, the ideal would be for the population not to produce waste. This way, all products would be made exclusively of recyclable or reusable material. This is especially true for the packaging of food or household products. The extraction of disposable plastics and the use of degradable materials would still be feasible. However, this solution would entail significant additional costs for both the manufacturer and the consumer. In the long run, therefore, the aim is to completely restructure the industry and consumer habits, i.e. to minimise the production of waste. In the short term, however, it is necessary to ensure that the waste generated so far is properly treated.

Figure 1 shows the levels of waste management, which can also be referred to as a waste pyramid.

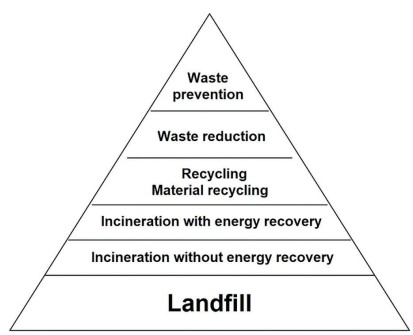


Figure 1: Levels of waste management, i.e. the "waste pyramid"

Source: Anikó Horváth – József Stipta: Csomagolóanyagok környezeti hatásvizsgálata. Műszaki Szemle, 10, nos. 39–40 (2007). 26.

[10] Barnabás Csőke: *Hulladékgazdálkodás.* Veszprém, Pannon Egyetem, 2011. 65.
[11] Géza Károly Kiss Leizer: Környezetbiztonság a hulladékok hasznosításában. *Hadmérnök,* 10, no. 3 (2015). 112.

In Hungary, the collection and removal of waste from residential areas is a key task in society. According to Decree 292/2013 (VII. 26.) on the rules of non-regular waste shipments and the designation of state bodies acting in this process, if the company providing public services in the area of competence is unable to transport the waste, the disaster management authority shall designate another economic organisation providing public services that carries out the transport of waste from the underserved area.

This regulation prevents emergency situations like the one that happened in Naples[12] in the early 2010s, or is still going on in Rome.[13] An important problem in these areas is the public protest against the establishment of new landfills. Municipal waste generated locally must be transported by the city administration to sites significantly further away. This causes supply problems and public health problems in cities due to additional costs and distance.

According to a 2014 survey, there are more than 2,500 public landfills in Hungary.[14] Of these, 70 have landfills that fully comply with EU standards.[15] Among the 2,500, however, there are some that have been illegally designed.

According to 2016 data, 65% of the waste generated in Hungary is landfilled.[16] The EU average for landfilling is 63%.[17] Of the remaining 35%, 9% will be recovered for energy through incineration and the other 26% will be recycled.[18] It is worth noting here that the selective collection and transport of paper and plastic waste and the disposal of green waste have significantly contributed to the development of good waste management practices.

3.2. Municipal solid waste landfills

The disadvantage of landfills is that the waste is not recovered materially or energetically. Bio-waste, such as green waste or food waste, forms various gases during natural decomposition (combustion), among which methane can also be identified. These gases are uniformly called landfill gas.[19] Methane is known primarily from mining as the cause of the blast. It can be seen, therefore, that the depositor can also be a serious source of danger. It is not possible to ventilate the waste, as in the vast majority of cases it is compacted by a so-called compactor with claw wheels.

[12] Christian Fraser: Naples: A City Swimming in Filth. *BBC News,* 28 May 2008.
[13] Giorgia Orlandi: Évek óta tart a hulladékválság az olasz fővárosban. *Euronews,* 13 July 2021.
[14] BME ABÉT: *Kommunális szilárd hulladéklerakók Magyarországon* [Municipal Solid Waste Landfills in Hungary]. s. a.
[15] Ákos Grecmájer: *Magyarország hulladékgazdálkodási adatainak földrajzi megjelenítése és elemzése.* Budapest, ELTE–TTK, 2014. 10.
[16] Képviselői Információs Szolgálat [Representative Information Service]: Hulladékerőművek, hulladékégetés [Waste-to-Energy Plants, Waste Incineration]. *Infojegyzet,* 2016/23. 3.
[17] Angéla Pál: A kommunális hulladékok környezeti hatásai, a hulladékgazdálkodás, mint ellenhatás. *Hadmérnök,* 11, no. 2 (2016). 96.
[18] Hornyacsek–László (2016): op. cit. 87.
[19] Imre Szabó: *Hulladéklerakók tervezése, üzemeltetése I.* Miskolc, Miskolci Egyetem, 2011.

Figure 2: Caterpillar 826C compactor at an Australian landfill
Source: Picture of a Caterpillar 826C landfill compactor being used at an Australian landfill site. s. a.

As a result, landfill gas must be drained. The extraction of the gases is carried out by means of perforated so-called drain pipes, which are placed horizontally in layers. Drain pipes are already introduced out of the ground into solid polyethylene pipes that branch into gas pumps. Geotextiles are then spread on the drain pipes. This releases the waste into an anaerobic environment, i.e. if possible, all the gas formed escapes into the pipes. Thus, the landfill gases can only have minimal contact with the outside air. Vertical piping can also be used for landfill gas discharge, but only in the case of abandoned landfills, as in this case landfill activity on the surface cannot be ensured. The methane formed so far is released into the air, which is not beneficial due to its greenhouse effect.[20] At the same time, the advantage of piping penetrating the layers is that the concentration of evaporating gases can also be measured. Despite the anaerobic environment, leakage occurs through capillary passages.

Methane in landfill gas can also be dangerous to the environment, as if an inclusion is formed or gas pumping stops, it can already cause an explosion. The amount of methane produced can be said to be energetically insignificant. Most typically, a boiler is set up in the landfill area itself, where it can generate hot water and/or electricity by burning it. The methane content of the landfill gas varies greatly from 30 to 70%, which may be responsible for the odour in the area. The other materials in the landfill gas can typically be carbon dioxide, which can make it difficult to burn methane as

[20] Pál (2016): op. cit. 96.

a perfect combustion product. This gas also has an ozone depleting effect. The energy generated here usually only serves the landfill's own energy needs.[21]

4. Resources in the field of solid landfills

One of the main problems of operating municipal waste landfills is that the composition of waste is considered to be significantly heterogeneous. Combustible and non-combustible waste can also include small amounts of hazardous waste, such as chemicals, infectious substances classified as hospital waste, and so on. In addition to the previously mentioned degradable waste, self-reactive substances can also be identified. In the latter category, lithium-ion batteries play a prominent role in which, if the separator membrane is damaged, a self-reactive process can occur during the reaction of the anode and cathode fluids. The cell is first physically deformed and then, by perforating the outer shell, the material is in contact with the oxygen in the ambient air during a severe and short-term refractive action. The flame is unquenchable because when the process starts, oxygen is released during the reaction, which fuels the combustion. For this reason, a burning fuel cell can burn even when submerged. This phenomenon can occur without an external heat source, merely due to mechanical damage.[22] In this way, conscious public waste management has a key role to play in order to avoid fires in landfills. Another important aspect is that collection machines typically dispose of waste uncontrolled, which makes it impossible to recycle waste in advance. Injury can often occur during the operation of compactors and grabs. At the same time, there is a greater burden on workers, as it is important to recycle the waste around the cell for post-processing. Monitoring and detecting sweats or the spread of fire is also a separate task.

We know from the work of researchers in the field that "74% of fires in waste management were caused by spontaneous combustion, 11% by other known causes and 15% by unknown causes".[23] In the event of a fire in the landfill, the fire brigade must be notified immediately. Experience shows that this is not always clear to those who work there.

For the most part, due to a lack of knowledge of the legal regulatory obligation, security guards are often wary of signalling the incident to the emergency services on duty during working hours and outside of working hours during the night shift, for fear of possible legal retaliation. Thus, unfortunately, a large proportion of fire alarms only reach disaster protection when the public also announces extensive smoke or light exposure at night.

In the migration area, the competent intervention staff must be trained and practiced to work in accordance with local conditions. Such is the case with the densely changing surface, as uncompressed waste is looser in some areas due to

[21] Hajdú (2009): op. cit. 13.
[22] Qingsong Wang et al.: Thermal Runaway Caused Fire and Explosion of Lithium Ion Battery. *Journal of Power Sources,* 208 (2012). 210–224.
[23] Imre Antal – Rudolf Nagy: A települési hulladékkezelés tűzbiztonságának munkavédelmi szempontú vizsgálata. *Védelem Tudomány,* 6, no. 4 (2021). 61.

continuous dumping, so accidents can occur due to the swampy nature of the soil. Elsewhere, chippings, subsidence and water washes may occur. However, compaction with compactors is not common in all landfills. The compactors use their claw wheels to compact the material to a workable density. However, in landfills where only wheeled excavators or grabs are available, no such work process takes place. This can also cause subsidence, which can lead to serious accidents. In poor visibility conditions such as night, fog, heavy smoke or snow cover, this can be an additional source of danger for the intervention fire brigade.

5. Conclusions

The facts presented in the present study show that there is room for improvement in the legal regulation of solid waste landfills in Hungary from a disaster management perspective. We can see that there are effective international and domestic initiatives to reduce the amount of waste generated. It can be said, however, that until the guidelines for the circular economy come into force in the European Union, we will have to deal with the solid waste generated by households. Non-recoverable waste can pose significant hazards to both the public and workers, and to our environment as a whole. It is clear that a number of events stem from landfill activities that cannot be prevented by primary interveners. An excellent example of this is self-inflammation.

In my opinion, conscious waste management and the prevention of major fires must be an important requirement for disaster protection. Further attention should be paid to the activities of on-site workers, as their responsibilities will be significantly increased in curbing initial fires over time and preventing their spread.

References

Antal, Imre – Rudolf Nagy: A települési hulladékkezelés tűzbiztonságának munkavédelmi szempontú vizsgálata. *Védelem Tudomány,* 6, no. 4 (2021). 42–72.

BME ABÉT: *Kommunális szilárd hulladéklerakók Magyarországon* [Municipal Solid Waste Landfills in Hungary]. s. a. Online: www.enfo.hu/index.php/etanfolyam/11579

Csőke, Barnabás: *Hulladékgazdálkodás.* Veszprém, Pannon Egyetem, 2011. Online: https://tudastar.mk.uni-pannon.hu/anyagok/12-Hulladekgazdalkodas.pdf

Fraser, Christian: Naples: A City Swimming in Filth. *BBC News,* 28 May 2008. Online: http://news.bbc.co.uk/2/hi/europe/7423245.stm

Grecmájer, Ákos: *Magyarország hulladékgazdálkodási adatainak földrajzi megjelenítése és elemzése.* Budapest, ELTE–TTK, 2014. Online: http://lazarus.elte.hu/hun/digkonyv/szakdolg/2014-bsc/grecmajer_akos.pdf

Hajdú, József: *Biogáz üzemek működése és biogáz üzemi technológiák.* Gödöllő, Szent István Egyetemi Kiadó, 2009. Online: https://docplayer.hu/280371-Biogazuzemek-mukodese-es-biogaz-uzemi-technologiak-obekk-tudomanyos-szakmai-kiadvanyok-szerzo-dr-hajdu-jozsef.html

Hornyacsek, Júlia – Erika László: A hulladéklerakás adaptálható tapasztalatai Ausztriában és Németországban. *Bolyai Szemle,* 25, no. 3 (2016). 84–95.
Horváth, Anikó – József Stipta: Csomagolóanyagok környezeti hatásvizsgálata. *Műszaki Szemle,* 10, nos. 39–40 (2007). 25–30.
Kátai-Urbán, Lajos – Tamás Parrag: *Szennyvizek mikroszennyező és mikroműanyag tartalma.* Iparbiztonsági és Hatósági Szakmai Nap, 2020.
Kátai-Urbán, Lajos – Gyula Vass – Alexandra Német: Veszélyes tevékenységek biztonsága a fenntarthatóság jegyében. *Védelem Tudomány,* 5, no. 1 (2020). 137–152.
Kátai-Urbán, Lajos: *Veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény- és eszközrendszer fejlesztése Magyarországon.* Budapest, Nemzeti Közszolgálati Egyetem, 2015.
Képviselői Információs Szolgálat [Representative Information Service]: Hulladékerőművek, hulladékégetés [Waste-to-Energy Plants, Waste Incineration]. *Infojegyzet,* 2016/23. Online: www.parlament.hu/documents/10181/595001/Infojegyzet_2016_23_hulladekegetes.pdf/c4ea1502-7026-4a7b-98eb-99bc653ece1a
Kiss Leizer, Géza Károly: Környezetbiztonság a hulladékok hasznosításában. *Hadmérnök,* 10, no. 3 (2015). 109–118.
Morvai, Cintia: Veszélyes hulladékok keletkezésének és ártalmatlanításának vizsgálata. *Védelem Tudomány,* 2, no. 1 (2017). 129–138.
Nemzeti Energia- és Klímaterv [National Energy and Climate Plan]. Ministry for Innovation and Technology, 2019. Online: https://ec.europa.eu/energy/sites/ener/files/documents/hu_final_necp_main_hu.pdf
Orlandi, Giorgia: Évek óta tart a hulladékválság az olasz fővárosban. Euronews, 13 July 2021. Online: https://hu.euronews.com/green/2021/07/13/evek-ota-tart-a-hulladekvalsag-az-olasz-fovarosban
Pál, Angéla: A kommunális hulladékok környezeti hatásai, a hulladékgazdálkodás, mint ellenhatás. *Hadmérnök,* 11, no. 2 (2016). 87–98.
Picture of a Caterpillar 826C landfill compactor being used at an Australian landfill site. s. a. Online: https://commons.wikimedia.org/wiki/File:Landfill_compactor.jpg
Rácz, Réka Magdolna – Balázs Lóderer: A klímaváltozás és annak következményeire való felkészülés lehetséges jövőbeni aspektusai. *Hadtudományi Szemle,* 4, no. 3 (2011). 91– 98.
Szabó, Imre: *Hulladéklerakók tervezése, üzemeltetése I.* Miskolc, Miskolci Egyetem, 2011. Online: https://hulladekonline.hu/files/81
Trenyik, Tamás: *A települési hulladék begyűjtés és a kapcsolódó elválasztási láncok folyamatmodell bázisú értékelése.* PhD thesis, University of Kaposvár, Faculty of Economics, 2019.
Wang, Qingsong – Ping Ping – Xuejuan Zhao – Guanquan Chu – Jinhua Sun – Chunhua Chen: Thermal Runaway Caused Fire and Explosion of Lithium Ion Battery. *Journal of Power Sources,* 208 (2012). 210–224. Online: https://doi.org/10.1016/j.jpowsour.2012.02.038

Legal sources

Act CXXVIII of 2011 on Disaster Management and amending certain related laws.
Act CLXXXV of 2012 on Waste.
Council Directive 1999/31/EC of 26 April 1999 on the landfill of waste.
Decree 219/2011 (X. 20.) on the protection against serious accidents related to hazardous substances.
Decree 6/2016 (VI. 24.) on Firefighting Tactics Regulations and Technical Rescue Regulations BM OKF instruction.
Decree 54/2014 (XII. 5.) of the Ministry of the Interior on the National Fire Protection Regulations.
Decree 292/2013 (VII. 26.) on the rules of non-regular waste transport and the designation of state bodies acting in this process.

HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 81–95.
DOI: 10.32567/hm.2022.3.6

Bak Gerda,[1] Kelemen-Erdős Anikó[2]

Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján

Information Security Awareness from Generation Y Perspective Based on a Qualitative Approach

A digitális technológia behálózza életünk, a pandémia pedig tovább növeli és erősíti az elektronikus eszközökkel való kapcsolatunkat. Ezzel együtt a kibertámadások száma is jelentősen megnövekedett, annak ellenére, hogy ezek jelentős része megelőzhető lenne.

Jelen tanulmány célja az Y generációs fiatalok információbiztonsággal kapcsolatos attitűdjét, tudatosságát befolyásoló tényezők feltárása, mélyebb megértése kvalitatív jellegű empirikus kutatás, mélyinterjúk alapján. Az interjúk elemzése trianguláció keretében két megközelítésben, tartalomelemzéssel és *grounded theory* módszertannal történt. Az interjúk rámutatnak, hogy az alanyok jelentős tényezőként tekintenek elméleti síkon az online és digitális biztonságukra, azonban a gyakorlatban a megfelelő védekezési módok hiányossága, az alanyok sebezhetősége derül ki a kutatásból. Az alapozó jellegű kutatás további kvantitatív kutatás alapját képezheti.

Kulcsszavak: **információbiztonság-tudatosság, kiberbiztonság, Y generáció, mélyinterjú, tartalomelemzés, grounded theory**

Digital technology is embedded in our lives, and the pandemic will further increase and strengthen our connection to electronic devices. At the same time, the number

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[2] Óbudai Egyetem Keleti Károly Gazdasági Kar Gazdaság- és Társadalomtudományi Intézet, e-mail: kelemen.aniko@kgk.uni-obuda.hu

of cyberattacks has increased significantly, despite the fact that a significant part of them could be prevented.

This study aims to explore and deepen the understanding of the factors influencing the attitudes and awareness of Generation Y youth towards information security, based on qualitative empirical research in form of in-depth interviews. The interviews were analysed using a triangulation approach with two perspectives: content analysis and grounded theory methodology. The interviews demonstrate that the interviewees consider their online and digital security as a significant factor on a theoretical level, however, the practice reveals the lack of appropriate protection methods and the vulnerability of the respondents. This foundational research can form the basis for further quantitative approaches.

Keywords: **information security awareness, cybersecurity, Generation Y, in-depth interview, content analysis, grounded theory**

1. Bevezetés

Az információbiztonság még mindig jelentős problémát okoz nemcsak a szervezetek számára, hanem az egyének életében is, annak ellenére, hogy számos technológiai megoldást, védekezési módot fejlesztettek ki a probléma leküzdésére,[3] s bár a szakirodalomban az a meglátás terjedt el, hogy az egyén a leggyengébb láncszem az információbiztonsági láncban,[4] mégsem sikerült erre megoldást találni.[5] Ez pedig akár egészen addig komoly problémákat okozhat, ameddig az egyének tudatosságát nem sikerül növelni.

Az információbiztonság-tudatosság (*information security awareness,* ISA) témakörét számos megközelítésből vizsgálják,[6] és annál is több kutatás próbálja feltárni, melyek azok a tényezők, amelyek hatással lehetnek az egyének és a szervezetek információbiztonság-tudatosságára, illetve annak mérése, növelése,[7] valamint előrejelzése miként lehetséges.

[3] Kevin Grant et al.: 'Risky Business': Perceptions of E-Business Risk by UK Small and Medium Sized Enterprises (SMEs). *International Journal of Information Management,* 34. (2014), 2. 99–122.

[4] Verena Zimmermann – Karen Renaud: Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies,* 131. (2019). 169–187.

[5] Gershon Hutchinson – Jacques Ophoff: A Descriptive Review and Classification of Organizational Information Security Awareness Research. In H. Venter et al. (szerk.): *Information and Cyber Security.* Cham, Springer, 2020. 114–130.

[6] Abdul Rahman Ahlan – Muharman Lubis – Arif Ridho Lubis: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72. (2015). 361–373.; Bak Gerda – Kiss Sándor: A biztonságtudatosság szisztematikus szakirodalmi áttekintése. *Hadmérnök,* 16. (2021), 4. 85–99.

[7] Zeng Zhongping et al.: Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In *2013 Fourth International Conference on Digital Manufacturing & Automation.* IEEE, 2013. 684–687.

A viselkedési modelleket alapul vevő kutatások megpróbálják megérteni és magyarázni az egyén és a biztonság, valamint a technológia viszonyát.[8] A viselkedéstudományi megközelítések közelebb visznek a releváns aspektusok megértéséhez, azonban az egyén vagy szervezet információbiztonság-tudatosságának hátterét nem képesek megvilágítani.[9] Jelen kutatás célja az információbiztonság-tudatosságot befolyásoló egyéni tényezők feltárása és azonosítása, valamint az interjúalanyok információbiztonság-tudatosságról alkotott képének, illetve a digitális technológiában rejlő veszélyek ismeretének vizsgálata, aminek következtében növelhető a tudatosság a digitális eszközöket használók körében, esetlegesen csökkenthetők és/vagy megelőzhetők a kibertámadások mind mennyiségben, mind az okozott károk értékében, hatásaiban.

Kutatásunkban az Y generációra fókuszálunk, az 1980 és 1994 között születetteket vizsgáljuk.[10] Számos, akár ettől eltérő kategorizálás létezik a generációs megkülönböztetésre, ugyanakkor azért választottuk a magyar szerző kormeghatározását, mert alapvetően történelmi, társadalmi fejlődésbeli eltérések határozzák meg az egyes generációk elkülönülését.

Ennek alapján a következő kutatási kérdéseket fogalmaztuk meg:

K1. Hogyan érzékelik a megkérdezett Y generációs fiatalok az információbiztonsági kockázatot?

K2. Mely tényezők határozzák meg az Y generációs interjúalanyok információbiztonság-tudatosságát?

K3. Mely tényezők járulhatnak hozzá az Y generációs interjúalanyok információbiztonság-tudatosságának fokozásához?

A cikk első felében szakirodalmi áttekintés keretében az információbiztonság-tudatosság témakörét vizsgáljuk, majd az Y generáció körében végzett kvalitatív mélyinterjúk elemzésére alkalmazott módszertant, a kvalitatív tartalomelemzést és a *grounded theory* módszertant mutatjuk be. Ezt követően a kutatás főbb eredményeit és további kutatási irányokat fogalmazunk meg.

2. Szakirodalmi áttekintés

A digitális technológia fejlődésével egyre több információt tárolunk digitális eszközeinken és a felhőben, a technológia nemcsak lehetőségeket, hanem biztonsági kockázatokat is magában rejt. A közösségimédia-felületek térnyerésével napjainkban egyre több információt tudnak megszerezni rólunk digitális lábnyomunk és digitális eszközeink nem megfelelő használatának eredményeképp. A felhasználók ennek következtében

[8] Burcu Bulgurcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34. (2010), 3. 523–548.

[9] Kathryn Parsons et al.: Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* 42. (2014). 165–176.

[10] Tari Annamária: *Y generáció. Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban*. Budapest, Jaffa Kiadó, 2010.

sokszor kellemetlen helyzetbe kerülhetnek, akár a saját, akár mások kárára, hiszen előfordulhat, hogy zsarolás áldozatai is lehetnek.[11] Mivel a döntéshozatal az egyének szintjén történik, az emberi tényező fontos szerepet játszik az információbiztonság szempontjaiban.

A szervezet információs rendszerének biztonságát gyengítő incidensek egyik leggyakoribb tényezője az alkalmazottak viselkedésére vezethető vissza.[12] A legmodernebb és legerősebb vírusirtórendszerek, szabályozások és egyéb védelmet célzó intézkedések ellenére, az alkalmazottak közül elég, ha csak egy valaki kaput nyit a támadók próbálkozásainak, mert ezáltal támadhatóvá válik a rendszer.[13] A technológiai biztonsági megoldásokra támaszkodva ezért soha nem tudjuk megfelelően megvédeni rendszereinket.[14] Fontos, hogy megértsük a megfelelő biztonsági viselkedéshez kapcsolódó emberi tényezőket, hogy ne csak a sebezhetőséget csökkentsük, hanem olyan képzési és oktatási programokat is tervezhessünk, amelyek ezeket a mögöttes tényezőket kezelik.

A *social engineering*[15] olyan támadásokra vonatkozik, amelyek során az embereket szándékosan manipulálják, hogy bizalmas információkat adjanak ki, vagy a támadó által kiszemelt személy vagy vállalat biztonságát veszélyeztető cselekményeket hajtsanak végre.[16] A támadás arra épít, hogy az egyének hiszékenyek és manipulálhatók.[17] A social engineering támadások fizikai, társadalmi és technikai szempontokat is tartalmaznak, amelyeket a támadás különböző fázisaiban használnak. Még ha egy ilyen támadás kezdetben sikertelen is, az egyéni és szervezeti biztonsági folyamatokba való betekintés felhasználható a jövőbeli támadásokhoz. A social engineerek olyan technikákat használnak, mint a célzott (szigonyozó) adathalászat *([spear] phishing),* a látszatüzenet, vagy egy kifejezőbb kifejezést használva operatív csapda *(pretexting),*[18] a célcsoport weboldalainak megfertőzése, a befurakodás *(water holing),* az adatkiszivárogtatás *(data breach),* a csalás *(scam),*[19] vagy a személyes adatokhoz, védett rendszerekhez való hozzáférés. Az adathalászat során a támadók főként e-mailek formájában szereznek az áldozataikról információkat, amelyet

[11] Samar Muslah Albladi – George R. S. Weir: User Characteristics that Influence Judgment of Social Engineering Attacks in Social Networks. *Human-centric Computing and Information Sciences,* 8. (2018), 1.

[12] Reza Alavi – Shareeful Islam – Haralambos Mouratidis: An Information Security Risk-Driven Investment Model for Analysing Human Factors. *Information & Computer Security,* 24. (2016), 2. 205–227.

[13] Sonja Stirnimann: *Der Mensch als Risikofaktor bei Wirtschaftskriminalität: Handlungsfähig bei Non-Compliance und Cyberkriminalität*. Wiesbaden, Springer, 2018.

[14] Steven Furnell – Kieran Millet – Maria Papadaki: Fifteen Years of Phishing: Can Technology Save Us? *Computer Fraud & Security,* (2019), 7. 11–16.

[15] A *social engineeringnek* nincs tudományos körökben széleskörűen elfogadott magyar megfelelője.

[16] Deanna Hauser: Social Engineering Awareness in Business and Academia. In *MWAIS 2016 Proceedings.* Wisconsin, 2016. 3–6.

[17] Oroszi Eszter Diána: Social engineering technikák. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 77–118.

[18] Magyar Sándor: *Adatbiztonság, adatvédelem az egészségügyben.* Előadás. Semmelweis Egyetem, 2019. március 4.

[19] Soudabeh Vahdati – Niloofar Yasini: Factors Affecting Internet Frauds in Private Sector: A Case Study in Cyberspace Surveillance and Scam Monitoring Agency of Iran. *Computers in Human Behavior,* 51. (2015), 180–187.

a későbbiekben akár egy további látszatüzenet keretében való támadás alkalmával felhasználnak. A célzott adathalászat esetében a célközönség szűkebb. A befurakodás során a célszemély által gyakran látogatott weboldalakat törik fel, és helyeznek el rajta vírust azzal a céllal, hogy így fertőzzék meg az áldozat számítógépét, vagy jussanak be a munkahelyi hálózatára.[20] Az adatkiszivárogtatás külső fél elektronikus vagy offline, sokszor titkos adatokhoz való szándékos vagy nem szándékos hozzáférése.[21] Az internetes csalás célja az áldozat(ok) becsapása,[22] amelynek során a csaló különböző módszereket alkalmaz az áldozatok személyes információinak ellopására és pénzügyi tranzakciók elvégzésére.[23] Ennek egyik legismertebb típusa az online vásárlásokhoz kapcsolódó csalás, amelynek során a csalók összegyűjtik az internetfelhasználók hitel- vagy bankkártyaadatait és PIN-kódját, amelyeket arra használnak, hogy pénzt hívjanak le az áldozat számlájáról.[24]

A social engineering biztonsági kockázataival kapcsolatos ismeretekkel nem rendelkező alkalmazottak a vállalat legnagyobb kockázatai közé tartoznak.[25] Jelen tanulmány az Y generációra fókuszálva kutatja az információbiztoság-tudatosság főbb tényezőit, hátterét.

3. Módszertan

Kvalitatív megközelítést, mélyinterjúkat alkalmaztunk a kutatási probléma mélyebb megértésére. A mélyinterjú lehetővé teszi, hogy a biztonságtudatosságot a fentiekben bemutatottaktól eltérő módon közelítse meg a tanulmány. Ez a módszertan hozzájárul a kutatási probléma és különösen annak érzékenyebb területe feltárásához.[26]

A vizsgálat eszközeként félig strukturált interjúkon keresztül tártuk fel az interjúalanyok információbiztonság-tudatosságának és az érzékelt kockázatnak a főbb tényezőit, illetve attitűdjüket.

Az interjúk átiratait tartalomelemzéssel és *grounded theory* (GT-) módszertannal, azaz megalapozott elmélettel elemeztük. A tartalomelemzés Krippendorff szerint egy komplex technika, amelynek segítségével a kutató nemcsak a szöveget, hanem a szöveg kontextusát is figyelembe véve értelmez és értékel.[27] A módszer lényege,

[20] Szappanos Gábor: Kártékony kódok használata a célzott támadások végrehajtásában. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 119–159.

[21] Freeha Khan et al.: Data Breach Management: An Integrated Risk Model. *Information & Management,* 58. (2021), 1. 103392.

[22] Tom Buchanan – Monica T. Whitty: The Online Dating Romance Scam: Causes and Consequences of Victimhood. *Psychology, Crime & Law,* 20. (2013), 3. 261–283.

[23] Vahdati–Yasini (2015): i. m. 31.

[24] Arokia Jesu Prabhu Lazar et al.: Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications,* (2021).

[25] Jéri Tamás: Az elektronikus levelezés és a kiberbiztonság összefüggései. *Hadmérnök,* 16. (2021), 2. 169–185.

[26] Hanna Kallio et al.: Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide. *Journal of Advanced Nursing,* 72. (2016), 12. 2954–2965.

[27] Klaus Krippendorff: *Content Analysis. An Introduction to Its Methodology*. Thousand Oaks, SAGE, 2018.

hogy az interjúkban elhangzottakból induktív módon következtetünk az elhangzottak mögött megbújó, rejtett gondolatokra, tartalmakra, ezáltal felfedjük az elsőre nem észrevehető összefüggéseket.[28] Ugyanakkor az elméleti megközelítés integrációjával abduktív megközelítést alkalmazunk. Az alapvetően kvalitatív jellegű tartalomelemzés lehetővé teszi a narratívák alapján a kutatás szempontjából releváns tényezők feltárását, azonosítását.[29]

A GT-módszertan lényege, hogy a kvalitatív adatok értelmezéséből jutunk el az elmélethez közeli általánosabb szintű megfogalmazásokig. Mint a szövegelemzési módoknál, itt is lényeges hangsúly van a kódoláson és az elemzésen, akárcsak a kutatón, ami általában a kvalitatív kutatások egyik korlátozó tényezője.[30]

A félig strukturált interjúk során projektív technikák közül is alkalmaztunk két módszer, a szóasszociáción alapuló módszert, illetve a mondatkiegészítési technikát. A szóasszociáció lényege, hogy az elhangzott ingerszavakra a vizsgált alany a számára elsőként eszébe jutó gondolatot adja meg.[31] A mondatkiegészítés során alkalmazott nyitott mondatok, amelyeket az alanyoknak kell befejezni korlátlan és változatos válaszokat eredményeznek.[32] A projektív technikák révén kapott eredményeket beépítettük az elemzésbe.

3.1. A minta

Az interjúalanyok kiválasztása során szűrőkritériumot alkalmaztunk. Az Y generáció tagjait, vagyis az 1980–1994 között születetteket kértük fel. A megkérdezett interjúalanyok közül kettő a szakmai hátterét, illetve tapasztalatait tekintve kiemelkedik a többiek közül, hiszen a biztonságtudatosságot tekintve a többiekhez képest messzemenően mélyebb információkkal rendelkeznek a témában.

Az interjúk során 11 személlyel, 7 nővel és 4 férfival, foglalkozásukat tekintve 5 tanulóval és 6 munkavállalóval készítettünk interjút. Az elméleti telítődést ezzel a mintával jól sikerült közelíteni, miután az interjúalanyok válaszai már a hetedik válaszadót követően összecsengtek. Az életkor terjedelem 27–40 év. Az aktuális pandémiás helyzet miatt az interjúk átlagosan 1–1,5 óráig online formában zajlottak.

[28] Ehmann Bea – Balázs László: A Sarkvidéktől a világűrig: A pszichológiai tartalomelemzés alkalmazása izolált kiscsoportok vizsgálatára. *Magyar Pszichológiai Szemle,* 70. (2015), 4. 723–742.
[29] Kelemen-Erdős Anikó – Molnár Adél: Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units. *Economics and Culture,* 16. (2019), 1. 58–69.
[30] Szokolszky Ágnes: *A pszichológiai kutatás módszertana*. Budapest, Osiris Kiadó, 2020.
[31] Lewis R. Aiken – Gary Groth-Marnat: *Psychological Testing and Assessment*. Boston, Allyn and Bacon, 2006.
[32] Horváth Dóra – Mitev Ariel Z.: *Alternatív kvalitatív kutatási kézikönyv.* Budapest, Alinea Kiadó, 2015.

4. Eredmények

A kutatási eredmények elemzésének első fázisában kvalitatív tartalomelemzést alkalmaztunk. Ennek keretében narratívák segítették elő az eredmények vizsgálatát. Ezt követően az elemzést *grounded theory* módszertannal végeztük.

4.1. Eredmények kvalitatív tartalomelemzés alapján

Az interjúalanyok digitális eszközökkel való kapcsolata úgy jellemezhető, hogy az a mindennapjaik szerves része, mondhatni létszükséglet mind a munkát, mind a magánéletet tekintve, annak ellenére, hogy igyekeznek offline módon is kikapcsolódni azért, hogy legalább a magánéletükben egyensúlyt tudjanak teremteni az offline és online tér között. Az interjúalanyok számára az információbiztonság az adatvédelemmel és az információmegosztás feletti kontrollal, valamint az információs önrendelkezéssel hozható kapcsolatba. Az információbiztonság „… nagyon fontos, pozitív dolog, amiért érdemes tenni…" (I3). Két olyan vélemény is elhangzott azonban, amelyek szerint figyelni kell az adataink és az okoseszközeink védelmére, annak ellenére, hogy ez „néha túl komplikált" (I4). Ez a biztonság percepciójának komplexitására utal.

4.1.1. A digitális eszközök használatának potenciális kockázatai

A válaszadók által azonosított észlelt kockázat főként a személyes adataik illetéktelenek általi megszerzésére, illetve az azokkal való visszaélésre vonatkoztak, azonban többen is megemlítették mint potenciális veszélyt az emberi felelőtlenséget, felkészületlenséget. Az alanyok által érzékelt digitális kockázatokat és a kockázatforrásokat az 1. táblázat tartalmazza.

A kockázatokkal összefüggésben a potenciális áldozatok körére is kitértek az interjúk, ahol elmondható, hogy az alanyok két gondolatsíkon fogalmazták meg válaszaikat. Egyrészt azt hangsúlyozták, hogy bárkiből lehet áldozat, illetve azt hogy, melyek azok az egyéni jellemzők, amelyek hozzájárulnak egy-egy személy kitettségének növekedéséhez. „A veszélyek nagyrészt a védekezés hiányából, emberi naivságból és lustaságból adódnak." (I4); „Sokan azt hiszik, hogy nekik nem lehet bajuk. A legtöbb ember még vírusirtót sem használ." (I6); „Miután feltörték a cégem rendszerét, az adataim többsége elveszett, új megoldásokat kerestem, most már tudatosabb vagyok." (I8). Másrészt az alanyok az áldozatok és elkövetők közötti elmosódó határvonalat hangsúlyozták, valamint az ipari, vállalati sebezhetőségre asszociáltak. „Vannak egyértelmű helyzetek, amikor elkülöníthető az áldozat és az elkövető […] nagyon sok esetben azonban a határok nem ilyen élesek […]. A GDPR rengeteg adatkezelési dolgot szabályoz, de a vállalatok felé semmiféle hivatalos elvárást nem támasztanak a hatóságok kiberbiztonsági szempontból." (I6).

1. táblázat: Az interjúalanyok által érzékelt digitális kockázatok

A kockázat forrása	Digitális kockázat – interjúrészlet
Emberi tényező	„az ember a leggyengébb láncszem, nem is a különböző jelszavak, tűzfalak, biztonsági megoldások" (I1); „elhúzzák az orra előtt a mézesmadzagot és ráharap…" (I3); „a felelőtlen viselkedés" (I4); „tudatlanság, nemtörődömség," (I3); „a kíváncsiság, felelőtlen kattintgatás" (I3); „egy része emberi hülyeség, másik része emberi lustaság, vagy szimplán felkészületlenség, plusz a távmunkát is idesorolnám" (I6); „amikor nem saját gépen kell bejelentkezned valamelyik e-mail-fiókodba, és utána elfelejtesz kijelentkezni" (I10);
Nem megfelelő technológiai adottságok	„webes alkalmazások, mobileszközök, végpontok és szerverek sérülékenysége – védelmi hiányosságok és egyéb technikai jellemzők, hozzáférési problémák" (I6)
Social engineering	*„a különböző social engineering technikák"* (I5)
potenciális adatsértés *(data breach)*	„jelszó meg hozzáférési adatok kiszivárogtatásáról vagy megszerzéséről" (I5)*;* „a különböző cégek adatokat gyűjtenek rólunk" (I2); „tudnak rólunk mindent, […] mindenhová követnek, hogy ez legális-e, nem tudjuk azonosítani." (I8); „Gyakran kapok olyan spameket, amit a spamszűrő nem ismer fel. Több levél megpróbálja elérni, hogy válaszoljak rá azért, hogy ellopja a jelszavaimat." (I11) „adatlopás (anyagi haszonszerzés, know-how-k megismerése, ipari kémkedés, zsarolás stb.)" (I6)
internetes csalás *(scam)*	„egyrészt megpróbálnak pénzt kicsalni az emberből, információt megtudni módszerek" (I1); „ellopják a kártyaadataimat, jelszavaimat, a személyes adataimat"; „már ellopták a kártyaadataimat valószínűleg" (I7); „visszaélhetnek az adataimmal" (I2); „elvesznek az adataim, vagy ellopják őket" (I4)
adathalászat *(phising)*	„a különböző felhasználói fiókok feltörése" (I1); „az adathalászati módszerek" (I4, I5); „a közösségimédia-profilok feltörése meg a kamuprofilok" (I9); „adatlopás (anyagi haszonszerzés, know-how-k megismerése, ipari kémkedés, zsarolás stb.)" (I6)
internetes befurakodás *(water holing)*	„bizonyos oldalak megnyitásával vírus kerülhet a gépünkre." (I11)

Forrás: a szerzők szerkesztése

4.1.2. Információbiztonság-tudatosság

Az információbiztonság-tudatos személy az interjúalanyok számára ismeri a rá leselkedő veszélyeket, tudja, hogy egyes tevékenységei, tettei mivel jár(hat)nak, valamint érti is ezeket. „Tisztában van a veszélyekkel, azzal hogy melyik lépésnek milyen következményei lehetnek, pl. ha az egyes internetes oldalakon elfogadja a sütiket…, érti is,,hogy miről van szó, illetve szem előtt tartja azt is, hogy semmi sincs ingyen, a kérdés csak az, hogy ezt hol és mivel fizeted meg." (I1) A tudatosság kapcsán egyéni tulajdonságokat is megemlítettek a válaszadók, miszerint olvasatukban egy információbiztonság-tudatos egyén kritikus gondolkodású, óvatos, felelősségteljes, mértékletes, és többnyire naprakész tudással rendelkezik a témában.

A biztonság növelése, vagy épp a sebezhetőség mértékének csökkentése kardinális kérdés az adatok védelmét tekintve. Az az érdekes következtetés vonható le, hogy

az általunk megkérdezett személyek főként a legalapvetőbb és talán a legnépszerűbb védekezési módokat gyakorolják, mint a bonyolult jelszavak és a biztonsági mentések.

„Igyekszem tudatosan többféle jelszót használni és próbálom nem a hétköznapi életből vett adatokat alkalmazni (pl. születési dátum, nevek), amelyek tartalmaznak speciális karaktereket. A több e-mail-cím használata is kifizetődő tud lenni, mindegyik egy-egy célra (egy magáncélra, egy munkaügyben stb.)." (I4); „Minimum egy vírusirtó használata azért ajánlatos, az adataimról, a különböző fájlokról van biztonsági mentésem a felhőben is és egy külső merevlemezen is, bár ezeknek a frissítése nem mindig rendszeres" (I3).

A kiszolgáltatottság csökkentésére egy-egy interjú során még említették a zárt rendszerek használatát, a hozzáférés korlátozását akár az interneten, közösségi médiában megosztott információkat tekintve, akár a munkahelyi hálózaton az egyes mappákat, dokumentumokat tekintve, továbbá a rendszeres sérülékenységvizsgálatát. A válaszokat tekintve meglepő, hogy az alanyok csak egy-két esetben tértek ki akár egyéni, akár szervezeti szinten az oktatásra, képzésekre, amelyek a felhasználók digitális tudását hivatottak növelni, ezáltal is csökkentve a kockázatot.

4.1.3. Potenciális kibertámadás lehetséges következményeinek értékelése

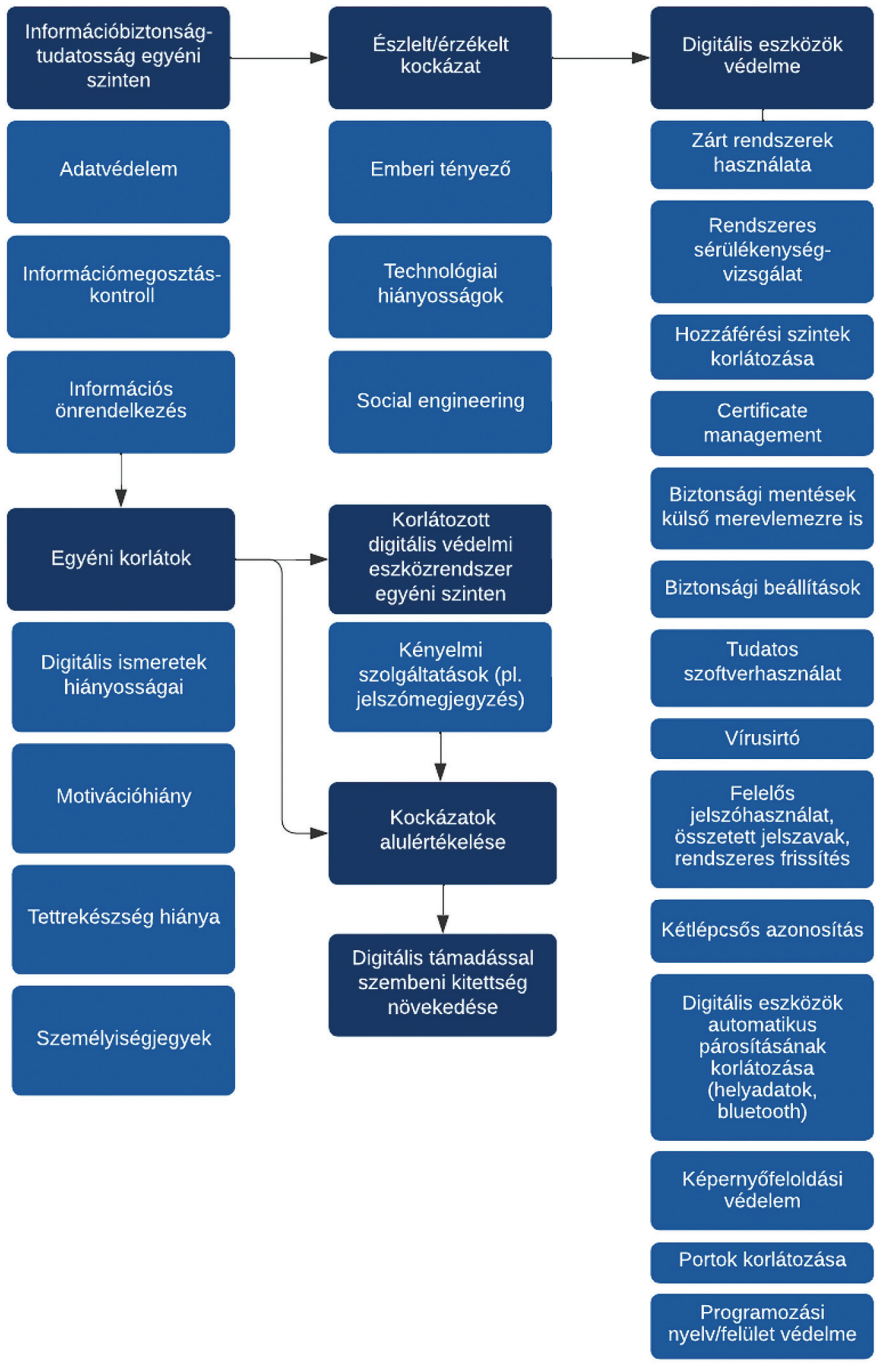
Egy esetleges kibertámadás potenciális következményeit is vizsgáltuk az adott alanyra nézve, illetve vállalati szinten. A felhasználók magukra nézve leginkább az anyagi kárt említették meg, míg a munkavállalók az anyagi kár mellett a jogi és presztízsbeli következményeket is említették.

„Mindig az anyagi kárról szól alapvetően, kivéve, ha valaki olyan személyről van szó […] és őt zsarolni, bár az is tulajdonképpen pénzre fordítható dolog, de szerintem alapvetően mindig a pénz körül forog." (I3); „Szinte elölről kéne kezdeni mindent, ez hatalmas anyagi ráfordítással járna, valószínűleg a vállalatoknál is, mivel esetükben akár hátrányba is kerülhetnek a versenytársakkal szemben, elveszthetik a vevőiket, meg persze a jogi következmények." (I2).

4.2. Eredmények grounded theory (GT-) módszertan alapján

Az interjúk vizsgálata abduktív módon történt, a *grounded theory* módszertan alapján. A GT szerinti elemzés során az interjúk egészére vonatkozó visszatérő motívumok keresése a fő mozzanat, ezt követően az egyes interjúkban beazonosított mintákat a többi interjúban is be kell azonosítani és összehasonlítani egymással, majd szükséges a kapcsolatokra rávilágítani, illetve szűrni az egyes tényezők között alkalmazva. A cél egy modell vagy keretrendszer felállítása, amely az adatok definiálása során integrálja az elméleti (szakirodalmi) tényezőrendszert is. A GT esetében egy négyszintű kódrendszer állítható fel, amelynek szintjei a következők: nyílt kódok, axiális, szelektív és teoretikus kódok.[33] Az 1. ábra a kódok hierarchikus rendszere, valamint a képzett fő kategóriák alapján definiálható modellt mutatja be.

[33] Szokolszky (2020): i. m. 42.



1. ábra: Információbiztonság-tudatosság grounded theory módszertan alapján
Forrás: a szerzők szerkesztése a mélyinterjúk alapján, N = 11

5. Összegzés

A kutatás célja az volt, hogy képet adjon az Y generációs felhasználók információbiztonság-tudatosságáról, kiberbiztonsággal és kibertámadásokkal kapcsolatos asszociációiról, attitűdjéről. Bár a jelen kutatás kvalitatív jellegéből adódóan nem minősül reprezentatívnak, nem tesz lehetővé általánosítást, illetve nem vonhatók le az eredményekből messzemenő következtetések, alapozó kutatásként hasznosítható eredményekkel szolgálhat. További vizsgálat, vállalatvezetők körében végzett szakértői mélyinterjú elősegítené a téma megközelítését más szemszögből.

A kutatás egyik legfontosabb eredménye, hogy az alanyok annak ellenére, hogy eltérő mértékben és mélységben rendelkeznek információkkal a különböző kibertámadásokról, azok módjáról, következményeiről, valamint azok kiváltó okairól, könnyelműen bánnak saját és személyes adataik védelmével. Egyes kutatások szerint az egyén biztonságtudatosságára a közvetlen környezetéhez való viszonya, gondolkodásmódja is hatással van,[34] mások szerint a személyiségjegyek is befolyásoló tényezőknek minősülnek.[35]

Az interjúalanyok biztonságtudatossága nem megfelelő szintű, esetenként az információbiztonsággal kapcsolatos ismereteikhez, tudásukhoz képest messze elmarad. Ezzel több nemzetközi kutatás is egybecseng, Hanus Bartlomiej és szerzőtársai[36] szerint a fenyegetések ismerete mit sem ér, ha a felhasználó nem képes felismerni és használni azokat az eszközöket, amelyek a védelmét szolgálják. Burcu Bulgurcu és munkatársai a szabályok mögötti okok megértését is kiemelik, azaz a tudatos viselkedést elősegíti, ha a felhasználó érti, mit miért tehet, vagy nem tehet.[37]

Az előzőkkel kapcsolatban álló újszerű eredmény, hogy az alanyok alulértékelik saját sebezhetőségüket. Az interjúalanyok annak ellenére, hogy saját elmondásuk alapján bárki lehet az emberi tényezőt kihasználó spam és *social engineering* áldozata, mégis úgy érzik, nem tartoznak különböző okok miatt (munkahely, jövedelem, online aktivitás stb.) ezek célpontjai közé, például „nem érdeklek senkit, hogy az én adataimra kíváncsiak legyenek" (I2). A nemzetközi kutatásokból egyértelműen kiderül, hogy a felhasználók kockázatérzékelése nagymértékben előrejelzi az online térben való viselkedést és a kiberbiztonság kérdéséhez való hozzáállást.[38]

További eredmény, hogy a kibertámadásokkal kapcsolatos személyes tapasztalatok nagyban befolyásolják a biztonságtudatosságot és a sebezhetőség megítélését. A 11 válaszadó közül három tapasztalt a saját eszközeihez, adataihoz kapcsolódóan

[34] Charlette Donalds – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020), 102056; Réka Saáry – Ágnes Csiszárik-Kocsir – János Varga: Examination of the Consumers' Expectations Regarding Company's Contribution to Ontological Security. *Sustainability,* 13. (2021), 17. 9987.

[35] Jaime Ortiz et al.: The Contradiction between Self-Protection and Self-Presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017). 406–416.

[36] Bartlomiej Hanus – Yu "Andy" Wu: Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management,* 33. (2015), 1. 2–16.

[37] Burgurcu et al. (2010): i. m. 29

[38] Mark J. Keith et al.: Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus with Actual User Behavior. *International Journal of Human-Computer Studies,* 71. (2013), 12. 1163–1173.; Ardion D. Beldad: Sharing to be Sociable, Posting to be Popular: Factors Influencing Non-Static Personal Information Disclosure on Facebook among Young Dutch Users. *International Journal of Web Based Communities,* 11. (2015), 3–4. 357–374.

kibertámadást, amelynek következtében azóta fokozottan ügyel a kiberbiztonságra. A kibertámadásokkal kapcsolatos tapasztalat és a biztonságtudatosság szintje közötti összefüggést más tanulmányok is megerősítik.[39]

Az oktatás hozzájárulhat az egyének információbiztonság tudatosságának növeléséhez, amelyet már az általános iskolai képzésbe célszerű integrálni. Ennek során érdemes újabb interaktív módszerekkel, illetve játékosítással (gamifikációval) egyéni elkötelezettséget kiváltani, amely támogatja a későbbi tudatos magatartást az egyének és a vállalatok tevékenysége során.[40] A képzési programok, illetve ennek eredményeként az információbiztonság-tudatosság növekedésének társadalmi és gazdasági haszna egyaránt jelentős.

Köszönetnyilvánítás

A kutatás az Innovációs és Technológiai Minisztérium ÚNKP-21-3 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

Felhasznált irodalom

Ahlan, Abdul Rahman – Muharman Lubis – Arif Ridho Lubis: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science,* 72. (2015). 361–373. Online: https://doi.org/10.1016/j.procs.2015.12.151

Aiken, Lewis R. – Gary Groth-Marnat: *Psychological Testing and Assessment.* Boston, Allyn and Bacon, 2006.

Alavi, Reza – Shareeful Islam – Haralambos Mouratidis: An Information Security Risk-Driven Investment Model for Analysing Human Factors. *Information & Computer Security,* 24. (2016), 2. 205–227. Online: https://doi.org/10.1108/ICS-01-2016-0006

Albladi, Samar Muslah – George R. S. Weir: User Characteristics that Influence Judgment of Social Engineering Attacks in Social Networks. *Human-centric Computing and Information Sciences,* 8. (2018). 1. Online: https://doi.org/10.1186/s13673-018-0128-7

Bak Gerda – Kiss Sándor: A biztonságtudatosság szisztematikus szakirodalmi áttekintése. *Hadmérnök,* 16. (2021), 4. 85–99. Online: https://doi.org/10.32567/hm.2021.4.7

Beldad, Ardion D.: Sharing to be Sociable, Posting to be Popular: Factors Influencing Non-Static Personal Information Disclosure on Facebook among Young Dutch Users. *International Journal of Web Based Communities,* 11. (2015), 3–4. 357–374. Online: https://doi.org/10.1504/IJWBC.2015.072132

[39] Lennart Jaeger – Andreas Eckhardt: Eyes Wide Open: The Role of Situational Information Security Awareness for Security–Related Behaviour. *Information Systems Journal,* 31. (2021), 3. 429–472.

[40] Kovács László et al.: Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program. *AARMS,* 16. (2017), 1. 5–16.

Buchanan, Tom – Monica T. Whitty: The Online Dating Romance Scam: Causes and Consequences of Victimhood. *Psychology, Crime & Law,* 20. (2013), 3. 261–283. Online: https://doi.org/10.1080/1068316X.2013.772180

Bulgurcu, Burcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34. (2010), 3. 523–548. Online: https://doi.org/10.2307/25750690

Donalds, Charlette – Kweku-Muata Osei-Bryson: Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents. *International Journal of Information Management,* 51. (2020). 102056. Online: https://doi.org/10.1016/j.ijinfomgt.2019.102056

Ehmann Bea – Balázs László: A Sarkvidéktől a világűrig: A pszichológiai tartalomelemzés alkalmazása izolált kiscsoportok vizsgálatára. *Magyar Pszichológiai Szemle,* 70. (2015), 4. 723–742. Online: https://doi.org/10.1556/0016.2015.70.4.2

Furnell, Steven – Kieran Millet – Maria Papadaki: Fifteen Years of Phishing: Can Technology Save Us? *Computer Fraud & Security,* (2019), 7. 11–16. Online: https://doi.org/10.1016/S1361-3723(19)30074-0

Grant, Kevin – David Edgar – Arun Sukumar – Martin Meyer: 'Risky Business': Perceptions of E-Business Risk by UK Small and Medium Sized Enterprises (SMEs). *International Journal of Information Management,* 34. (2014), 2. 99–122. Online: https://doi.org/10.1016/j.ijinfomgt.2013.11.001

Hanus, Bartlomiej – Yu "Andy"Wu: Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management,* 33. (2015), 1. 2–16. Online: https://doi.org/10.1080/10580530.2015.1117842

Hauser, Deanna: Social Engineering Awareness in Business and Academia. In *MWAIS 2016 Proceedings.* Wisconsin, 2016. 3–6.

Horváth Dóra – Ariel Mitev: *Alternatív kvalitatív kutatási kézikönyv.* Budapest, Alinea Kiadó, 2015.

Hutchinson, Gershon – Jacques Ophoff: A Descriptive Review and Classification of Organizational Information Security Awareness Research. In H. Venter – M. Loock – M. Coetzee – M. Eloff – J. Eloff (szerk.): *Information and Cyber Security.* Cham, Springer, 2020. 114–130. Online: https://doi.org/10.1007/978-3-030-43276-8_9

Jaeger, Lennart – Andreas Eckhardt: Eyes Wide Open: The Role of Situational Information Security Awareness for Security–Related Behaviour. *Information Systems Journal,* 31. (2021), 3. 429–472. Online: https://doi.org/10.1111/isj.12317

Jéri Tamás: Az elektronikus levelezés és a kiberbiztonság összefüggései. *Hadmérnök,* 16. (2021), 2. 169–185. Online: https://doi.org/10.32567/hm.2021.2.12

Kallio, Hanna – Anna-Maija Pietilä – Martin Johnson – Mari Kangasniemi: Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide. *Journal of Advanced Nursing,* 72. (2016), 12. 2954–2965. Online: https://doi.org/10.1111/jan.13031

Keith, Mark J. – Samuel C. Thompson – Joanne Hale – Paul Benjamin Lowry – Chapman Greer: Information Disclosure on Mobile Devices: Re-Examining Privacy Calculus

with Actual User Behavior. *International Journal of Human-Computer Studies,* 71. (2013), 12. 1163–1173. Online: https://doi.org/10.1016/j.ijhcs.2013.08.016

Kelemen-Erdős, Anikó – Adél Molnár: Cooperation or Conflict? The Nature of the Collaboration of Marketing and Sales Organizational Units. *Economics and Culture,* 16. (2019), 1. 58–69. Online: https://doi.org/10.2478/jec-2019-0007

Kelemenné Erdős Anikó: A közforgalmú közlekedési szolgáltatás és piac vizsgálata marketing és fenntarthatósági nézőpontból. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2014.

Khan, Freeha – Jung Hwan Kim – Lars Mathiassen – Robin Moore: Data Breach Management: An Integrated Risk Model. *Information & Management,* 58. (2021), 1. 103392. Online: https://doi.org/10.1016/j.im.2020.103392

Krippendorff, Klaus: *Content Analysis – An Introduction to Its Methodology.* Thousand Oaks, SAGE, 2018. Online: https://doi.org/10.4135/9781071878781

Lazar, Arokia Jesu Prabhu – Sudhakar Sengan – Luigi Pio Leonardo Cavaliere – Thillaiarasu Nadesan – Deepesh Sharma – Mukesh Kumar Gupta – Thangam Palaniswamy – Mahendiran Vellingiri – Dilip Kumar Sharma – Thirukumaran Subramani: Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud. *Wireless Personal Communications,* (2021). Online: https://doi.org/10.1007/s11277-021-08585-y

Oroszi Eszter Diána: Social engineering technikák. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 77–118. Online: https://bit.ly/3D5AqlD

Ortiz, Jaime – Shu-Hao Chang – Wen-Hai Chih – Chia-Hao Wang: The Contradiction between Self-Protection and Self-Presentation on Knowledge Sharing Behavior. *Computers in Human Behavior,* 76. (2017). 406–416. Online: https://doi.org/10.1016/j.chb.2017.07.031

Parsons, Kathryn – Agata McCormac – Marcus Butavicius – Malcolm Pattinson – Cate Jerram: Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security,* 42. (2014). 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Saáry, Réka – Ágnes Csiszárik-Kocsir – János Varga: Examination of the Consumers' Expectations Regarding Company's Contribution to Ontological Security. *Sustainability,* 13. (2021), 17. 9987. Online: https://doi.org/10.3390/su13179987

Stirnimann, Sonja: *Der Mensch als Risikofaktor bei Wirtschaftskriminalität: Handlungsfähig bei Non-Compliance und Cyberkriminalität.* Wiesbaden, Springer, 2018. Online: https://doi.org/10.1007/978-3-658-20813-4

Szappanos Gábor: Kártékony kódok használata a célzott támadások végrehajtásában. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 119–159. Online: https://bit.ly/3z4dl1J

Szokolszky Ágnes: *A pszichológiai kutatás módszertana.* Budapest, Osiris Kiadó, 2020.

Tari Annamária: *Y generáció. Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban.* Budapest, Jaffa Kiadó, 2010.

Vahdati, Soudabeh – Niloofar Yasini: Factors Affecting Internet Frauds in Private Sector: A Case Study in Cyberspace Surveillance and Scam Monitoring Agency of Iran. *Computers in Human Behavior,* 51. (2015). 180–187. Online: https://doi.org/10.1016/j.chb.2015.04.058

Zhongping, Zeng – Yang Kaifeng – Zhang Yi – Zhou Peipei: Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management. In *2013 Fourth International Conference on Digital Manufacturing & Automation.* IEEE, 2013. 684–687. Online: https://doi.org/10.1109/ICDMA.2013.162

Zimmermann, Verena – Karen Renaud: Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindset. *International Journal of Human-Computer Studies,* 131. (2019). 169–187. Online: https://doi.org/10.1016/j.ijhcs.2019.05.005

HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 97–107.
DOI: 10.32567/hm.2022.3.7

Bihaly Barbara[1]

A mesterséges intelligencia felhasználása az információs és kibertérműveletekben – az orosz minta

Use of Artificial Intelligence in Information and Cyberspace Operations – The Russian Way

Napjainkban a legnagyobb veszély nem a kinetikus, hanem az információs térből érkezik. Az orosz hadsereg számára a védelmi eszköztár fő fegyvere az információ. Az információs műveletek koncepciója különleges helyet foglal el az orosz (és előtte a szovjet) katonai gondolkodásmódban. A mesterséges intelligencia mint a következő meghatározó technológia már a hadviselésben is megjelent. Az orosz hadsereg a mesterséges intelligencia katonai felhasználására való fejlesztésével beszállt az új típusú fegyverkezési versenybe, sajátos gondolkodásmódjával pedig új szintre léptette azt.

Kulcsszavak: **mesterséges intelligencia, hadviselés, Oroszország**

Nowadays, the biggest danger is not kinetic, but comes from the information space. For the Russian army, the main weapon of the defence toolbox is information. The concept of information operations occupies a special place in the Russian (and before that Soviet) military mindset. Artificial intelligence, as the next defining technology, has already appeared in warfare. By developing artificial intelligence for military use, the Russian army entered a new type of armaments race and took it to a new level with a specific way of thinking.

Keywords: **artificial intelligence, warfare, Russia**

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: bihaly.barbara@hm.gov.hu

1. Bevezetés

A mesterséges intelligencia (MI) napjaink meghatározó technológiája lett, bár még sok kérdést felvet.

A 2019-ben kiadott orosz mesterségesintelligencia-stratégia a következőképpen definiálja a mesterséges intelligenciát:

„[t]echnológiai megoldások összessége, amely lehetővé teszi az emberi kognitív funkciók szimulálását (beleértve az öntanulást és a megoldások keresését előre meghatározott algoritmus nélkül), és olyan eredmények elérését, amelyek olyan konkrét feladatok elvégzése során érhetők el, amelyek legalább összehasonlíthatók az emberi szellemi tevékenység eredményeivel. A technológiai megoldások komplexuma információs és kommunikációs infrastruktúrát, szoftvereket (beleértve a gépi tanulási módszereket is használó szoftvereket), adatfeldolgozási és megoldáskeresési folyamatokat és szolgáltatásokat tartalmaz."[2]

Az orosz stratégia az MI hivatalosan elismert meghatározását úgy mutatja be, mint

„olyan technológiai megoldások összességét, amelyek lehetővé teszik az emberi kognitív funkciók szimulálását […], valamint olyan eredmények elérését a konkrét feladatok elvégzése során, amelyek legalább összehasonlíthatóak az emberi szellemi tevékenység eredményeivel. Ez a technológiai megoldáskészlet információs és kommunikációs infrastruktúrából, szoftverekből […], valamint adatkezelési eljárásokból és szolgáltatásokból áll".[3]

A stratégia hangsúlyozza a mesterséges intelligencia stratégiai jelentőségét, amely előfeltétele annak, hogy Oroszország bekerüljön a gazdasági világvezetők csoportjába, valamint az ország függetlensége és technológiai versenyképessége is nagyban függ tőle. Annak ellenére, hogy Oroszország jelenleg nem számít vezetőnek a mesterséges intelligencia területén (hisz az USA-t számítjuk ebben is vezető hatalomnak), a dokumentum kijelenti, hogy Oroszországnak lehetősége van arra, hogy „nemzetközi vezetővé váljon a mesterségesintelligencia-technológiák fejlesztésében és használatában".[4]

Az MI felhasználása elég széles körű lehetőségeket mutat az élet mindennapi területein és az ipari vagy a katonai szektorban egyaránt. Ennélfogva nem túlzó az állítás, miszerint az MI területén folyamatos nemzetközi fegyverkezési verseny zajlik. De amíg a nyugati katonai szervezetek a mesterséges intelligenciát elsősorban a taktikai terület elemének tekintik, az orosz hadsereg az MI legnagyobb hasznát stratégiai szinten látja. Az orosz fókuszpont a mesterséges intelligenciával továbbfejlesztett információs

[2] „искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений;" Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

[3] Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

[4] Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

műveleti eszközök alkalmazására irányul (beleértve a kibertéri műveleteket is) abból a célból, hogy mérhető stratégiai hatásokat érjenek el az ellenérdekelt államokkal szemben. Az MI ebben a minőségben való használata „harmadik forradalmat jelent a katonai ügyekben".[5]

Az MI az elkövetkező évek meghatározó technológiai trendje, tagadhatatlan hatása van a gazdaságra, a politikára és a társadalomra. Ezért a világ vezető államaiban kialakult az igény ennek a technológiának a fejlesztésére és felhasználására. Oroszországban nominálisan a hadsereg áll az ilyen témájú K+F élmezőnyében, a nyugati országokban és Kínában a fejlesztés a magánszektor sajátja. Elmondható tehát, hogy Oroszországban a hadsereg vezet jelenleg minden jellegű technológiai fejlesztésben.[6] A kiber- és információs képességeket használó rosszindulatú befolyásoló kampányok jelentős politikai zavart okoztak az egyes államok működésében (például létfontosságú infrastruktúra működésének zavarása, kormányzati rendszerek túlterhelése, dezinformációs kampányok stb.), de a kampányok következő generációja jelentősen károsabb lehet az MI széles körű használata miatt.

A kampányok sikeres lebonyolításának módszerei jelenleg (most még) függenek a mögöttük álló humán erőforrástól. A mesterséges intelligencia bevezetése nagymértékben javítani fogja a tömeges közönség személyre szabott és elfogadható tartalommal való elérése automatizálásának képességeit. Következésképpen még erőteljesebbé teszik a rosszindulatú szereplőket.

Jelen cikk célja bemutatni a mesterséges intelligencia információs és kibertér műveleti felhasználásának módjait az orosz hadviselés kontextusában.

2. A mesterséges intelligencia és lehetőségei a katonai szektorban

Ez a szakasz csupán néhány kiragadott példát mutat be, ahol az MI alkalmazható a katonai képességek fokozására.

Első példa a felderítés. A tengeri felügyeletet rögzített radarállomások, járőrrepülőgépek, hajók, valamint az utóbbi években az automatikus azonosító rendszert használó tengeri hajók elektronikus nyomon követését végzi az MI. Ezek az információforrások nagy mennyiségű adatot szolgáltatnak a hajók mozgásáról, ami illegális, nem biztonságos, fenyegető és rendellenes viselkedést tárhat fel. A hajómozgásokkal kapcsolatos nagy mennyiségű információ azonban megnehezíti az ilyen viselkedés észlelését, ha csupán emberi erőforrásra támaszkodunk. Ehelyett a gépi tanulási megközelítéseket használják arra, hogy különböző modelleket hozzanak létre a hajómozgások adataiból. A modellektől eltérő bármilyen egyéb mozgást rendellenesnek tekintik, és ellenőrzés céljából bemutatják az üzemeltetőknek.[7]

[5] Rod Thornton – Marina Miron: Towards the 'Third Revolution in Military Affairs'. The Russian Military's Use of AI-Enabled Cyber Warfare. *The RUSI Journal,* 165. (2020), 3. 12–21.

[6] Vooruzhennyye Sily RF Vnedryayut Tekhnologii Iskusstvennogo Intellekta. *Voenniye Materialy,* 2018. március 15.

[7] Peter Svenmarck et al.: Possibilities and Challenges for Artificial Intelligence in Military Applications. In *Proceedings of the 2018 NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*. 2018.

A modellek lehetővé teszik azoknak a hajóknak a felismerését, amelyek irányt váltanak, tengeri sávokat kereszteznek, ellentétes irányba vagy nagy sebességgel haladnak. A legújabb megközelítések a Bayes-hálózatokkal[8] fedezik fel a hamis hajótípust, valamint a szakaszos, lehetetlen és lebegő hajómozgást.[9] A tengeri anomáliák felderítése jövőbeli fejlesztéseinek figyelembe kell venniük a környező hajókat és a több hajó közötti kölcsönhatást is.

Második példa a gépi látás és a mély neurális hálózatokat (*deep neural network,* DNN) alkalmazó technológiák gyakorlati felhasználásának lehetősége a mélytengeri aknák felderítésében.

A víz alatti aknák komoly veszélyt jelentenek a tengeri hajókra, a mozgás irányítására vagy a korlátozott vizeken való áthaladás megakadályozására szolgálnak. Az aknakeresést egyre inkább autonóm víz alatti járművekkel (*autonomous underwater vehicle,* AUV) hajtják végre, amelyek olyan szintetikus apertúrájú szonárral (*synthetic aperture sonar,* SAS) vannak felszerelve, amelyek centiméteres felbontású akusztikus képeket nyújtanak a tengerfenékről. Mivel az AUV-k nagy mennyiségű SAS-képet gyűjtenek, az automatikus célosztályozás hasznos a potenciális aknák és más objektumok megkülönböztetéséhez. Míg az aknák automatikus célbesorolását hosszú ideje tanulmányozták, a DNN-ek nagy teljesítménye a képosztályozás során felvetette annak lehetőségét, hogy miként lehetnek alkalmasak az aknák automatikus észlelésére.

A DNN megtanítható az AUV- és az SAS-rendszerek által gyűjtött adatokkal, hogy milyen formájú egy próbaakna, milyen egy aknaszerű célpont, illetve milyen ember alkotta tárgyak találhatók meg a tengerfenéken. Az eredmények azt mutatják, hogy a DNN szignifikánsan nagyobb teljesítménnyel rendelkezik, nagyobb valószínűséggel észleli az aknák alakjait, és alacsonyabbak a téves riasztási arányok, mint egy hagyományos célosztályozó esetén.[10]

Harmadik példa a kiberbiztonság. A behatolásfelismerés a kiberbiztonság fontos része a rosszindulatú hálózati tevékenységek felderítéséhez. Erre fejlesztették ki az úgynevezett behatolásészlelő rendszert (*intrusion detection system,* IDS), amely a hálózati forgalmat elemzi és jelez a normálistól eltérő forgalom esetén. Mivel azonban a normális hálózati forgalomnak gyakran hasonló jellemzői vannak, mint a tényleges támadásoknak, ezeket szakemberek külön elemzik. Ugyanakkor, amíg az aláírás-alapú IDS-ek gyakran alkalmasak az ismert támadási minták észlelésére, nem képesek korábban nem látott támadásokat észlelni, ezért az aláírás-alapú észlelés fejlesztése gyakran lassú és költséges.[11] Ennek eredményeképpen ez akadályozza a rendszerek alkalmazkodóképességét a gyorsan fejlődő kiberfenyegetésekkel szemben.

[8] A bayesi hálózat (más néven a Bayes-hálózat, hiedelemhálózat, vagy döntési hálózat) egy valószínűségi grafikus modell, amely változók halmazát és azok feltételes függőségeit ábrázolja egy irányított aciklusos grafikonon (DAG) keresztül. A bayesi hálózatok ideálisak egy bekövetkezett esemény felvételére és annak valószínűségének előrejelzésére, hogy a lehetséges ismert okok bármelyike a hozzájáruló tényező. Lásd: https://hu.wiki4maps.com/438896-bayesian-network-CTDYOZ

[9] Steven Mascaro – Ann E. Nicholso – Kevin B Korb: Anomaly Detection in Vessel Tracks Using Bayesian Networks. *International Journal of Approximate Reasoning,* 55. (2014), 1. 84–98.

[10] David P. Williams: Underwater Target Classification in Synthetic Aperture Sonar Imagery Using Deep Convolutional Neural Networks. In *Pattern Recognition (ICPR), 2016 3rd International Conference,* Cancún, 2016. 2498–2503.

[11] Gulshan Kumar – Krishan Kumar – Monika Sachdeva: The Use of Artificial Intelligence Based Techniques for Intrusion Detection: A Review. *Artificial Intelligence Review,* 34. (2010), 4. 369–387.

Sok fejlesztés során használnak gépi tanulási (*machine learning,* ML) és más MI-hoz köthető technológiákat az ismert támadások osztályozási pontosságának növelésére, a rendellenes hálózati forgalom észlelésére (mivel ez új támadási mintákat jelezhet, amelyek eltérnek a normál hálózati forgalomtól), és automatizálják a modell felépítését.

E rendszerek közül azonban keveset használnak operatív módon. Ennek az oka, hogy az olyan kérdések, mint például a behatolások észlelése, olyan speciális kihívásokat jelentenek, mint az MI tanításához szükséges adatbázisok hiánya. Másik probléma általában a hálózati forgalom nagy változatossága, de a szükséges értékelések elvégzését is sokszor akadályozza a megfelelően képzett és mennyiségű szakértő hiánya. Noha nagy mennyiségű hálózati forgalom gyűjthető, az információk gyakran érzékenyek és csak részben névtelenek.[12]

A szimulált adatok használata egy másik lehetőség, de ezek gyakran nem elég valósághűek. Az adatokat kategorizálni kell a felügyelt tanuláshoz, azért, hogy eldönthető legyen, a minták a normális mintának megfelelnek-e, vagy behatolásnak számítanak-e. Végül a modelleknek átláthatóknak kell lenniük, hogy a kutatók megértsék a jellemzők észlelési határait és jelentőségét.[13]

A kiberbiztonság növelésének másik módszere a behatolási tesztek (*penetration test,* penetrációs teszt) elvégzése. A biztonsági auditok során a potenciálisan kihasználható biztonsági gyengeségeket azonosítják ezekkel a tesztekkel. A behatolási tesztek gyakran automatizáltak, mivel sok hálózat bonyolult és nagyszámú gazdagépet tartalmaz.

Jörg Hoffmann tanulmánya azt vizsgálta, hogyan lehet az MI-technikákat felhasználni szimulált penetrációs tesztelésre a hálózat logikai modelljeivel, nem pedig a tényleges hálózattal.[14] A hálózatot gyakran ábrázolják támadási grafikonok vagy fák, amelyek azt mutatják, az ellenfél hogyan tudja kihasználni a sebezhetőségeket, hogy behatoljon egy rendszerbe.

Hoffmann azonban leírja, hogy a modellek hogyan különböznek azok jellemzői alapján: a) a támadás függ az absztrakt sikertől, az észlelési valószínűségektől és a hálózati állapot bizonytalanságától, és b) a támadó cselekedetei függenek az ismert pre- és posztfeltételektől, az általános érzékeléstől és az eredmények megfigyelésétől.[15]

Ezenkívül a hálózatok és a gazdagépek formális modelljeivel lehetőség van a különböző mérséklési stratégiák elemzésére. A behatolási tesztelés jövőbeni kutatása valószínűleg kognitív módon érvényes modelleket fog felhasználni a támadó és a védő közötti interakcióról, például mélyreható tanulási módszerrel a lehetséges támadások nagy problématerületének feltárására.

[12] Carlos A. Catania – Carlos García Garino: Automatic Network Intrusion Detection: Current Techniques and Open Issues. *Computers & Electrical Engineering,* 38. (2012), 5. 1062–1072.

[13] Robin Sommer – Vern Paxson: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In *2010 IEEE Symposium on Security and Privacy (SP).* IEEE, 2010. 305–316.

[14] Jörg Hoffmann: Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In *Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS).* 25. (2015), 1. 364–372.

[15] Hoffmann (2015): i. m.

3. A mesterséges intelligencia katonai felhasználása Oroszországban

Nem volt meglepetés, hogy a mesterséges intelligencia megjelenésével Oroszország is beszáll a versenybe, hogy először használhassa katonai célokra az új képességet. Bár kezdetben az orosz beruházás mértéke elmaradt versenytársaiétól (Amerikai Egyesült Államok, Kína), a 2008-ban megkezdett szélesebb körű védelmi modernizációs erőfeszítések részeként az Orosz Katonai Ipari Bizottság célul tűzte ki, hogy a katonai felszerelések 30%-a 2025-re robotizálódjon.[16] 2016-ban az orosz kormány létrehozott egy védelmi kutató szervezetet, amely az Alapítvány a Haladó Tanulmányokért (Фонд перспективных исследований[17]) nevet viselte, és éves konferenciát kezdeményezett az „Orosz Föderáció fegyveres erőinek robotizálása" témában.[18] 2017-ben Oroszországból regisztrált a negyedik legtöbb felhasználó a Kaggle-re, a nyílt forráskódú platform mesterségesintelligencia-kutatásra.[19] Ez jól jelzi, amellett, hogy az orosz kockázati tőkések aktívan keresik a lehetőségeket a mesterségesintelligencia-piacon külföldön, hogy milyen komolyak az orosz szándékok a fegyverkezési versenyben.

Az orosz hadsereg számos védelmi alkalmazási módot kutat az MI felhasználására, nagy hangsúlyt fektetve az autonóm járművekre és a robotikára. 2017. november 1-jei hivatalos nyilatkozatában ezt alátámasztotta Viktor Bondarev, a Föderációs Tanács Védelmi és Biztonsági Bizottságának elnöke, amikor kijelentette, hogy „a mesterséges intelligencia képes lesz helyettesíteni a katonát a harctéren, a pilótát pedig a repülőgép pilótafülkéjében", és később bejelentette, hogy „közeleg a nap, amikor a járművek mesterséges intelligenciát kapnak".[20]

Bondarev ezeket a megjegyzéseket közvetlenül a Nerehta pilóta nélküli földi rendszer sikeres tesztje után tette. A moduláris jármű, amely a teszt során állítólag „felülmúlta a már meglévő ember vezette harci járműveket", képes egy 7,62 mm-es géppuska hordozására, és használható harci, hírszerzési vagy logisztikai célokra. Az orosz hadsereg azt tervezi, hogy a Nerehtát az MI kutatási és fejlesztési platformjaként használja, amely potenciálisan magában foglalja az autonóm célfelismerési képességet.[21]

Ezek a fejlemények aggodalmat ébresztettek a nemzetközi helyzetelemzőkben, akik azt is megjegyzik, hogy az orosz hadsereg sokféle autonóm járműkoncepciót kutat, beleértve a harckocsi méretű eszközöket is, míg az ellenérdekelt hadseregek eddig csak a támogató funkciókra fókuszáltak. Ugyanakkor a versenytársakhoz hasonlóan az orosz hadsereg azt tervezi, hogy beépíti a mesterséges intelligenciát pilóta nélküli légi járművekbe, haditengerészeti eszközökbe és személyzet nélküli tengeralattjárókba, a rajképességek integrálása érdekében.[22]

Ezenkívül egyes elemzők úgy vélik, hogy az orosz hadsereg valószínűleg a kémkedés és a propagandacélú mesterségesintelligencia-alkalmazásokat is kutatja. Ezen

[16] Tom Simonite: For Superpowers, Artificial Intelligence Fuels New Global Arms Race. *Wired,* 2017. szeptember 8.
[17] Lásd: https://fpi.gov.ru
[18] Samuel Bendett: Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems. *The Strategy Bridge,* 2017b. december 12.
[19] Leon Bershidsky: Take Elon Musk Seriously on the Russian AI Threat. *Bloomberg,* 2017. szeptember 5.
[20] Samuel Bendett: Should the US Army Fear Russia's Killer Robots? *The National Interest,* 2017a. november 8.
[21] Patrick Tucker: Russia Says It Will Field a Robot Tank that Outperforms Humans. *Defense One,* 2017. november 8.
[22] Sydney J. Freedberg Jr.: Armed Robots: US Lags Rhetoric, Russia. *Breaking Defense,* 2017. október 18.

elemzők feltételezése szerint Oroszország olyan eszközöket vizsgálhat, amelyek az eredeti forrásanyag kis mintamérete alapján nagy pontosságú videó- és hanghamisításra képesek.[23]

4. Mesterséges intelligencia vezette orosz információs és kibertérműveletek

Az orosz hadsereg számára a védelmi eszköztár fő fegyvere az információ. Az információs műveletek koncepciója különleges helyet foglal el az orosz (és előtte a szovjet) katonai gondolkodásmódban.

Geraszimov a közelmúltban többször hangsúlyozta az információ növekvő jelentőségét az állami ellenfelek semlegesítésének érdekében. „Az információs technológiák (…) az egyik legígéretesebb fegyvertípussá válnak, amelyet más országokkal szemben lehet használni."[24] Ebből következik, hogy az információs műveletek előkészítése és lebonyolítása kérdéseinek tanulmányozása a hadtudomány legfontosabb feladata napjainkban.

Geraszimov e kijelentéséből az is kitűnik, hogy az információs műveletek elsődlegesek, és az ehhez tartozó eszköztár fejlesztése nagyobb prioritást élvez az orosz hadseregben, már csak abból is kiindulva, hogy az ilyen jellegű műveleteket támogató technológiai fejlesztések középpontjában jelenleg a mesterséges intelligencia áll.

Az orosz hadsereg gondolkodását arról, hogyan lehetne a legjobban használni az MI-t ebben a tekintetben, Losev 2018-as *A katonai mesterséges intelligencia* című cikke részletezte az *Arsenal Otechestva* című folyóiratban. A cikk bemutatja, hogy az MI milyen előnyökkel járhat a fegyveres erők törekvéseiben. A lista élén nem írt az MI szerepéről az autonóm rendszerekben vagy más kifejezetten katonai technológiában. Inkább annak információstér-beli funkcióját vizsgálta, konkrétan a nagy stratégiai szintet megcélozva.[25]

Polyakova a *Weapons of the Weak* című cikkében a következőképp fogalmazott: „Az MI potenciálisan felerősítheti Oroszország dezinformációs műveleteinek hatását, valamint a hamis és félrevezető információk szándékos terjesztésének sebességét a politika és a társadalmak befolyásolása céljából."[26] Azonban az orosz gondolkodás az MI használatáról az információs környezetben sokkal tovább megy, mint pusztán a befolyásolás. Ha a mesterséges intelligenciának a „harmadik forradalmat kell képviselnie a katonai ügyekben",[27] akkor sokkal többet kell tennie, mint pusztán befolyásolni, következésképpen az MI-vel támogatott információs hadviselésnek is képesnek kell lennie a pusztításra. Ahogy Ilnitsky és Losev kifejezik, a mai konfliktusokban, „ahol a forró háború annyira valószínűtlen, ott az ellenség pusztításának fő

[23] Samuel Bendett: Red Robots Rising. *RealClear Defence,* 2017c. december 12.
[24] Gerasimov, 'Vektory Razvitiya Voyennoy Strategii' ['The Vectors of Military Strategic Development'], 11.
[25] Aleksandr Losev: Voennii Iskusstvenii Intellekt ['Military Artificial Intelligence']. *Arsenal Otechestva,* 6. (2018), 32. 12–21.
[26] Alina Polyakova: Weapons of the Weak: Russian and AI-Driven Asymmetric Warfare. *Brookings Institution,* 2018. november 15.
[27] Thornton–Miron (2020): i. m.

eszköze az [ellenségen belüli] nagy fokú instabilitás megteremtése, az információk manipulálása és kiberhatások révén".[28]

Az orosz katonai gondolkodásban a kiberhadviselés az információs hadviselés részhalmaza. E gondolat logikájának mentén megállapítható, hogy az MI által támogatott kibertérműveletekből fakadó stratégiai fenyegetés mélyreható.

Orosz szempontból a kibertéri műveleteknek pszichológiai és technológiai vonatkozásai egyaránt vannak.[29] A pszichológiai vonatkozás magában foglalja azon számítógépes (kiber-) eszközöket, amelyeket olyan információk terjesztésére használnak, amelyek célja a nagymértékű befolyás generálása, akár propaganda, akár álhírterjesztés (hoaxkampányok) formájában.

A mesterséges intelligenciával kapcsolatos fejlemények arra mutatnak, hogy alapvetően fokozzák az orosz kibertérműveletek ezen formájának hatásait. Az MI-t támogató eszközök képessé válhatnak igen valósághű, hamis információk létrehozására (például *deepfake* videók révén). Ahogy Losev leírja, az MI „nagy mennyiségű, mesterségesen előállított adattal töltheti be az információs teret, ez a »virtuális igazság« megzavarja a potenciális ellenfeleket".[30]

Egy ilyen művelet káros hatással lenne az ellenérdekelt állam döntéshozatalára, mivel nagyon kevés megbízható információ állna rendelkezésre. Alapvetően képes lenne aláásni a kormányokba és a demokratikus működésbe vetett hitet. Az információkba vetett hit nélkül a kormányok, a társadalmak és a katonai szervezetek nem tudnak hatékonyan működni. Az állami funkciók egyszerűen összeomolhatnak, mivel nem képesek felismerni az igazságot.[31] Ezzel elérkezne a kognitív háború kora a kibertérben.

A kibertérműveletek másik eleme a technológiai infrastrukturális háttér.[32] Ennek középpontjában egyaránt állnak a rosszindulatú programok, az alkalmi pusztítás és a felderítés a számítógépes rendszerek gyengeségeinek felkutatásában.

Losev rámutat, hogy a technológiai szférában az MI megjelenése most sokkal könnyebbé teszi a sebezhetőségek felkutatását az ellenfél informatikai rendszereiben. Az MI-vel, ahogy ő fogalmaz, a gyengeségekre való vadászat hatalmas méreteket fog ölteni.[33] Ez azt jelenti, hogy a kibertámadások sokkal összetettebbé és nagyon veszélyessé válnak a megcélzott állam számára. Továbbá valós lehetőségét látja annak, hogy néhány jövőbeli „harmadik világháború" néhány másodpercen belül ténylegesen véget érjen, ha az egyik állam átveszi az irányítást a riválisországok kritikus (információs) infrastruktúrái felett, az MI segítségével. Ugyanakkor, amint egy másik orosz forrás kifejezi, „minden katonai szervezet, amely ilyen módon használja az MI-t, világvége *(doomsday)* technológiát hozhat létre".[34]

[28] Thornton–Miron (2020): i. m.
[29] Timothy Thomas: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts. *Journal of Slavic Military Studies,* 27. (2014), 1. 101–130.
[30] Losev (2018): i. m. 2.
[31] Andrei Bezrukov: Vyklyuchit' Svet v Kremle: Chego Zhdat' ot Kibervoyn [Turn off the Lights in the Kremlin: What to Expect from Cyberwar]. *Gazeta,* 2018. október 13.
[32] Thorton–Miron (2020): i. m. 17.
[33] Losev (2018): i. m. 2.
[34] Tekhnologii "Sudnogo Dnya": Vooruzhennyye Sily Rossii Vnedryayut Iskusstvennyy Intellekt ['Doomsday Technologies': Russia's Armed Forces Introduce Artificial Intelligence]. *Yandex,* 2018. március 16.

5. Összegzés, következtetések

„Jelenleg a csatákat nem a csatatéren vívják, hanem először az információs térben" – fogalmazta meg Jurij Boriszov egykori miniszterhelyettes 2018-ban.[35]

Oroszországban a mesterséges intelligenciával támogatott információs és kibertérműveletek stratégiai szinten való használata a legmagasabb szintű politikai támogatást élvezi. Oroszország végső célját ismerve – az információs tér végső és kizárólagos kontroll alá vonása – az is megjegyezhető, hogy a mesterséges intelligencia fejlesztése lehetővé tenné az információs térben a hatékony ellentevékenységet, és elősegítené a végső győzelmet – legalábbis a fegyverkezési versenyben mindenképp.

Az Oroszországból érkező legnagyobb fenyegetés a Nyugatra nézve nem kinetikus, sokkal inkább technológiai és pszichológiai lesz.

Másrészről komoly intézkedéseket vezet be Oroszország az információstér-beli védelem növelésének, a sérülékenységi lehetőségek minimalizálásának, valamint a szuverenitás megőrzésének érdekében.

Az MI támogatta kiberfenyegetés már nem csupán elmélet. Akár rosszindulatú programokról, akár álhírekről van szó, a kiber- és információstér-beli fenyegetések és támadások lerombolhatják a nemzeti kritikus (információs) infrastruktúrákat és alááshatják a demokráciát.

Amíg a nyugati lineáris gondolkodásban az MI csak kiegészítője a meglévő katonai technológiáknak és műveleteknek, az orosz hadsereg gondolkodása az állandó stratégiai előnyre való törekvés kultúrája miatt nem korlátozódik ennyire: a hadviselés új módjait igyekszik kialakítani az új technológiák alkalmazásával. Ezt a gondolkodást érdemes elsajátítani, nem csak megfigyelni.

Felhasznált irodalom

Bendett, Samuel: Should the US Army Fear Russia's Killer Robots? *The National Interest,* 2017a. november 8. Online: http://nationalinterest.org/blog/the-buzz/should-the-us-army-fear-russias-killer-robots-23098

Bendett, Samuel: Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems. *The Strategy Bridge,* 2017b. december 12. Online: https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-therapid-development-of-russian-unmanned-military-systems

Bendett, Samuel: Red Robots Rising. *RealClear Defence,* 2017c. december 12. Online: www.realcleardefense.com/articles/2017/12/12/red_robots_risin_112770.html

Bershidsky, Leon: Take Elon Musk Seriously on the Russian AI Threat. *Bloomberg,* 2017. szeptember 5. www.bloomberg.com/view/articles/2017-09-05/take-elon-musk-seriously-on-the-russian-ai-threat

[35] Iskusstvennyi Intellekt: Puti i Resheniya [Artificial Intelligence: Problems and Solutions]. *Arsenal Otechestva,* 2018. március 27. 1.

Bezrukov, Andrei: Vyklyuchit' Svet v Kremle: Chego Zhdat' ot Kibervoyn [Turn off the Lights in the Kremlin: What to Expect from Cyberwar]. *Gazeta,* 2018. október 13. Online: www.gazeta.ru/comments/2018/10/12_a_12018991.shtml

Catania, Carlos A. – Carlos García Garino: Automatic Network Intrusion Detection: Current Techniques and Open Issues. *Computers & Electrical Engineering,* 38. (2012), 5. 1062–1072. Online: https://doi.org/10.1016/j.compeleceng.2012.05.013

Freedberg Jr., Sydney J.: Armed Robots: US Lags Rhetoric, Russia. *Breaking Defense,* 2017. október 18. Online: https://breakingdefense.com/2017/10/armed-robots-us-lags-rhetoric-russia/

Hoffmann, Jörg: Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In *Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS).* 25. (2015), 1. 364–372. Online: https://doi.org/10.1609/icaps.v25i1.13684

Kumar, Gulshan – Krishan Kumar – Monika Sachdeva: The Use of Artificial Intelligence Based Techniques for Intrusion Detection: A Review. *Artificial Intelligence Review,* 34. (2010), 4. 369–387. Online: https://doi.org/10.1007/s10462-010-9179-5

Losev, Aleksandr: Voennii Iskusstvenii Intellekt ['Military Artificial Intelligence']. *Arsenal Otechestva,* 6. (2018), 32. 12–21.

Mascaro Steven – Ann E. Nicholso – Kevin B. Korb: Anomaly Detection in Vessel Tracks Using Bayesian Networks. *International Journal of Approximate Reasoning,* 55. (2014), 1. 84–98. Online: https://doi.org/10.1016/j.ijar.2013.03.012

Polyakova, Alina: Weapons of the Weak: Russian and AI-Driven Asymmetric Warfare. *Brookings Institution,* 2018. november 15. Online: www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

Simonite, Tom: For Superpowers, Artificial Intelligence Fuels New Global Arms Race. *Wired,* 2017. szeptember 8. Online: www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/

Sommer, Robin – Vern Paxson: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In *2010 IEEE Symposium on Security and Privacy (SP).* IEEE, 2010. 305–316. Online: https://doi.org/10.1109/SP.2010.25

Svenmarck, Peter – Linus Luotsinen – Mattias Nilsson – Johan Schubert: Possibilities and Challenges for Artificial Intelligence in Military Applications. In *Proceedings of the 2018 NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. 2018.* 1–16.

Tekhnologii "Sudnogo Dnya": Vooruzhennyye Sily Rossii Vnedryayut Iskusstvennyy Intellekt' ['Doomsday Technologies': Russia's Armed Forces Introduce Artificial Intelligence'], *Yandex,* 2018. március 16. Online: https://bit.ly/3slQkU6

Thomas, Timothy: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts. *Journal of Slavic Military Studies,* 27. (2014), 1. 101–130. Online: https://doi.org/10.1080/13518046.2014.874845

Thornton, Rod – Marina Miron: Towards the 'Third Revolution in Military Affairs'. The Russian Military's Use of AI-Enabled Cyber Warfare. *The RUSI Journal,* 165. (2020), 3. 12–21. Online: https://doi.org/10.1080/03071847.2020.1765514

Tucker, Patrick: Russia Says It Will Field a Robot Tank that Outperforms Humans. *Defense One,* 2017. november 8. Online: www.defenseone.com/technology/2017/11/russia-robot-tank-outperforms-humans/142376/

Vooruzhennyye Sily RF Vnedryayut Tekhnologii Iskusstvennogo Intellekta. *Voenniye Materialy,* 2018. március 15. Online: https://warfiles.ru/176763-vooruzhennye-sily-rf-vnedryayut-tehnologii-iskusstvennogo-intellekta.html

Williams, David P.: Underwater Target Classification in Synthetic Aperture Sonar Imagery Using Deep Convolutional Neural Networks. In *Pattern Recognition (ICPR), 2016 23rd International Conference,* Cancún, 2016. 2498–2503. Online: https://doi.org/10.1109/ICPR.2016.7900011

HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 109–131.
DOI: 10.32567/hm.2022.3.8

Annamária Edegbeme-Beláz,[1] András Kerti[2]

A New Approach to Information Security Auditing in Public Administration

Due to the rapid pace of globalisation and digitalisation and the better usage of ICT technology, cybercrime is also rising. Hence, the secure operation of controlling and auditing information systems is fundamental in both the private and public sectors. It is generally accepted in the private sector that companies seek an independent third-party's assistance to carry out information security audits. However, how do information security audits work in public administration?

The article aims to characterise and assess information security auditing in public administration and define a new solution for conducting such audits. The article is considered a theoretical research paper. Theoretical research explains the basic terms related to auditing and defines conditions for efficient and effective information security auditing. Additionally, the research aims to answer whether the internal (bureaucratic, within the public administration organisational system) or external (third-party) audits prove more effective.

Keywords: **information systems security, auditing, public administration, audit principles, internal and external auditing**

1. Introduction

Public administration is an independent system with data and workflow, terminology, special procedures and rules. The primary mission of the public sector institutions is to realise public tasks within the internal and external domain; at the core of this mission stands nothing else but information. Therefore, information security management and auditing in public administration affect the efficiency, reliability

[1] PhD candidate, Óbuda University Doctoral School on Safety and Security Sciences, e-mail: belaz.annamaria@uni-obuda.hu
[2] Associate Professor, University of Public Service, e-mail: kerti.andras@uni-nke.hu

and quality of the realised public tasks. Information security audit is a complex process that requires good knowledge and understanding of the internal and external environment of public administration and its structure in systems and processes. Hence, information security management and auditing in public administration are often analysed in a way that separates it from the functioning of a public institution as an entirety.[3]

For the public administration system to remain operational in the long run, and the protection of data generated, stored, processed and transmitted in the systems to be ensured, the state has a significant task of organising, developing and maintaining an information security approach. To achieve this goal, information security tasks and programs must be orchestrated at both legal and strategic levels; moreover, risk analysis, evaluation processes and solutions, and predictive functions must form an integral part of them. Many countries and organisations acknowledge the need to develop efficient solutions that facilitate increased information security levels.[4]

The protection of the organisational system and infrastructure of the public administration is principally justified because public administration is responsible for the implementation of fundamental state tasks, so when we talk about administrative tasks and functions, we examine the underlying prevailing state interests behind these tasks.[5] The five primary domains of public administration (foreign affairs, law enforcement, military affairs, jurisdiction and financial administration) stem from the statehood of the state, scilicet, the exercise of public power. With the modernisation of the state and public administration, these five essential functions will not disappear but will be constantly extended and differentiated. It is indisputable that the protection of public administration and the infrastructure supporting it is a crucial area for all states.

For the subject of the present study, the question is inevitable: what do we mean by security? For most people, security is nothing more than a calm, threat-free state. At the same time, we must acknowledge that this definition is rather superficial, as there are many theories and different scientific approaches to the concept of security. After examining the definitions used to describe security, Máté Gábri [6] made the following statement:

[3] Ana-Maria Suduc et al.: Audit for Information Systems Security. *Informatica Economică,* 14, no. 1 (2010). 43–48; Kenneth J. Knapp et al.: Key Issues in Data Center Security: An Investigation of Government Audit Reports. *Government Information Quarterly,* 28, no. 4 (2011). 533–541; Dalibor Drljača – Branko Latinović: Audit in Public Administration's Information Systems – External or Internal? *IOP Conference Series: Materials Science and Engineering,* 200, no. 1 (2017). 1–7.

[4] Edyta Karolina Szczepaniuk et al.: Information Security Assessment in Public Administration. *Computers and Security,* 90 (2020). 1–11; Costel Mironeasa – Georgiana Gabriela Codină: A New Approach of Audit Functions and Principles. *Journal of Cleaner Production,* 43 (2013). 27–36.

[5] Annamária Beláz: A közigazgatás információbiztonsága: megjósolhatók az incidensek? *Hadtudomány,* 29, no. 3 (2019). 92–104.

[6] Máté Gábri: Biztonsági komplexumok az információs korban. *Hadmérnök,* 5, no. 4 (2010). 110–121.

"… in general, the concept of security is built around some kind of threat, which has a source and a subject. The definition of a threat can be objective or subjective. The former is characteristic of the traditional theory, while the latter is characteristic of novel thinking. In connection with a threat, security may mean the complete absence of a threat or the existence of assets that can be used to limit or reduce the threat."

Among security professionals, Ole Wæver is one of the novel thinkers. In his perspective, security is a state where threats exist, but we can take countermeasures.[7] We believe that this definition can be adequately applied in the present study, as information security threats from cyberspace are constantly present, i.e. they exist. However, the governments in the context of the performance of security tasks can defend against security incidents and develop existing capabilities. We will present a new solution for handling such threats by an innovative approach of information security auditing in the public administration sector.

The subject of the research is the public administration institutions in Hungary, in the context of the security of auditing information systems. The public administration constitutes a complex mega-system comprised of multiple subsystems. Functional and organisational complexity of public administration, regarding the security management of information systems, constitutes an interdisciplinary subject of research. The theoretical basis of the discussed issue originates in various academic fields, e.g. computer science, public administration science, management and quality sciences, security sciences and legal theory.

The main goal of the research is to propose a new public institution for information systems security auditing. Reaching the adopted goal required realisation of the following, theoretical in nature, detailed goals:

- defining information security auditing in the public sector
- demonstrating and identifying the challenges and risks of the two major audit types used currently
- explaining why there is a need for a new perspective and what possible advantages may the new approach bring

2. Overview of auditing

To understand the disparities between the bureaucratic internal and the suggested new independent information security auditing models in the public sector, we first need to understand the fundamental auditing concepts. In the following section, we will scrutinise: 1. the purpose of auditing; 2. the types of audits; 3. the function of audit; and 4. the audit process. Information security (IS) systems audit differs from auditing financial records, general operations, or business processes. Each of these disciplines share the common foundation of principles, standards, processes and

[7] Fen Osler Hampson: Review: Barry Buzan – Ole Wæver – Jaap de Wilde: Security: A New Framework for Analysis. *International Journal,* 53, no. 4 (1998). 798–799.

activities.[8] However, to distinguish from the more common financial connotation, it is important to highlight that in this research the focus is on IS auditing and not on the financial assessments.

2.1. Audit goals

In the literature, there are several definitions for auditing,[9] but all of them involve the following keywords: effective, efficient and economical use of resources; data integrity; compliance with national and international standards; collecting and evaluating evidence.

Based on these theories, auditing is a complex notion, and a management tool that evaluates an organisation's performance determines the implementation of the management principles and controls if the criteria for the activities are met. Through auditing, the status of the auditable institution and its enterprise capabilities can be measured. An audit always has a baseline, or standard of reference against which the auditee is compared. As a management tool, audit generates trust in: support and implementation of performance policy, the achievement of objectives and the creation of added value. Completing the audit process will provide relevant and representative conclusions on which directions for improvement can be established.[10]

Auditing purposes are not always alike, different areas can be audited for numerous purposes in an organisation.[11] Firstly, legally compulsory audits are conducted to inform external stakeholders about the company's operation, the supervision system and the functioning of certain restrictions and policies. The regulation of mandatory audits applicable to every organisation in the same domain, so in addition to reliability and supervision, audits impact the development of equal opportunities and fair competition.

---

[8] Stephen D. Gantz: Chapter 5. Types of Audits. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014c.

[9] Mironeasa–Codină (2013): op. cit.; Drljača–Latinović (2017): op. cit.; Andrea Kő – Balázs Molnár: *Az információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei.* Budapest, Corvinno Technology Transfer Kft., 2009; Giorgia Mattei et al.: Exploring Past, Present and Future Trends in Public Sector Auditing Research: A Literature Review. *Meditari Accountancy Research,* 29, no. 7 (2021). 94–134; Bjørn Stensaker: *External Quality Auditing: Strengths and Shortcomings in the Audit Process*. *External Quality Audit: Has It Improved Quality Assurance in Universities?* Woodhead Publishing Limited, 2013.

[10] Costel Mironeasa – Silvia Mironeasa: The Process Approach and the Generated Value at the Process Level. *Metalurgia International,* 14, no. 6 (2009). 89–93; Mironeasa–Codină (2013): op. cit.; Ling Lei Lisic et al.: You Can't Get There from Here: The Influence of an Audit Partner's Prior Non-Public Accounting Experience on Audit Outcomes. *Accounting, Organizations and Society,* 100 (2021); Qiu Gaosong – Yuan Leping: Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis. *Microprocessors and Microsystems,* (2021); Stephen D. Gantz: Chapter 1. IT Audit Fundamentals. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014a.

[11] Gantz (2014a): op. cit.

The condition is different in the second circle: voluntary audits. As its name suggests, the institutions are not obliged to conduct voluntary audits but carry out these evaluations to reach the highest possible self-control and development level. Moreover, these organisations collect more data on their operation by conducting audits, giving them broader control over their processes, and implementing management plans.

The third possible goal of auditing is to get certified. For a third-party audit, the audit baseline is usually defined in rules or legal or regulatory requirements related to the purpose or objective of the audit.[12] These assessments often result in a certificate stating that the organisation's management systems and processes conform with that baseline. The most popular quality management standard is ISO 9001, and the ISO/IEC 27001 is the leading international standard for information security management systems (ISMS).

There are unique objectives for information security audits,[13] which are the following:

- check the existence of security policy, standards, guidelines and procedures
- identify the inadequacies and examine the effectiveness of the prevailing policy, standards, guidelines and procedures
- identify and understand the actual vulnerabilities and risks
- review present security controls on operational, administrative and managerial issues, and ensure compliance to minimum security standards
- provide recommendations and corrective actions for enhancements

2.2. Types of audits

To understand the question of auditing, it is necessary to see the differences between the audit types. There are several classification methods of audits in the professional and academic literature, depending on the scholars' aspects and viewpoints.[14] In this article, we typified the audits by three features: 1. independence; 2. scope; and 3. application domain. The following table summarises our cataloguing.

[12] Gantz (2014a): op. cit.

[13] Suduc et al. (2010): op. cit.

[14] Drljača–Latinović (2017): op. cit.; Gantz (2014c): op. cit.; Gregory Michener et al.: Are Governments Complying with Transparency? Findings from 15 Years of Evaluation. *Government Information Quarterly,* 38, no. 2 (2021); Deniz A. Appelbaum et al.: Analytical Procedures in External Auditing: A Comprehensive Literature Survey and Framework for External Audit Analytics. *Journal of Accounting Literature,* 40 (2018). 83–101; Gary Giroux – Rowan Jones: Measuring Audit Quality of Local Governments in England and Wales. *Research in Accounting Regulation,* 23, no. 1 (2011). 60–66.

Table 1: Main types of audits

Category	Audit type	Description
Independence	Internal audit	The audit process is an integral part of the organisation. It means the continuous control of the systems' security status and reliability, the existence of security requirements; the implementation of the organisation's security policy; the compliance and application of internal regulations.
	External audit	Also known as third-party auditing, independently and impartially monitors the internal audit, the operation of the internal control and management system and the audited system's security status.
Scope	Organisational audit	The extent of this audit is the organisation as a whole, with all its functions, subsystems and processes.
	Specialised audit	This is a targeted audit; the examination's extent is limited to specific procedures, functions, or systems.
Application domain	Operational audit	Operating audit has the purpose of evaluating the structure of internal controls of a given process or work area. An example of this type of audit is the audit of application controls and logical security systems. This is a specific and targeted audit.
	Financial audit	The purpose of this audit is to evaluate the validity of financial reports. It relates to the integrity and reliability of financial information. This audit in public administration institutions is obligatory by law and usually performed by contracted auditing companies such as PricewaterhouseCoopers and Deloitte. It can also be done by an authorised independent and licensed auditor under the condition that there is no conflict of interest, and the auditor is not an employee of the institution auditing.
	Integral audit	The integral audit, in essence, is implemented to evaluate organisational goals related to the financial information, preserving of property, efficiency and harmonisation with the overall goals of the audited institution.
	Administrative	Aims to evaluate issues related to the efficiency of operative productivity within the organisation or institution. An administrative audit can be agreed even as part of more complex reviews and audits.
	Information security audit	IS auditing is an umbrella term, relates to the next sections: technical evaluation auditing management of IT control procedures auditing the processes of the IT department, software development and inspection of application systems compliance with international and national standards Its goal is to maintain the confidentiality, availability and integrity of the data stored and the system by collecting and evaluating evidences. This should assure achievement of business, organisational and control aims and that the unwanted events will be discovered, prevented and/or corrected.

Source: Compiled by the authors.

2.3. Audit functions

The ecosystem where an organisation activates affects its functions, system and processes; thus, one must consider the environment and the flow exchange between the system processes during the evaluation process.[15] As discussed earlier, the audit is a management tool, a process with its functions, which must be integrated into the organisation's management scheme.

Mironeasa and Codină (2013) argue that irrespective of the nature of the audit mission, application domain, or type, audit functions must be the same as follows:

- Function 1 – management tool – provides information for the decision-making process
- Function 2 – quality assurance vector – sets the performance level of the audited entity by assessing the effectiveness and efficiency
- Function 3 – intelligence provider – the participating persons develop additional well-defined competencies
- Function 4 – recognised authority – results are appreciated and put into practice
- Function 5 – mediator – the level of compliance is judged concerning the referential used
- Function 6 – means of influence – communicates management and stakeholders' expectations
- Function 7 – priority setting – establishes a hierarchy of the most important aspects (risks) that may affect functionality
- Function 8 – reliability provider – brings added value by relying on facts and real evidence
- Function 9 – impact creator – produces effects upon evidence

2.4. Audit process

Having in mind various aspects and points of interest for audit, the organisation's management must define the audit program (known as the Audit Charter), including the aim, type, scope and volume. Generally, the audit program falls into two phases: investigation and reporting. The auditor gathers the data, facts and evidence from the report's basis during the investigation phase. The report shall include the audit findings, whether the management complies with professional practice and regulations.[16]

Information security audits usually follow a risk-based approach, which results in a longer audit program consisting of the following phases:

1. *Planning* – determining and selecting effective and efficient methods for performing the audit and obtaining all necessary information. Since audits can last from just a few hours to several months, planning must include the audit schedule at least a year in advance.

[15] Alexandra Kanellou – Charalambos Spathis: Auditing in Enterprise System Environment: A Synthesis. *Journal of Enterprise Information Management,* 24, no. 6 (2011). 494–519; Michener et al. (2021): op. cit.

[16] Kő–Molnár (2009): op. cit.

2. *Data collection* – determining how much and what type of information to be captured and how to filter, store, access and review the audit data and logs.

To get the most out of the audit process, the auditor needs to gather intelligence. The volume and type of information and how to filter, store, access and review the audit data and logs are determined before the auditing in the planning phase. During the audit process, there can be several data sources. Figure 1 demonstrates the most common ways how auditors can collect data.

Figure 1: Data sources during an audit
Source: Compiled by the authors.

1. *Audit tests* – audit tests can be a compliance test (general review of existing security policies or standards and their compliance with the professional requirements) or substantive tests (detailed review of the existing security configurations and technical investigation).
2. *Reporting* – present the current security environment.

Report of findings should be promptly issued and present in the current security context. The audit report must be complete (contain all selected criteria), pertinent (stick to the audit scope) and accurate. It must contain appropriate conclusions and findings revealed during the audit, resulting in recommendations in line with the audit objectives, efficient, feasible and scheduled. The report is written in a language that is comprehensible to the management. The auditor's opinion expresses the interests concerned in applying the audit functions and is found in the audit results called audit findings. In this way, the opinion becomes a value that fits the organisation's culture.

Since vulnerabilities and threats evolve with time and the situation, security audits should be conducted periodically. This way, the fulfilment of security policy and the set of controls required to reduce risks to a satisfactory level can be ensured. Therefore, auditing should not be viewed as a one-way practice but a crucial part of the organisational life cycle.

3. Internal – bureaucratic – audits

As outlined in Table 1, we classify audits by different features; one is independence. Based on independence, we can talk about internal and external audits. With internal audits, the whole process is an integral part of the organisation. It means the continuous control of the systems' security status and reliability, the existence of security requirements; the implementation of the organisation's security policy; the compliance and application of internal regulations.

In practice as Figure 2 demonstrates, it implies that – depending on the size and structure of the organisation – at least one employee works as an auditor. He/she plans the audit, gathers the information, carries out the audit process and reports to the management. The auditor should be a competent person with sufficient skills and knowledge needed to implement the audit. The management should make all necessary efforts to make the internal auditing as independent as possible.

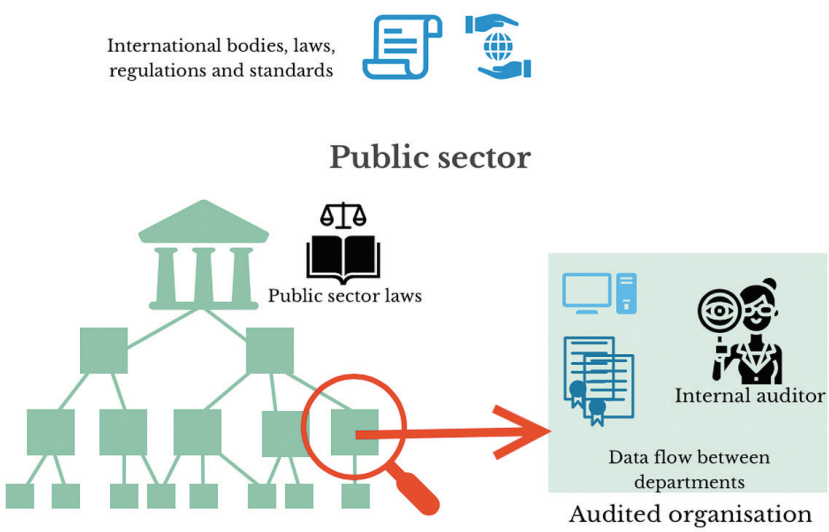


Figure 2: Internal auditing in the public sector
Source: Compiled by the authors.

Internal auditing is widely used in all sectors and every organisational level and it is especially popular in the public sector. Internal auditors are not just skilful professionals

but members of the organisation they are auditing; therefore, they can quickly evaluate the processes and procedures due to working experience and affiliation. The required information is easily reachable; there is no need for data transmission, which means the risk of data loss or leakage is extremely low. Moreover, as employees of the auditee, they strive to get the best outcome for their institution, are eager to pay attention to details, and focus on security aspects.

Despite the numerous advantages of internal auditing, there are many concerns regarding the efficiency and effectiveness of such audits. Unfortunately, to date, there is no settled term or usage in the scientific literature for the various descriptions of audit efficiency (so-called efficiency, value for money, comprehensive or performance auditing); therefore, when used in this article, we are referring to the broad area of efficiency meaning getting the most from the inputs and the expected results from the outputs.

What is the primary concern regarding the effectiveness of internal audits? Auditing has previously been the subject of extensive fieldwork and ethnographic analysis, regarding this Kanellou and Spathis (2011) notes: "Auditors' notions of 'effectiveness' were seen as key to the expression of auditing findings. Simply put, auditors said what they thought their audiences were ready to hear, both in terms of a willingness to act, in terms of political possibility, and in terms of an ability to act." Nevertheless, what happens when the auditors say what their audience is ready to hear? There must be a discrepancy between the audit findings and reality; consequently, auditing itself cannot fulfil its purpose. In his studies about a distortion of truth, Michael Taussig refers to such kind of discrepancy as 'public secret' that is generally known but cannot be articulated or spoken.[17] Later in his analysis amplifies this to things that are so 'publicly secret' that even the appearance of knowledge of the secret must be avoided: hence people "know they must not know".

Based on Taussig's public secret concept Vaughan S. Radcliffe presents that people may become wrapped up in the public secret to the extent that at times they deny its existence entirely, while others may recognise the importance of upholding the public secret in the functioning of society. He states that auditors recognise the role of public secrets in the auditing world, and hence to the ready adherence to the public secrets of modern society, government auditing may unintentionally tend towards an attendance to those in power. How so?

The auditing language is itself defining and facilitating; therefore, an internal auditor in the public sector may define political problems as business problems, thus transferring political debate of potentially threatening matters. The auditing's ability to redesign what might otherwise be political only requires proper management and language techniques; consequently, an auditor only includes 'strategically wise' findings in the audit report. This practice decreases auditing efficiency because it cannot fulfil its function as an intelligence and reliability provider. In order to understand the real problems, the management has to critique the audit report from within, comparing audit findings with the public secrets – the things that are known but cannot be said

[17] Beryl Bellman: Defacement: Public Secrecy and the Labor of the Negative. *American Anthropologist,* 103, no. 3 (2001). 878–879.

or cannot be seen to be known. As Radcliffe summarises,[18] the truth value of audit findings in areas marked by public secrecy is highly questionable.

Besides the truth content of the audit reports, another area of apprehension towards internal auditing in the public sector concerns the auditors themselves regarding how they understand their work, position and function. Senior auditors who have several years of experience upholding public secrets might think that knowing what not to say or what not to know is essential in writing a successful and efficient audit report. "If the only positive outcomes seen from audit work are those cases in which recommendations are enacted then there is the potential for an inherently conservative and unambitious taint to enter audit inquiry. Auditors must deal with this as they manage their presentation of self, both to others and […] as a matter of identity."[19] In many organisations, the relationships among the various functional groups involved in information security are less than ideal. Internal auditors often experience conflict and even adversarial relationships with other organisational functions.[20] Thus, it is not surprising that the relationship between the internal audit and information security functions is sometimes characterised by conflict and distrust.[21] Auditors must deal with this as they manage their presentation of self, both to others and in representing and making sense of their work internally as a matter of identity.[22]

The two characteristics mentioned above – truth content and auditor profession – can apply to all application domains of internal auditing. However, when designing information security audits, four more areas should be analysed. These are: 1. knowledge and reliability; 2. dependency; 3. outcome and customer satisfaction; 4. information safety and security. The following heading will discuss these areas and how internal auditing works compared to the suggested independent auditing model.

4. New approach: independent auditing

4.1. Concept

As outlined in the introduction within source literature, the issue of information security management and auditing in public administration is often analysed in a manner that separates it from the functioning of a public institution as an entirety. Public administration is an independent system with its data- and workflow, terminology,

[18] Vaughan S. Radcliffe: Public Secrecy in Auditing: What Government Auditors Cannot Know. *Critical Perspectives on Accounting,* 19, no. 1 (2008). 99–126.

[19] Radcliffe (2008): op. cit. 115.

[20] Zaini Ahmad – Dennis Taylor: Commitment to Independence by Internal Auditors: The Effects of Role Ambiguity and Role Conflict. *Managerial Auditing Journal,* 24, no. 9 (2009). 899–925; Mortimer A. Dittenhofer et al.: *Behavioral Dimensions of Internal Auditing. A Practical Guide to Professional Relationships in Internal Auditing.* Altamonte Springs, Florida, The Institute of Internal Auditors Research Foundation (IIARF), 2010.

[21] Paul John Steinbart et al.: The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems,* 13, no. 3 (2012). 228–243.

[22] António Samagaio – Teresa Felício: The Influence of the Auditor's Personality in Audit Quality. *Journal of Business Research,* 141 (2022). 794–807.

special procedures and rules; therefore, a systemic approach must be applied when interpreting security. When perceiving public administration as a system, it is reasonable to interpret security from systemic research. System security is understood as a property of an object, defined as the ability to protect an object's internal values (resources) against the occurrence of dangerous situations (threats).[23] If we accept this definition, the term security should be considered concerning possible threats and the risk of those. Information security secures legally protected information against unauthorised interference (disclosure, modification, erasing) in line with these statements.

During the examination we must keep in mind that the core mission of the public sector institutions is to realise public tasks within the internal (providing services for citizens) and external domain (cooperation of public administration units or with private sector institutions). According to Herbert A. Simon, public administration institutions carry out their tasks by finding the best decisions based on available information.[24] Decision-making in an institution is realised by processing input information into output information. In public administration, an institution is a set of cooperating elements that gather and process data (input data), emit and deliver feedback to achieve an adopted goal (output data). An example of the process described is the issuance of an administrative decision, e.g. license card, where the input data are the documents – such as certificate of driver's education course, certificate of the successful driving test, proof of residency and proof of age – delivered by the citizen, and the output data is the issued driving license.

We can boldly state that the functioning of public administration is based on gathering, processing, transmitting, storing and sharing information; therefore, information is one of the fundamental assets, and it is considered a protected value. Since information is a crucial element of public administration, a security incident can significantly lower the quality of administrative service. In extreme cases the disruption of these processes can lead to a complete breakdown of service delivery.

Both realisation and quality of provided services simultaneously must be taken into consideration as attributes of information security. Szczepaniuk et al. (2020) suggest defining information security in public administration as a state and a process in which:

- information security is achieved and sustained on a predetermined level of confidentiality, integrity and accessibility
- security of provided services is achieved and sustained on a predetermined level of reliability, accessibility and integrity of services
- authentication and accountability of entities, related to authentication of users utilising specific information and services are provided
- elements which constitute the public administration system are characterised with the ability to protect against current and future disruptions (threats) for

[23] Szczepaniuk et al. (2020): op. cit.

[24] Herbert A. Simon: Decision-Making and Administrative Organization. *Public Administration Review,* 4, no. 1 (1944). 16–30.

functioning or loss of specific values – the system is resistant toward threats (internal, external, accidental, purposeful)
- information and service users and recipients are aware of threats and are invulnerable to them
- perpetuators of security incidents have restricted possibilities to use cyber-space for the purpose of generating threats by utilising vulnerabilities and gaps within the security system

Since information itself and information security play a crucial part in the functioning of the public administration system, information security auditing has to play a vital role. Considering the above-mentioned internal auditing is not sufficient for public sector information security. However, a question is arising: Is third-party auditing considered the core mission of the public sector, or is there a demand for renewal?

We have to briefly revise how third-party auditing works and why it is used mainly in public administration to answer that question. From the dependency viewpoint, third-party auditing independently and impartially monitors the internal audit, the operation of the internal control and management system, and the audited system's security status. Regarding the scope, these audits can be organisational or specialised.

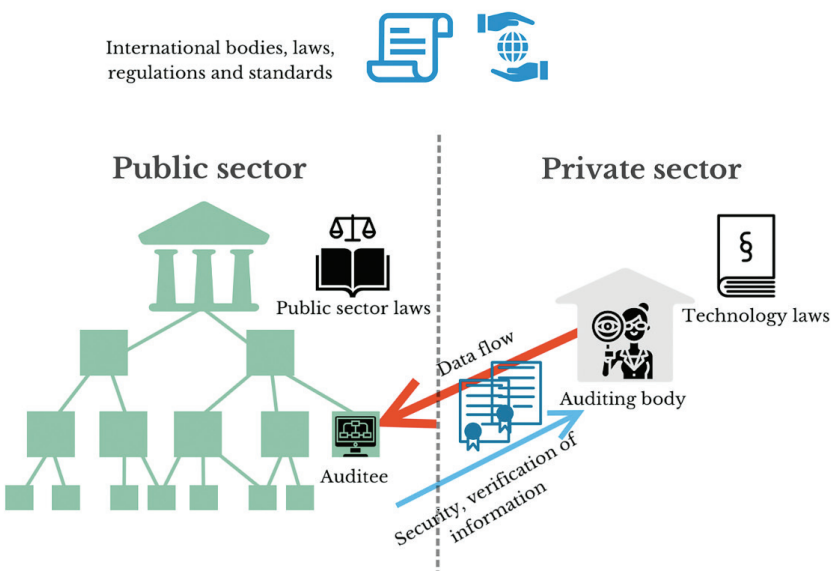


Figure 3: Third-party auditing of a public sector institution
Source: Compiled by the authors.

Third-party or external audits are performed by an auditing firm, entity outside the subject organisation. Depending by the size and the complexity of the IS audit,

the assessment is performed by a single auditor or a team.[25] As shown in Figure 3, whenever a public entity wants a third-party auditor to scrutinise its workflow and security state, they have to hire a private sector company. Though these companies must be accredited by the state to conduct audits (usually these corporations are registered or licensed with oversight bodies, such as the Committee of European Auditing Oversight Bodies [CEAOB]), undoubtedly, several risks arise when working with them.

Since public sector organisations are not obliged to work with the same auditor, each time a third party is introduced, the organisation is required to trust the new entity. Moreover, as discussed earlier, an audit ends with the issuance of the audit report, which contains appropriate conclusions and findings revealed during the audit, resulting in recommendations in line with the audit objectives. Since the recommendations are not obligatory, the organisation has no legal responsibility to modify its system or workflow. As the research by Stensaker (2013) shows "an external audit panel may be reluctant to reach and make explicit its conclusions and recommendations during the visit". This may imply that the opportunity of improvement for the client is lost, hence the impact of the audit process is extremely limited.

Regarding the internal auditing, Steinbart makes the following comment: "Certainly, self-monitoring is useful […]. Yet, there is considerable evidence that people have great difficulty in identifying and in correcting errors in systems that they created themselves."[26] In our opinion, this statement is true to third-party audits particularly in the public sector. The goal of these audits in the private sector is usually to prepare an organisation for accreditation or certification; however, holding such certifications is not shared in the public sector. Moreover, if we see public administration as a system, auditing should be considered an integral part of it. But how?

The solution is the adoption of a new approach by the establishment of the Autonomous Public Auditing Agency (APAA). Thanks to technological change, multi-causality, ad hoc approaches and short-termism, governments face many challenges these days. To address rapidly developing technologies, they need a more profound knowledge of these technologies and evolving policies simultaneously.[27] Instead of letting the control over their bodies, the governments should institute an auditing entity.[28]

[25] Stephen D. Gantz: Chapter 4. External Auditing. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014b.

[26] Paul John Steinbart et al.: The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Accounting, Organizations and Society,* 71 (2018). 15–29.

[27] Piret Tõnurist – Angela Hanson: Anticipatory Innovation Governance: Shaping the Future through Proactive Policy Making. *OECD Working Papers on Public Governance,* no. 44 (2020).

[28] Zoltán Nyikes – András Kerti: Proposals for Amending the Regulation of the Administrative System. *Journal of Emerging Research and Solutions in ICT,* 1, no. 1 (2016). 68–74.

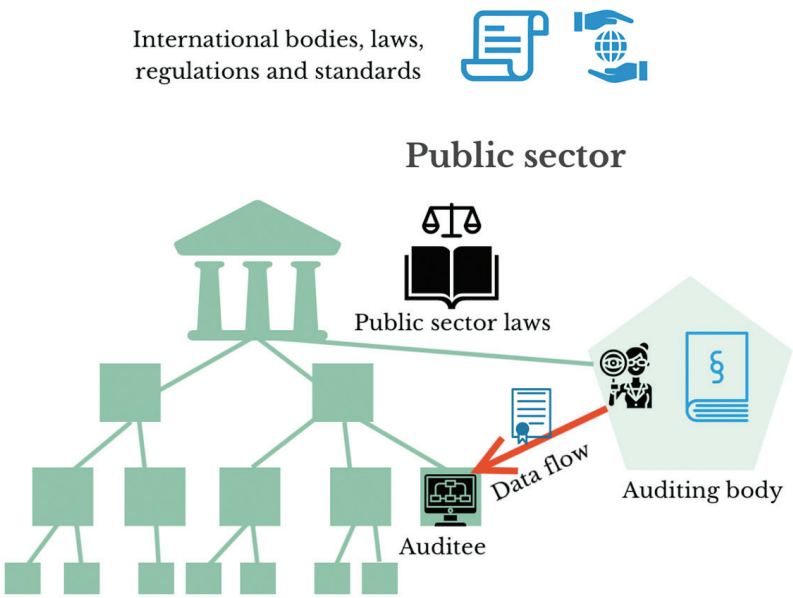


Figure 4: Autonomous Public Auditing Agency (APAA)
Source: Compiled by the authors.

As Figure 4 shows, the APAA is an auditing institution within the public administration system established by the government. Its goal is to overview and strengthen the information system security of the public sector by conducting regular audits. In the practice of analysis of information threats, various risk assessment methods are used, such as:

- OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation
- CRAMM – CCTA Risk Analysis and Management Method
- MEHARI – Method of Risk Analysis
- FMEA – Failure Mode and Effect Analysis
- ISRAM – Information Security Risk Analysis Method

Moreover, compliance with risk management methods within norms, standards and good practice would be required, such as: ISO/IEC 27001 norm and related norms (ISO/IEC 27001; ISO 27005), COBIT methodology, or NIST 800–37.

There are several specifications of the APAA compared to the third-party audits. The most significant are:

- the central government budget finances the APAA audit process; therefore, all public entities can participate in the audit programs irrespective of their financial status
- the personnel of the institution is made up of public servants with the necessary regulatory and technical expertise
- the audit report contains the analysis of non-compliance and errors accompanied by the set of controls required to reduce risks to a satisfactory level until the

next audit date. The failure to implement the necessary controls can conclude in receiving a fine. Since the feedback is not only in writing, but a detailed and executable action plan, there are no possibilities for misinterpreting it, finding in 'between the lines' information.[29]

The following section will analyse the advantages of setting up the Autonomous Public Auditing Agency for information security auditing and broader general audits for the public sector compared to internal and third-party auditing based on four characteristics. 1. knowledge and reliability; 2. dependency–independency; 3. outcomes; 4. data safety and security.

4.2. Advantages of the Autonomous Public Auditing Agency

The following table summarises the four areas of discussion:

- knowledge and reliability
- dependency–independency
- outcomes
- data safety and security

Table 3: Comparison between internal, third-party and APAA auditing methods

	Internal	**Third-party**	**Autonomous Public Auditing Agency (APAA)**
Knowledge and reliability	Skilful to evaluate the status of the technology, processes and procedures due to working experience and affiliation.	May only follow the instructions from frameworks and standards and not specifically experienced in the field.	Experienced both in the public administration system procedures and the best worldwide practices, standards and regulations.
Dependency	Public servant, member of the auditee organisation, complete objectivity is unapproachable.	Completely independent from the auditee organisation and the public sector as a whole.	Member of the public administration system, but fully independent from the evaluated organisation.
Outcomes and customer satisfaction	Pays less attention to the achievement of customer satisfaction; focuses more on security aspects.	Customer satisfaction is essential; focuses on overall functioning, especially in communication and information flow.	Main goal is the compliance with national and international regulations, achieving the 3 "E" management.
Safety and security	Narrowly defined "in-house" – no data transmission.	Potential point for "leaking of information"; may cause false interpretation of the collected data and mistrust.	Broadly defined "in house" – regulated methods of data storage and transmission within the public administration system.

Source: Compiled by the authors.

[29] Stensaker (2013): op. cit.

4.2.1. Knowledge and reliability

An auditor should be a technically competent person with sufficient skills and knowledge needed to implement an audit. "Auditing internal IT controls requires broad IT knowledge, skills, abilities and expertise in general and IT-specific audit principles, practices and processes."[30] Information security audits require more profound technical knowledge in a large and fast-changing field of ICT and the broad area of the information system component. "It is likely that when auditors possess technical knowledge, they can ask the kinds of important questions that cause information security professionals to see the potential value of further interaction."[31] Moreover, the auditor must understand the legal framework (legal aspects related solely to the audit of information systems and legal aspects of the audit topic, which is more specific) and the international standards and best practices on auditing. However, it is also necessary to know the legal framework for business operations in the company or the institution.

On the one hand, based on the working experience and familiarity with the organisation, the internal auditor is skilful in evaluating the IS technology, processes and bureaucratic procedures.[32] On the other hand, a third-party external auditor may demonstrate adequate IS knowledge and expertise supported by professional certifications. However, since public administration certificates and knowledge is not a prerequisite by law from external auditors to carry out assessments, it is possible that an auditor who has no work experience with public institutions may only follow the instructions from frameworks and standards and might lack the knowledge on legal aspects of the audit topic. Not having directly experienced counterparts' perspectives can leave auditors vulnerable to their pre-existing motivations.

Organisations need to either develop or acquire personnel with the specialised understanding of control objectives and experience in IT operations necessary to effectively conduct IS audits. The auditor of the APAA would be a professional equipped with the required technical knowledge and experience both in the procedures of public administration systems and the IS industry best practices, standards and regulations. When auditors possess detailed expertise about public administration and information security, they can develop deeper relationships with the information systems security function. Moreover, based on the experimental research conducted by Lisic et al. (2021) combined public sector and industry experience enhances the auditors' understanding of managers' motivations, and pressures, as well as their understanding of business processes and risk, thereby enabling them to more effectively evaluate and address risks leading to better audit judgments and higher audit quality.

[30] Gantz (2014a): op. cit.
[31] Steinbart et al. (2018): op. cit.
[32] Karim Hegazy – Anne Stafford: Internal and External Auditors Responsibilities and Relationships with Audit Committees in Two English Public Sector Settings. *Corporate Ownership and Control,* 18, no. 3 special issue (2021). 395–409.

4.2.2. Dependency

For auditing to reach its goal, as discussed earlier, the independence of the audit process is vital. If implemented as an internal audit, the management should make all necessary efforts to make this audit as independent as possible. However, a hint of subjectivity will always be present in these processes. At the core of information security audit is the evaluation of related risks. Even the most objective persons from the institution or organisation can be biased in evaluating the information systems and their functionalities.

Moreover, internal auditors are public servants and members of the auditee organisation; they are responsible to the top management of the public administration agency. The aims of the internal audit should be aligned with the mission and vision of the organisation, and the audit findings should support that vision. The notion of bureaucracy and the organisational hierarchy put auditors under the management. Their suggestions and recommendations therefore are subjected to the approval of the management, which is likely to ignore them in a situation where the findings of the internal auditors are adverse.[33] If we remember Radcliffe's discoveries on public secrets, the truth value of audit findings in areas marked by public secrecy is profoundly doubtful. Therefore, the accuracy of the internal audit findings will always be disputed. Significant amount of research was carried out to highlight the level of independence of internal auditors, and many came to the same conclusion as Dwamena and Ofori stating that internal auditors lack independence from management since they are mostly working under the direction and control of the management.[34]

In the context of external auditing such independence is often not just required, but legally enforced.[35] Nevertheless, since the third-party auditors are entirely independent of the auditee organisation and the public sector, they will lack the understanding of the bureaucratic public administration bodies' processes, terminology and organisational structure, which could unintentionally support public secrets.

An APAA professional is a member of the public administration system, equipped with the necessary knowledge but entirely independent from the evaluated organisation. The auditor would have no benefit from upholding a public secret but would understand the mechanism of public secrecy; therefore, the audit findings would be reliable and objective. Moreover, when an auditor "perceives its role to be more of an advisor instead of a policeman, mutual trust between the audit and information systems security functions is more likely to develop. In turn, as mutual trust between the two functions increases, so too does cooperation".[36]

[33] Richard Ofosu Dwamena – Nicholas Yaw Ofori: The Roles and Status of Internal Auditors in Public Sector Organizations. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 1–22.

[34] Richard Ofosu Dwamena: Investigating the Relationship Exist Between Internal Auditors and Management. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 23–35; Masruddin Jamaluddin et al.: Role Ambiguity, Role Conflict, Auditor Competence on Audit Quality: The Mediating Effects of Auditing Planning and Independence. *Universal Journal of Accounting and Finance,* 9, no. 6 (2021). 1551–1557.

[35] Gantz (2014b): op. cit.

[36] Steinbart et al. (2018): op. cit.

4.2.3. Outcomes and customer satisfaction

Client satisfaction is a related construct to audit quality.[37] Since the clients hire and pay the auditors to discover gaps and non-compliance in their processes, client satisfaction should be an important goal to most auditors. As the result of continuous digitalisation, many organisations process thousands of terabytes of internal and even more external data. Over time it is foreseeable that the audited institutions will expect deeper insights from the auditors (possibly through the usage of big data analytics) to maximise the benefits of their investments.[38] For this need, the APAA would be a suitable solution since it could act as a hub of IS information for the public sector. Given that the financial resources are provided by the state budget, the Agency would be able to invest in complex data mining and processing systems. With the advantage of data processing speed, these systems will help to improve the quality and efficiency of the audit, meet the requirements, and increase the trust level of clients.[39]

An audit can potentially add value in many ways because the feedback from audit can identify opportunities to improve the effectiveness of all types of information systems controls. The results target is the compliance of organisations with their own policies, moreover the coherence with national and international regulations, and it can identify the extent of corrective actions. Thus, the APAA auditor can achieve the "triple E" management (economy, efficiency and effectiveness).

The internal auditor will pay less attention to customer satisfaction and pay more to the security aspects of the information systems. In contrast, the external auditor can focus instantly on the overall functioning of the information systems independently, especially when dealing with communication and information flow. The primary goal of the external auditor is customer satisfaction and reliability of processes. As shown in the results of the empirical study conducted by Giroux and Jones (2021), it indicates that private sector auditors provide higher quality audits on lower fees than in-house auditors. Other research proved that although an auditor's expertise in public sector auditing increased satisfaction and quality, yet the Big 4 external auditors did not provide either higher client quality or increased satisfaction.[40]

Many studies found[41] that job pressure of internal auditors and auditors at third-party auditing firms (time management and volume of audits) can lead to dysfunctional behaviours and those may directly affect the audit report. This will culminate in shortened audits, (signing off audit report before completion), lack of research on standards, superficial reviews of the auditees' documents and accepting weak explanations. Similarly, stress reduces the likelihood of detecting material misstatements.

---

37 Giroux–Jones (2021): op. cit.

38 Appelbaum et al. (2018): op. cit.

39 Thi Tam Le et al.: Risk-Based Approach and Quality of Independent Audit Using Structure Equation Modeling – Evidence from Vietnam. *European Research on Management and Business Economics,* 28, no. 3 (2022).

40 Donald Samelson et al.: The Determinants of Perceived Audit Quality and Auditee Satisfaction in Local Government. *Journal of Public Budgeting, Accounting and Financial Management,* 18, no. 2 (2006). 139–166; Mattei et al. (2021): op. cit.

41 Le et al. (2022): op. cit.; Mattei et al. (2021): op. cit.; Gaosong–Leping (2021): op. cit.

4.2.4. Safety and security

As previously stated, the auditor needs to gather intelligence to get the most out of the audit process. The volume and type of information and how to filter, store, access and review the audit data and logs are determined before the auditing in the planning phase. During the data collection phase, the auditor examines the data sources such as documents, testing, interviews.

From a safety aspect, the internal auditor is the most desirable choice since all the knowledge and data stay "in the house" – there is no need for data transmission and storage outside the organisation. Despite signed confidentiality agreements, the external third-party auditor may be perceived as a potential point for data leakage and a security problem. This perception might lead to not providing quality access to data; therefore, the auditor might misinterpret it, culminating in mistrust from both sides.

During APAA auditing, the data must be transmitted to another agency from the auditee organisation for processing purposes. Since the data does not leave the public administration system, the predefined data storage, transmission methods and laws apply, the transmission could be viewed as broadly defined in-house data exchange. Moreover, the management can trust the auditor on its skills and independent views.

5. Conclusions and recommendations

Governments are generally known to be risk-averse and rule-driven, based on stable structures and predictable decision-making. Avoiding risks is often justified for political reasons. However, by design, governments do not tend to act when confronted with new challenges. From the position of 'wait and see', governments are pushed to act when hazards materialise.[42] This approach is sometimes easier than intervention: it frees authorities from having to justify risky or interventionist policies but is insufficient in response to information security since adverse outcomes have already arrived.

This article established that information security management and auditing in public administration affect the realised efficiency, reliability and quality of public tasks. Information security audit is a complex process that requires good knowledge and understanding of the internal and external environment of public administration and its structure in systems and processes. We presented a new solution for handling threats by an innovative approach of information security auditing in the public administration sector called Autonomous Public Auditing Agency. This approach could help governments provide more efficient, effective and economical answers to information security threats. We believe that establishing the APAA approach and making rationalisations in the information security auditing might solve the problems concealed through public secrecy. There is ultimately pressure that means that auditors want to believe that some positive outcomes can come from their work.

Limitations: The theoretical foundations of the APAA model are aimed at indicating the fundamental problem in auditing of information systems security, which

[42] Tõnurist–Hanson (2020): op. cit.

is the lack of a systemic approach that would include the institution's mission and its aspect of providing proper quality of delivered services. However, evaluating the audit process of information systems security utilising this new method would require further empirical research to adopt scientifically justified assessment criteria.

References

Ahmad, Zaini – Dennis Taylor: Commitment to Independence by Internal Auditors: The Effects of Role Ambiguity and Role Conflict. *Managerial Auditing Journal,* 24, no. 9 (2009). 899–925. Online: https://doi.org/10.1108/02686900910994827

Appelbaum, Deniz A. – Alex Kogan – Miklos A. Vasarhelyi: Analytical Procedures in External Auditing: A Comprehensive Literature Survey and Framework for External Audit Analytics. *Journal of Accounting Literature,* 40 (2018). 83–101. Online: https://doi.org/10.1016/j.acclit.2018.01.001

Beláz, Annamária: A közigazgatás információbiztonsága: megjósolhatók az incidensek? *Hadtudomány,* 29, no. 3 (2019). 92–104. Online: https://doi.org/10.17047/HADTUD.2019.29.3.92

Bellman, Beryl: Defacement: Public Secrecy and the Labor of the Negative. *American Anthropologist,* 103, no. 3 (2001). 878–879. Online: https://doi.org/10.1525/aa.2001.103.3.878

Dittenhofer, Mortimer A. – R. Luke Evans – Sridhar Ramamoorti – Douglas E. Ziegenfuss: *Behavioral Dimensions of Internal Auditing. A Practical Guide to Professional Relationships in Internal Auditing.* Altamonte Springs, Florida, The Institute of Internal Auditors Research Foundation (IIARF), 2010.

Drljača, Dalibor – Branko Latinović: Audit in Public Administration's Information Systems – External or Internal? *IOP Conference Series: Materials Science and Engineering,* 200, no. 1 (2017). 1–7. Online: https://doi.org/10.1088/1757-899X/200/1/012026

Dwamena, Richard Ofosu: Investigating the Relationship Exist Between Internal Auditors and Management. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 23–35. Online: https://doi.org/10.15557/FMEJA/2021/VOL3/ISS9/SEPT002

Dwamena, Richard Ofosu – Nicholas Yaw Ofori: The Roles and Status of Internal Auditors in Public Sector Organizations. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 1–22. Online: https://doi.org/10.15557/FMEJA/2021/VOL3/ISS9/SEPT001

Gábri, Máté: Biztonsági komplexumok az információs korban. *Hadmérnök,* 5, no. 4 (2010). 110–121.

Gantz, Stephen D.: Chapter 1. IT Audit Fundamentals. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014a. Online: https://doi.org/10.1016/B978-0-12-417159-6.00001-8

Gantz, Stephen D.: Chapter 4. External Auditing. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014b. 63–82. Online: https://doi.org/10.1016/B978-0-12-417159-6.00004-3

Gantz, Stephen D.: Chapter 5. Types of Audits. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014c. 83–104. Online https://doi.org/10.1016/B978-0-12-417159-6.00005-5

Gaosong, Qiu – Yuan Leping: Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis. *Microprocessors and Microsystems,* (2021). Online: https://doi.org/10.1016/j.micpro.2021.104046

Giroux, Gary – Rowan Jones: Measuring Audit Quality of Local Governments in England and Wales. *Research in Accounting Regulation,* 23, no. 1 (2011). 60–66. Online: https://doi.org/10.1016/j.racreg.2011.03.002

Hampson, Fen Osler: Review: Barry Buzan – Ole Waever – Jaap de Wilde: Security: A New Framework for Analysis. *International Journal,* 53, no. 4 (1998). 798–799. Online: https://doi.org/10.2307/40203739

Hegazy, Karim – Anne Stafford: Internal and External Auditors Responsibilities and Relationships with Audit Committees in Two English Public Sector Settings. *Corporate Ownership and Control,* 18, no. 3 special issue (2021). 395–409. Online: https://doi.org/10.22495/cocv18i3siart13

Jamaluddin, Masruddin – Indra Basir – Rahma Masdar – Lucyani Meldawati: Role Ambiguity, Role Conflict, Auditor Competence on Audit Quality: The Mediating Effects of Auditing Planning and Independence. *Universal Journal of Accounting and Finance,* 9, no. 6 (2021). 1551–1557. Online: https://doi.org/10.13189/ujaf.2021.090632 ; DOI: https://doi.org/10.13189/ujaf.2021.090632

Kanellou, Alexandra – Charalambos Spathis: Auditing in Enterprise System Environment: A Synthesis. *Journal of Enterprise Information Management,* 24, no. 6 (2011). 494–519. Online: https://doi.org/10.1108/17410391111166549

Knapp, Kenneth J. – Gary D. Denney – Mark E. Barner: Key Issues in Data Center Security: An Investigation of Government Audit Reports. *Government Information Quarterly,* 28, no. 4 (2011). 533–541. Online: https://doi.org/10.1016/j.giq.2010.10.008

Kő, Andrea – Balázs Molnár: *Az információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei.* Budapest, Corvinno Technology Transfer Kft., 2009. Online: https://doi.org/978-963-06-7254-2

Le, Thi Tam – Thi Mai Anh Nguyen – Van Quang Do – Thi Hai Chau Ngo: Risk-Based Approach and Quality of Independent Audit Using Structure Equation Modeling – Evidence from Vietnam. *European Research on Management and Business Economics,* 28, no. 3 (2022). Online: https://doi.org/10.1016/j.iedeen.2022.100196

Lisic, Ling Lei – Jeffrey Pittman – Timothy A. Seidel – Aleksandra B. Zimmerman: You Can't Get There from Here: The Influence of an Audit Partner's Prior Non-Public Accounting Experience on Audit Outcomes. *Accounting, Organizations and Society,* 100 (2021). Online: https://doi.org/10.1016/j.aos.2021.101331

Mattei, Giorgia – Giuseppe Grossi – James Guthrie A.M: Exploring Past, Present and Future Trends in Public Sector Auditing Research: A Literature Review. *Meditari Accountancy Research,* 29, no. 7 (2021). 94–134. Online: https://doi.org/10.1108/MEDAR-09-2020-1008

Michener, Gregory – Jonas Coelho – Davi Moreira: Are Governments Complying with Transparency? Findings from 15 Years of Evaluation. *Government Information Quarterly,* 38, no. 2 (2021). Online: https://doi.org/10.1016/j.giq.2021.101565

Mironeasa, Costel – Georgiana Gabriela Codină: A New Approach of Audit Functions and Principles. *Journal of Cleaner Production,* 43 (2013). 27–36. Online: https://doi.org/10.1016/j.jclepro.2012.12.018

Mironeasa, Costel – Silvia Mironeasa: The Process Approach and the Generated Value at the Process Level. *Metalurgia International,* 14, no. 6 (2009). 89–93.

Nyikes, Zoltán – András Kerti: Proposals for Amending the Regulation of the Administrative System. *Journal of Emerging Research and Solutions in ICT,* 1, no. 1 (2016). 68–74. Online: https://doi.org/10.20544/ERSICT.01.16.P07

Radcliffe, Vaughan S.: Public Secrecy in Auditing: What Government Auditors Cannot Know. *Critical Perspectives on Accounting,* 19, no. 1 (2008). 99–126. Online: https://doi.org/10.1016/j.cpa.2006.07.004

Samagaio, António – Teresa Felício: The Influence of the Auditor's Personality in Audit Quality. *Journal of Business Research,* 141 (2022). 794–807. Online: https://doi.org/10.1016/j.jbusres.2021.11.082

Samelson, Donald – Suzanne Lowensohn – Laurence E. Johnson: The Determinants of Perceived Audit Quality and Auditee Satisfaction in Local Government. *Journal of Public Budgeting, Accounting and Financial Management,* 18, no. 2 (2006). 139–166. Online: https://doi.org/10.1108/JPBAFM-18-02-2006-B001

Simon, Herbert A.: Decision-Making and Administrative Organization. *Public Administration Review,* 4, no. 1 (1944). 16–30. Online: https://doi.org/10.2307/972435

Steinbart, Paul John – Robyn L. Raschke – Graham Gal – William N. Dilla: The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Accounting, Organizations and Society,* 71 (2018). 15–29. Online: https://doi.org/10.1016/j.aos.2018.04.005

Steinbart, Paul John – Robyn L. Raschke – Graham Gal – William N. Dilla: The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems,* 13, no. 3 (2012). 228–243. Online: https://doi.org/10.1016/j.accinf.2012.06.007

Stensaker, Bjørn: *External Quality Auditing: Strengths and Shortcomings in the Audit Process*. *External Quality Audit: Has It Improved Quality Assurance in Universities?* Woodhead Publishing Limited, 2013. Online: https://doi.org/10.1016/B978-1-84334-676-0.50013-3

Suduc, Ana-Maria – Mihai Bîzoi – Florin Gheorghe Filip: Audit for Information Systems Security. *Informatica Economică,* 14, no. 1 (2010). 43–48.

Szczepaniuk, Edyta Karolina – Hubert Szczepaniuk – Tomasz Rokicki – Bogdan Klepacki: Information Security Assessment in Public Administration. *Computers and Security,* 90 (2020). 1–11. Online: https://doi.org/10.1016/j.cose.2019.101709

Tõnurist, Piret – Angela Hanson: Anticipatory Innovation Governance: Shaping the Future through Proactive Policy Making. *OECD Working Papers on Public Governance,* no. 44 (2020). Online: https://doi.org/10.1787/cce14d80-en

HADMÉRNÖK
VÉDELEMINFORMATIKA
17. évfolyam (2022) 3. szám 133–152.
DOI: 10.32567/hm.2022.3.9

Zsolt Haig,[1] Zsolt Illési,[2] János Péter Varga[3]

Possibilities of Electronic Jamming of WLAN Networks in the Physical Layer

Wireless local area networks or WLANs are the necessary underlying communication technology of consumer electronics, mobile computers and mobile phones of our days. Thanks to the comfortable operations and ubiquitous applicability for work and entertainment, the demand surged for these devices in the last 15 years. WLAN solutions provide the opportunity for mobility. But these networks communicate via radio waves with devices, which can be eavesdropped on and attacked. One form of attack is jamming. This article analyses the most frequent WLAN standards and the jamming options, particularly the execution of electronic jamming in the physical layer.

Keywords: **WLAN, wireless networks, jamming, SDR**

1. Introduction

These days civilian society is also greatly dependent on wireless communication. Therefore, the confidentiality, integrity and availability of radiofrequency communication are a growing concern due to the widespread security threats. Wireless networks, and thus WLAN, are susceptible to software attacks, which are widely used against computer networks and vulnerable to eavesdropping and especially radio jamming. Attackers can exploit the access to the radio frequency communication channel without physical connection, making jamming more beneficial.

In the context of this scientific problem, the aim of this paper is to systematise the attacks, namely electronic jamming that can be applied at the physical layer against WLANs. A further goal is to experimentally prove that jamming is an effective form of attack against WLAN. To achieve these goals, we first provide a literature overview and then perform a measurement of some WLAN jamming methods in a test environment.

[1] Professor, University of Public Service, e-mail: haig.zsolt@uni-nke.hu
[2] Associate Professor, Milton Friedman University, e-mail: illesi.zsolt@uni-milton.hu
[3] Associate Professor, Óbuda University, e-mail: varga.peter@kvk.uni-obuda.hu

2. WLAN technology

Wireless local area network (WLAN) solutions are based on the IEEE 802.11 standard. Laptops, tablets, smartphones and consumer electronics devices use this technology for communications. There are two frequency bands within the radio spectrum the WLAN devices can communicate in a local area network. These frequency bands were divided into channels to permit identification. Selecting a channel within a frequency band plays an important role. It is inevitable to plan the allocation of these channels to maximise the overall performance of wireless networks where multiple access points are used at close quarters, like in an office building or a housing estate. The local networking solution of the technology addresses the unauthorised use of the spectrum. This was solved in two frequency bands. The first is the Industrial, Scientific and Medical (ISM) band in the 2.4 GHz range. The second is the Unlicensed National Information Infrastructure (UNII) band in the 5 GHz range. Devices can be operated in these frequency bands without special licences under specific conditions. ISM and UNII bands can be used not only by WLAN devices. Thus, for example, particular devices might be jamming each other. The IEEE 802.11 standard family defines multiple transfer modes and protocols, of which the 802.11n (Wi-Fi 4), the 802.11ac (Wi-Fi 5) and the 802.11ax (Wi-Fi 6) are the most widely used ones. The following table shows the parameters of the standard family.[4]

Table 1: Key parameters of 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6)

PARAMETER	**IEEE 802.11N (Wi-Fi 4)**	**IEEE 802.11AC (Wi-Fi 5)**	**IEEE 802.11AX (Wi-Fi 6)**
Maximum data rate (Mbps)	600	6930	9607
RF Band (GHz)	2.4 or 5	5	2.4 or 5
Modulation type to maximum data rate	64-QAM	256-QAM	1024-QAM
Channel width (MHz)	20 or 40	20, 40, 80 or 160	20, 40, 80 or 160

Source: Wi-Fi Channels, Frequencies, Bands & Bandwidths. Electornics Notes, s. a.

Developers created a variety of methods in the Wi-Fi 4, 5, 6 standards, ensuring that wireless networking solutions can serve user demands and eliminate the opportunity that the wireless network could be the bottleneck in the system.

The experiments described in this paper are testing the potential options of the electronic jamming of n and x devices of the 802.11 standard families in the 2.4 GHz frequency band. After that, the paper summarises the related parameters of these WLAN ranges.

Both 802.11n ac and ax standards apply quadrature amplitude modulation (QAM) to maximise data transfer. The advantages of the modulation are the effective

[4] Rashmi Bhardwaj: Wi-Fi generation comparison Wifi6 vs Wifi5 vs Wifi4. *Network Interview,* s. a.

utilisation of the bandwidth. This method ensures the effectiveness of the data transmission of the radio communication. A significant disadvantage of this modulation method is the noise sensitivity. The transmission states are too close to each other. This issue is illustrated in Figure 1.

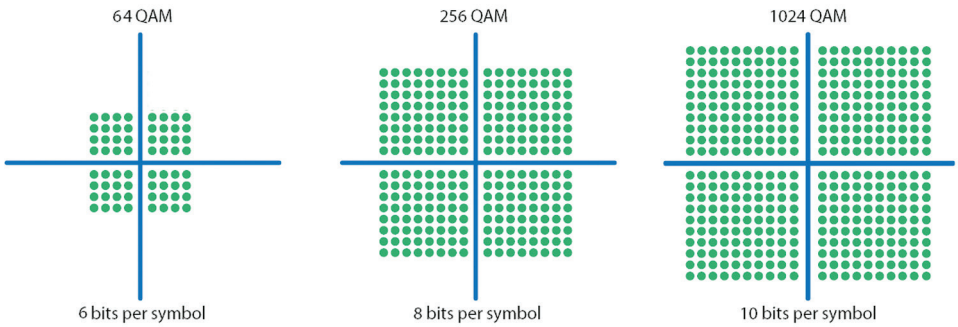


Figure 1: 64-QAM, 256-QAM and 1024-QAM states
Source: QAM modulator and demodulator. Faststream Technologies, 28 February 2022.

WLAN technology ensures that multiple users can use the available resources simultaneously. The Orthogonal Frequency-Division Multiplexing (OFMD) and Orthogonal Frequency-Division Multiple Access (OFMDA) permit it. The OFDM supports Time Division Multiple Access (TDMA) connections, while OFDMA or Frequency Division Multiple Access (FDMA) provide user support. The following figure illustrates the difference between OFDM and OFDMA.[5]

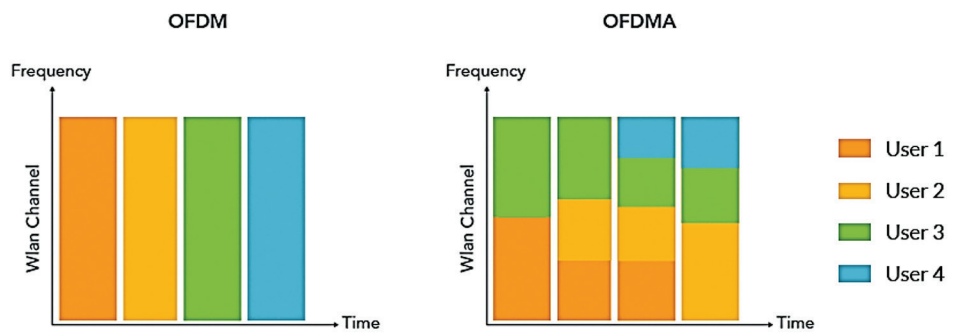


Figure 2: OFDM and OFDMA modulation
Source: Eve Danel: Wi-Fi 6's OFDMA Challenges Make Verification Crucial. RF Globalnet, 02 December 2019.

[5] Caleb McKee: *OFDMA vs OFDM explained.* 04 March 2021.

802.11n and 802.11ac standards support OFDM, while 802.11ax now supports OFDMA technology.

2.1. WLAN 2.4 GHz channels

WLAN devices in the 2.4 band provide 13 distinct channels in Europe, distributed by 5MHz from each other. Three non-overlapping channels are available when considering 20 MHz bandwidth channels. The following figure illustrates this.

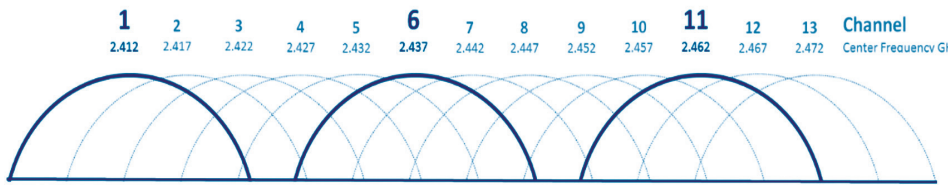


Figure 3: 64- Non-overlapping channels in the 2.4 GHz WLAN band
Source: Wi-Fi 4/5/6/6E (802.11 n/ac/ax). Duckware, 03 September 2022.

It is possible to find 20–30 WLAN Access Points (AP) in the overall 13 channels in some geographical areas due to the spread and the rapid development of the 2.4 GHz band-related technologies. These devices share those 13 channels, meaning that some of these operate overlapping and interfere with each other. There is a possibility of using 802.11n devices for channel bonding, making 40MHz bandwidth channels possible. Of these 40 MHz channels, only two are non-overlapping. Therefore, these bonded channels are prone to higher noise emitted by the other channels. Applying bonded channels requires a compromise between the throughput of the channel and signal quality.

2.2. Received Signal Strength Indicator and Signal/Noise Ratio

The Received Signal Strength Indicator (RSSI) is a value measured by the user device, which specifies signal quality. The measurable value is a relative number. The higher the number, the better the signal quality. The scale is from –100 to 0. The RSSI unit is dBm. The following table illustrates signal quality levels related to these values.[6]

[6] What is WiFi Strength and RSSI? *SimpliSafe,* s. a.

Table 2: RSSI value and Signal Strength

RSSI Value	Signal Strength
> -40 dBm	Perfect
-50 to -40 dBm	Excellent
-60 to -50 dBm	Very good
-70 to -60 dBm	Good
-80 to -70 dBm	Fair
-90 to -80 dBm	Poor
< -90 dBm	No connection

Source: Compiled by the authors based on What is WiFi Strength and RSSI? SimpliSafe, s. a.

The ability of the receiver device to separate the background signals of a given radio spectrum from its own plays a crucial role in wireless communication solutions. The Signal/Noise Ratio (SNR) indicator was introduced to measure this.

The SNR value indicates the relationship between the signal to noise. The SNR unit is dB. The unwanted or undesirable information for the receiver is the noise. The noise could stem from radio traffic of other units or malfunctioning devices. The SNR value shows whether the quality of the selected communication channel is adequate. The following table indicates the quality classifications for SNR values.[7]

Table 3: SNR value, Signal quality and WLAN signal indication

SNR Value	Signal quality	WLAN signal indication
> 40 dB	Excellent	
25 to 40 dB	Very good	
15 to 25 dB	Low	
10 to 15 dB	Very low	
5 to 10 dB	No signal	

Source: Compiled by the authors, based on Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. CISCO, s. a.

These classifications visualise the quality of the AP and the channel between the user. This feedback also shows the user which services can be used fault-free. Above 40 dB all services of the communication channels shall be used. Between 5 and 10 dB, the noise level is so high that it is impossible to differentiate it from the sender's signal. Electronic jamming is to be used if the aim is to deny communication.

[7] Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. *CISCO*, s. a.

3. Basics of electronic jamming

Electronic jamming is an electronic attack method that came out with radios in the military at the beginning of the 1900s. Electronic jamming is, in military terms, the subset of electronic warfare. Electronic warfare aims to gather intelligence and deny the operations of systems operating in the electromagnetic spectrum of the adversary and maintain the operational capabilities of its similar systems. Jamming in military operations is a widely used action. The aim is to curtail the operations of the receiver units of the electronic devices used by the adversary's intelligence, command and control systems and deny the reception of signals carrying information.[8]

Figure 4 illustrates the general geometry of the jamming of radio communication networks and the main factors to consider. An essential precondition of effective jamming is to identify the characteristics (e.g. frequency, power, modulation) of the network to be jammed. These pieces of information can be collected by Communication Intelligence (COMINT). Jamming always appears at the receiver. Therefore, it is necessary to analyse the signal-to-noise ratio at the receiver input (jamming-to-signal ratio [J/S]), which is also called jamming coefficient (K). The jamming coefficient means the ratio of jamming noise power (P_{jr}) and signal power (P_{tr}) measured at the receiving point. Jamming is effective if the jamming noise/signal power ratio at the receiver's input is higher than the minimum value of the jamming coefficient (K_{min}).

The jamming coefficient depends primarily on the modulation method. Therefore, the more complex modulation method is used, the higher the J/S ratio is needed for effective jamming.

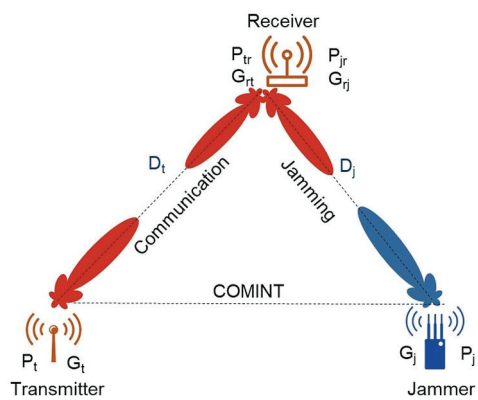


Figure 4: The general geometry of effective jamming of radio communication networks
Source: Compiled by the authors.

The effectiveness of electronic jamming of radio communication networks depends on the following factors:

- power of communication transmitter (P_t)
- gain of transmitter antenna towards receiver (G_t)

[8] Sándor Gyányi: Informatikai WLAN-hálózatok zavarása. *Bolyai Szemle,* 18, no. 4 (2009). 119–132.

- gain of receiver antenna towards transmitter (G_{rt}) and towards jamming source (G_{rj})
- jamming signal power (P_j)
- gain of jammer antenna towards receiver (G_j)
- distance between transmitter and receiver (absorption loss) (D_t)
- distance between jammer and receiver (absorption loss) (D_j)
- bandwidth of jamming signal (Δf_j) and receiver's effective adjacent channel rejection
- mode of the applied modulation (interference tolerance, signal processing) and modulation of jamming signal
- carrier frequency, bandwidth and other factors that have an impact on wave delegation[9]

It is practical to align the jamming signal to the applied modulation from an effective jamming perspective. Thus, the modulation should be regarded as reconciled. In addition, especially in WLAN networks, the receiver antenna gain is the same both towards the transceiver and the jamming unit in practice because these mainly use circular broadcast antennas. Considering these factors, by knowing K_{min} and the main technical and location parameters, after some simplifications, the power required for jamming can be calculated by using the following formula:[10]

$$P_j = K_{min} \frac{P_t G_t D_j^2 \Delta f_j}{G_j D_t^2 \Delta f_r} \quad [1]$$

where:
P_j – minimum jamming power
P_t – transmitter power
G_t – gain of transmitter
G_j – gain of jammer antenna
D_t – distance between transmitter and receiver
D_j – distance between jammer and receiver
Δf_j – jamming signal bandwidth
Δf_r – receiver's effective adjacent channel rejection
The jamming distance can be calculated by rearranging the formula above:[11]

$$D_j = D_t \sqrt{\frac{P_j G_j \Delta f_r}{K_{min} P_t G_t \Delta f_j}} \quad [2]$$

[9] Zsolt Haig et al.: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 80.
[10] Haig et al. (2014): op. cit. 81.
[11] Haig et al. (2014): op. cit. 81.

From this it is evident that the effectiveness of jamming primarily depends on the distance, the antenna gain, the power conditions, the jamming-to-signal ratio and the modulation-dependent jamming coefficient. Bandwidth is also an important parameter, especially in broadband jamming, which requires significant jamming power.

There are different jamming types against communication systems. Figure 5 illustrates these types.

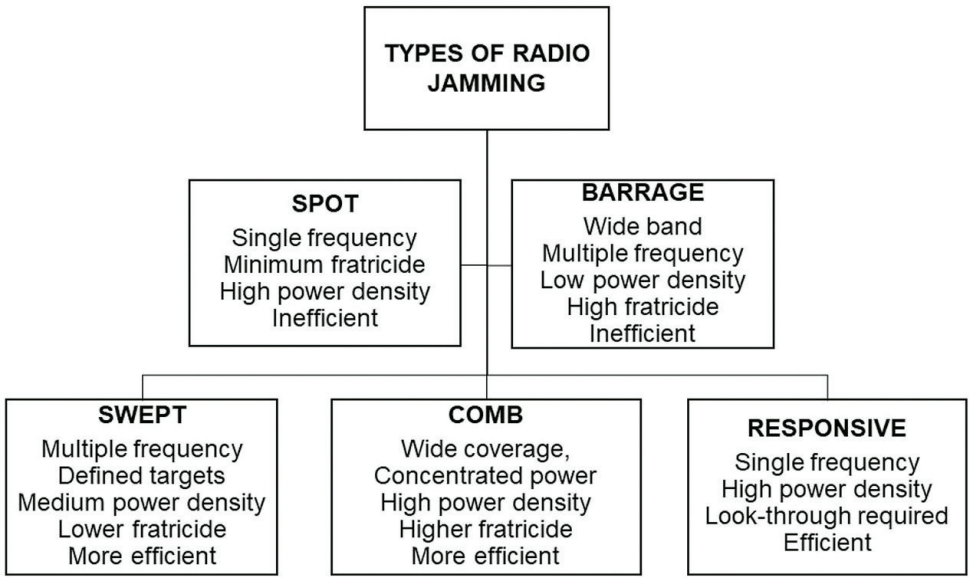


Figure 5: Types of radio jamming

Source: Michael R. Frater – Michael Ryan: Electronic Warfare for the Digitized Battlefield. London– Norwood, Artech House, 2001.

The two basic and longest-used jamming types are spot and barrage. The spot is single-channel jamming, using high power density per single channel. However, because of its low capacity, it has low effectiveness (it only jams a single channel). The barrage is the opposite of the spot. It can jam multiple channels simultaneously on broadband. However, its power density decreases proportionally to bandwidth. Swept and comb combine the advantages of these. The swept in broadband continuously sweeps across the jamming signal with high speed (for example, in the receiver's input bandwidth). As a result, it can be considered spot jamming at each discrete time. On the other hand, the fast frequency sweeping makes it possible to jam multiple channels. In the case of comb jamming, the jammer, which has a pre-programmed list of channels, simultaneously jams the targeted channels, for example, by utilising Frequency Divison Multiple Access (FDMA). The most effective and most challenging to implement jamming is responsive jamming. The receiver of the jammer of this type of jamming continuously scans the bandwidth. Where it finds a jammable channel, there it begins to transmit a jamming signal.

4. Possible ways of jamming WLANs in the physical layer

When jamming WLAN networks, the aim is to deny the communication between the access points (AP) and the connected Wi-Fi devices. Wi-Fi jamming can be implemented in the physical layer by applying the previously introduced radio jamming techniques individually or combined. Another option is to implement jamming in the MAC sublayer, called a protocol-stack attack or protocol-aware attack by the professional literature.[12]

APs or the devices connected to the AP can be targeted by jamming. When APs are targeted, the whole WLAN network becomes inoperable. The user devices cannot connect to the AP, and the network communication discontinues. This can be regarded as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on the physical layer. When individual WLAN devices are attacked, the receiver is targeted using different methods. This does not result in the overall discontinuation of the Wi-Fi network communication. In the following, the paper reviews the most typical attack methods in the physical layer, using the taxonomy of Pirayesh and Zeng primarily.[13]

The key to physical layer jamming is the relations between jamming signals and useful signal power ratios. The radiated power of the outdoor APs, depending on the applied frequency band, is 23–30dBm (200–1,000mW) on average. This power makes possible a 5–15 km range.[14]

Indoor APs usually use less power. These devices might have 10–20 dBm (10–100 mW) power.

Contrary to these APs, the commercial jammers have 1–10 W (30–40 dBm) total power, but also there is some 100 W (50 dBm) jammer on the market. These devices are usually multi-channel devices (e.g. Wi-Fi, 2G, 3G, 4G, 5G, GPS).[15]

Both the receiver (AP) and the jammer use circular broadcast antennas. Therefore, based on the power parameters, it is evident that it is possible to achieve more than 10–100 times J/S values.

This is true even if most of these jammers apply basic barrage jamming. As a result, it is possible to jam from greater distances (even from hundreds of meters). In the following, the paper summarises the most typical jamming methods.

High-power, continuous, broadband jamming: This type aims to deny access to the channel and packet reception. Measurements proved that 100% packet loss could be achieved in the case of an indoor AP using approximately 100 mW power and 4 dB (~2.5 times) J/S.[16]

Responsive jamming: When packets are detected, a jamming signal is transmitted. This is an effective jamming method because there is no continuous jamming signal

[12] Marc Lichtman et al.: A Communications Jamming Taxonomy. *IEEE Security and Privacy,* 14, no. 1 (2016). 47–54.
[13] Hossein Pirayesh – Huacheng Zeng: *Jamming Attacks and Anti-Jamming Strategies. Wireless Networks: A Comprehensive Survey.* 2021.
[14] CPE220 2,4 GHz-es 300 Mb/s 12 dBi Kültéri Egység. *TP-Link,* s. a.
[15] WiFi Jammer Bluetooth Signals Blocker. *Perfect Jammers,* s. a.
[16] Pirayesh–Zeng (2021): op. cit.; T. Karhima et al.: IEEE 802.11b/g WLAN Tolerance to Jamming. *IEEE MILCOM 2004. Military Communications Conference,* 3 (2004). 1364–1370.

transmission, only when communication is in the channel. The difficulty lies in the short response time. An OFDM symbol time is 4 µs, within which one needs to detect the package and transmit the jamming signal, for example. This makes a rigorous time correlation necessary.[17]

Spoofing (disguising a communication or identity): Sending many seemingly authentic data packets to the AP or a Wi-Fi device. With these data packets, spoofing exhausts the resources of the receiver. The target receives, processes spoofed data and has no remaining resources to process legitimate communication. It shows the effectiveness of spoofing that a low-yield jammer can exhaust all resources of an AP.[18]

Random and periodic jamming: The jammer transmits a jamming signal at random times and is dormant for the remaining time. During periodic jamming, the jamming signal is transmitted at pre-defined periods. It is easier to detect the latter because the jamming follows a predictable pattern. Random and periodic jammers have better energy efficiency because they do not transmit continuously. At the same time, data packet loss is less compared to continuous broadband jamming.[19]

Sweep jamming: In this case, the jammer seeps the overall band with high speed (within less than 10 µs), i.e. it keys up its transmitter from frequency to frequency. Measurements prove that it can reach more than 66% capacity loss in the 2.4 GHz band due to the excellent power density.[20] Its main limit is the need for a quick re-keying sweep jammer. One magnitude higher sweep in the 5 GHz band is necessary than in the 2.4 GHz band because the keyable bandwidth is 10 times larger.

5. Implementing electronic jamming in the physical layer

The authors tested three jamming types in a lab environment introduced previously. A USRP B200 SDR device was used as a jammer. The SDR can operate a full-duplex mode between 70 MHz and 6 GHz in 56 MHz bandwidth. Due to its open-source driver, it is possible to adapt it to many platforms. The GNU Radio application in the Windows environment was selected to control the device from the possible options. The tests were performed in the 2.4 GHz WLAN band.

The test was performed in an interference-free environment, with no other APs operating nearby. The jammer, the transmitter and the receiver were 10 m from each other. 2 dBi gain circular broadcast antennas were used in all test devices. In the GNU Radio application, the output power was set to 100 mW (20 dBm) during the measurement.

[17] Pirayesh–Zeng (2021): op. cit.; Yifeng Cai et al.: Joint Reactive Jammer Detection and Localization in an Enterprise WiFi Network. *Computer Networks,* 57, no. 18 (2013). 3799–3811.

[18] Pirayesh–Zeng (2021): op. cit.; Ioannis Broustis et al.: FIJI: Fighting Implicit Jamming in 802.11 WLANs. In Yan Chen – Tassos D. Dimitriou – Jianying Zhou (eds.): *Security and Privacy in Communication Networks. SecureComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.* Volume 19. Berlin–Heidelberg, Springer, 2009.

[19] Pirayesh–Zeng (2021): op. cit.

[20] Suresh Bandaru: Investigating the Effect of Jamming Attacks on Wireless LANs. *International Journal of Computer Applications,* 99, no. 14 (2014). 5–9.

To ascertain the adequate operation of the jammer, a spectrum analyser was used in the test environment to evaluate the radio spectrum before, during and after jamming. Figure 6 illustrates the test environment.

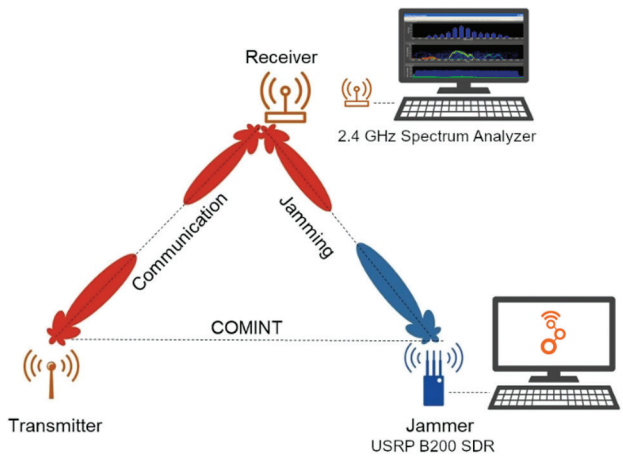


Figure 6: Network configuration for electronic jamming
Source: Compiled by the authors.

The 2.4 GHz WLAN frequencies and channels should be known to set up the jammer properly. This is summarised in the following table.

Table 4: 2.4 GHz WLAN Band channel numbers and frequencies

Channel Number	Lower Frequency MHz	Center Frequency MHz	Upper Frequency MHz
1	2401	2412	2423
2	2406	2417	2428
3	2411	2422	2433
4	2416	2427	2438
5	2421	2432	2443
6	2426	2437	2448
7	2431	2442	2453
8	2436	2447	2458
9	2441	2452	2463
10	2446	2457	2468
11	2451	2462	2473
12	2456	2467	2478
13	2461	2472	2483

Source: Compiled by the authors based on Wi-Fi Channels, Frequencies, Bands & Bandwidths. Electornics Notes, s. a.

Before the experiment, the radio status of the environment was tested by the spectrum analyser in the 2.4 GHz WLAN band. The spectrum snapshot indicates that two devices broadcasted in the test band. Based on the mid-frequencies, the first AP was on channel 2 (2417 MHz), and the second device was on channel 10 (2457 MHz). Figure 7 shows the spectrum state before the test.

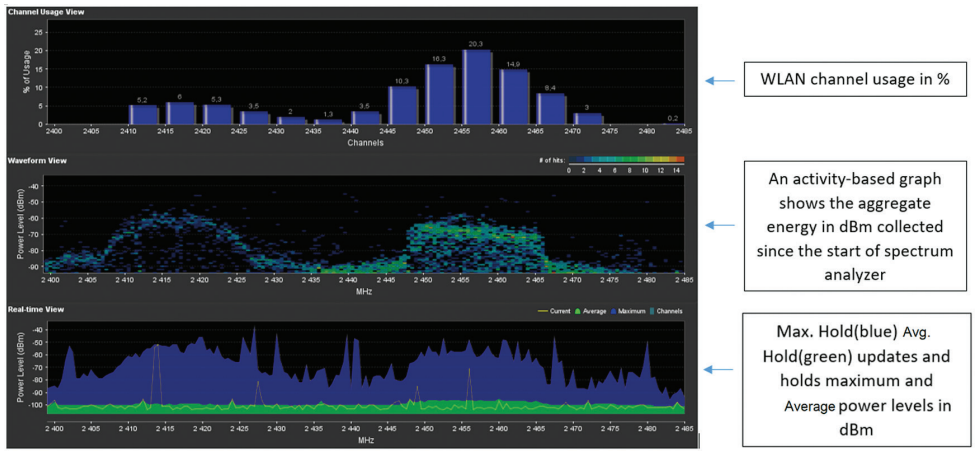


Figure 7: The 2.4 GHz WLAN spectrum before the tests
Source: Compiled by the authors.

The following figure summarises the J/S (Jamming-to-Signal) value per WLAN channel before the test.

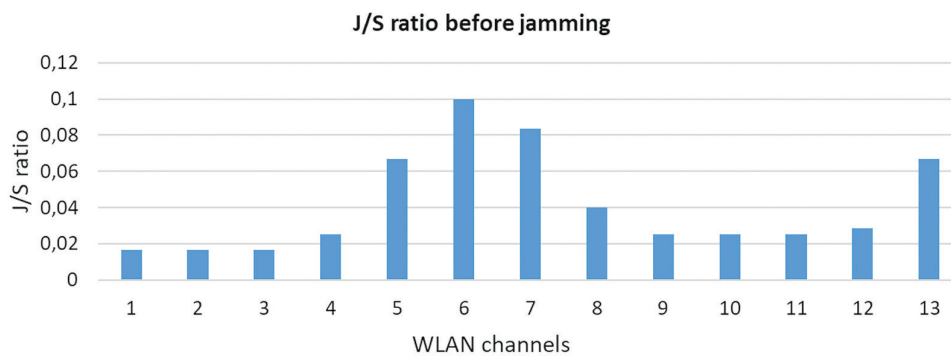


Figure 8: J/S value per the 13 WLAN channels before the test
Source: Compiled by the authors.

The low J/S values represent that the 2.4 GHz band is practically noise-free at the starting point. The connection between the devices is error-free.

5.1. Broadband barrage jamming

A Gauss noise signal was selected and configured in the GNU Radio application to implement the jammer. Channel 2 frequency was set as mid-frequency. Figure 9 shows the block structure built in the application.

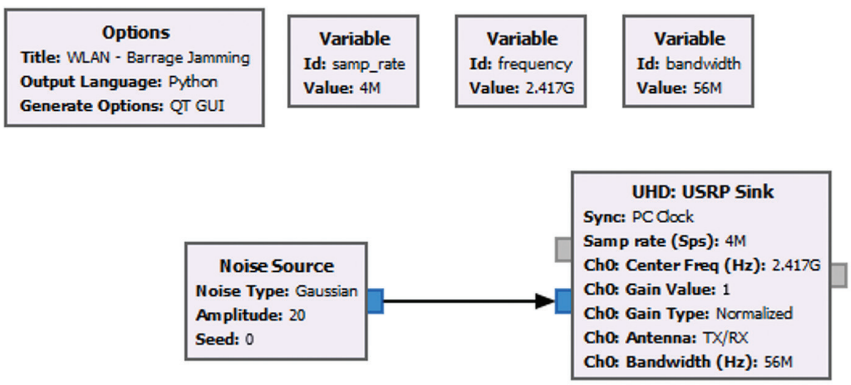


Figure 9: The block scheme of barrage jamming in the GNU Radio application
Source: Compiled by the authors.

Taking advantage of the available options of the SDR device, the 56 MHz bandwidth was selected. The emitted jamming power was 100 mW (20 dBm). The radio spectrum was analysed during the run of the jammer. Figure 10 shows this spectrum image.

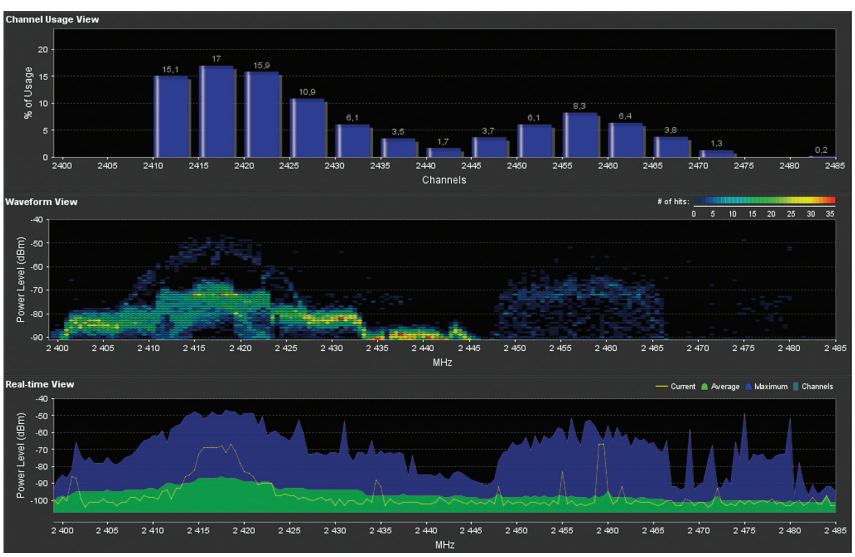


Figure 10: The effect of barrage jamming on the 2.4 GHz WLAN spectrum
Source: Compiled by the authors.

The spectrum image illustrates that the jamming signal of the barrage affects the overall WLAN spectrum. The top segment of the figure shows the channel load. This indicates that the main load was on channel 2. The middle segment of the figure shows the spectrum image varying from the more active to the less active values in red to blue. The drawn-out-shape of the jamming stands out in this image. The bottom segment of the figure indicates the minimum and maximum values of the signal. Here the signal and jamming are mixed. The spectrum image shows that jamming on the centre frequency was –65 dBm RSSI, and the average emitted frequency was –75 dBm. Due to jamming, the transmission signal of the device on channel 2 is not significant. The following figure shows the J/S value projected to the WLAN channels during barrage jamming.

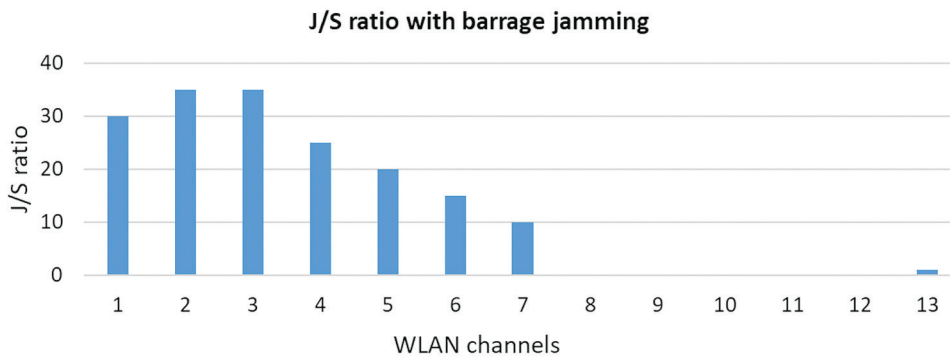


Figure 11: J/S value projected to the 13 WLAN channels during barrage jamming
Source: Compiled by the authors.

This jamming affects the first seven channels. The peak is on channels 2 and 3. The J/S value here was 45. The objective of this test was to jam the communication between devices using channel 2. As a result of this jamming, devices were unable to establish communication. The loss was 100%.

5.2. Spot jamming

The objective of this test was to deny the communication of devices using channel 2, but with spot jamming on the 22 MHz bandwidth. The bandwidth was selected because the bandwidth of an effective WLAN channel is closely 22 MHz. The jamming bandwidth is the same as the signal bandwidth in spot jamming. The jamming mid-frequency was set to 2417 MHz in this case. For the implementation, the previously implemented structure was used. This is illustrated in Figure 12.

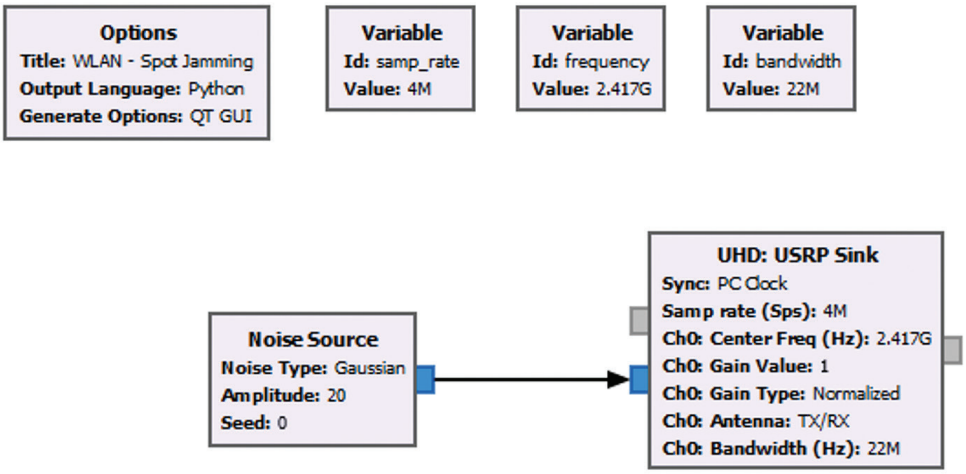


Figure 12: The block scheme of spot jamming in the GNU Radio application
Source: Compiled by the authors.

The radio spectrum was analysed during the operation of the jammer. Figure 13 shows this spectrum image.

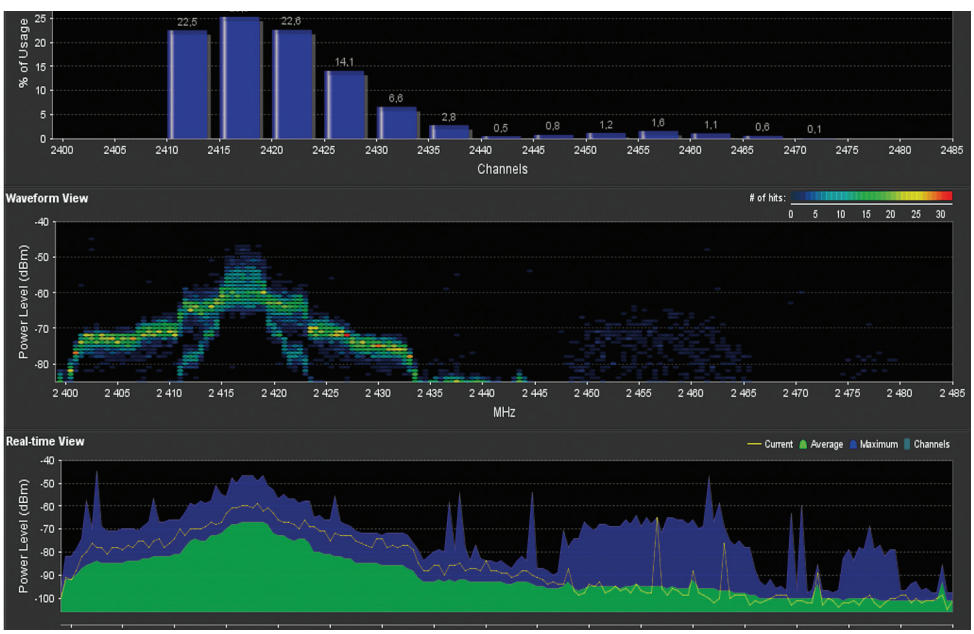


Figure 13: Spot jamming spectrum image on WLAN channel 2
Source: Compiled by the authors.

The image shows that the jamming primarily affects channel 2. On the mid-frequency of the channel, the jamming signal is –50 dBm RSSI. As a result of spot jamming, the transmission signal of the device on channel 2 is not significant. The following figure shows the J/S value projected to the WLAN channels during spot jamming.

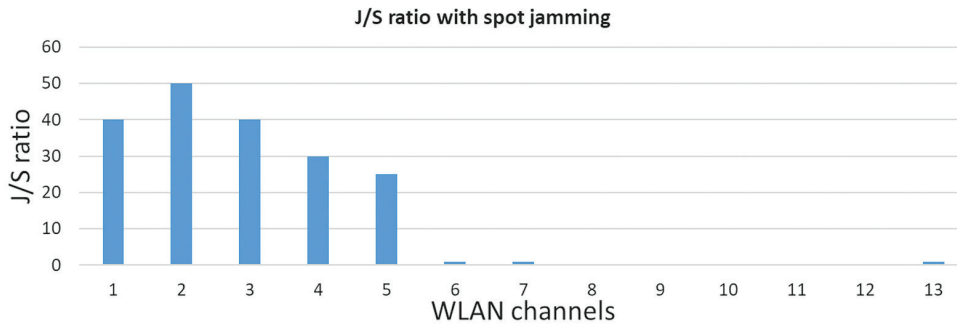


Figure 14: J/S value projected to the 13 WLAN channels during spot jamming
Source: Compiled by the authors.

This jamming affects the first five channels. The peak is in channel 2. The J/S value here was 55. The objective of this test was to jam the communication between devices using channel 2. As a result of this jamming, devices were unable to establish communication. The loss was 100%.

5.3. Sweep jamming

The start and end frequencies and the forward steps had to be determined during this test. From the frequency table, the centre frequencies were selected. The forward steps were set to 5 MHz. In the GNU Radio application, the sweep function was implemented by a custom-made Python code. This application defined the frequency values for the blocks in each step. Figure 15 shows the block level structure of this automated solution.

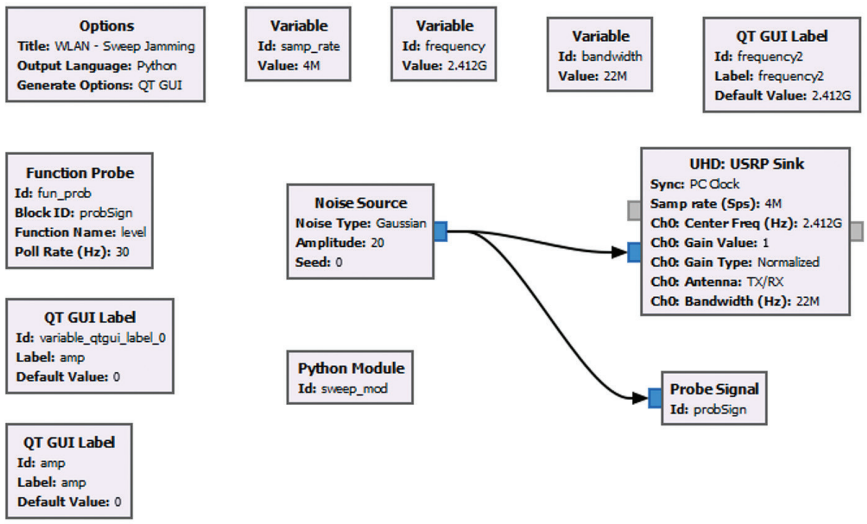


Figure 15: The block scheme of sweep jamming in the GNU Radio application
Source: Compiled by the authors.

The bandwidth was set to 22 MHz in this test. The radio spectrum was analysed again during the operation of the jammer. Figure 16 shows the result of this radio spectrum analysis.

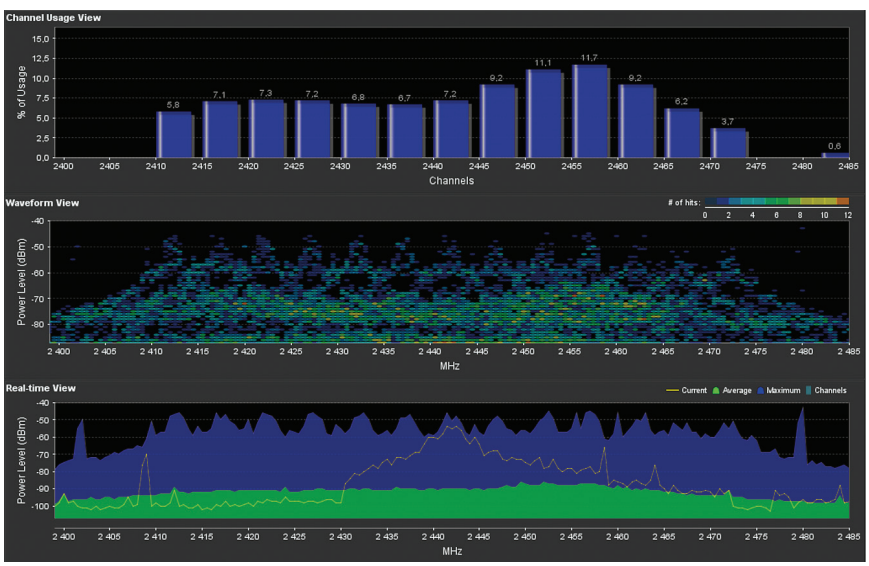


Figure 16: Sweep jamming spectrum image on the overall 2.5 WLAN band
Source: Compiled by the authors.

The following figure shows the J/S value projected to the WLAN channels during sweep jamming.

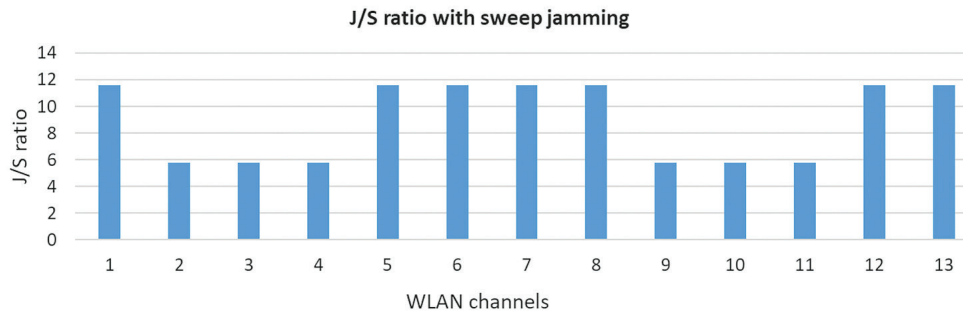


Figure 17: J/S value per the 13 WLAN channels during sweep jamming
Source: Compiled by the authors.

As a result of this test, the networking devices on this channel had a 45% of packet loss. This value was calculated from the up and download speed trends. The J/S ratio was in the range of 5.8 and 11.8 due to jamming. The spectrum image illustrates the jamming effects in the full WLAN band. Still, its intensity is below both spot and barrage jamming.

6. Conclusions

WLAN networks and devices are prone to electronic jamming day after day. In some instances, the applied technology permits jamming to be hidden from users or barely perceptible. Deliberate and targeted jamming, however, can render the communication channel unusable fully or partially for users. This paper summarised the possibilities of jamming WLANs in the physical layer. The paper also provides experimental evidence that the applicable jamming in the physical layer, which is described in theory, can be implemented by anybody with a widely available SDR.

A comparatively low (100 mW) jamming power was used in all cases. From the J/S effectiveness perspective, spot jamming was the best during the tests. It is also notable that jamming does not only affect the targeted channel (channel 2) but also was significant in four neighbouring channels (channels 1, 3, 4 and 5). Falling in all cases, the J/S ratio of spot jamming was above 20. Following the theory, the J/S value during the barrage jamming was lower than in the case of spot jamming. However, this jamming affected seven channels, and falling in all the cases, the J/S ratio of spot jamming was above 10. One of the exciting findings of the tests is that the J/S value is lower for spot jamming than the other two; in this case, the theory suggests that the spectral power density projected to 22 MHz is better than 56 MHz bandwidth barrage. However, these J/S values were sufficient to classify the jamming as effective.

The tests ascertained that the data loss in channel 2 was 100% due to both barrage and sweep jamming and 45% as a result of sweep jamming.

The experiments also highlighted that there is no need for high jamming power to implement some methods to deny communications effectively in WLANs if the jammers are close enough to the target devices. Of course, higher power is needed to jam from greater distances or implement jamming from an external source in all the tested methods. Based on theoretical calculations and causations, the smaller jamming distance reduces the required adequate jamming power by the square root, which means that in the case of half distance between the jammer and the target, only 1/4th of jamming power is sufficient. Of course, this works both ways. Twice the distance between the jammer and the target requires four times higher jamming power. This paper highlighted the vulnerability of contemporary WLAN networks in the physical layer, which could cause a severe cybersecurity issue and should be considered, especially in critical infrastructures.

References

Bandaru, Suresh: Investigating the Effect of Jamming Attacks on Wireless LANs. *International Journal of Computer Applications,* 99, no. 14 (2014). 5–9. Online: https://doi.org/10.5120/17439-8180

Bhardwaj, Rashmi: Wi-Fi generation comparison Wifi6 vs Wifi5 vs Wifi4. *Network Interview,* s. a. Online: https://networkinterview.com/wi-fi-generation-comparison-wifi6-vs-wifi5-vs-wifi4/

Broustis, Ioannis – Konstantinos Pelechrinis – Dimitris Syrivelis – Srikanth V. Krishnamurthy – Leandros Tassiulas: FIJI: Fighting Implicit Jamming in 802.11 WLANs. In Yan Chen – Tassos D. Dimitriou – Jianying Zhou (eds.): *Security and Privacy in Communication Networks. SecureComm 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Volume 19. Berlin–Heidelberg, Springer, 2009. Online: https://doi.org/10.1007/978-3-642-05284-2_2

Cai, Yifeng – Konstantinos Pelechrinis – Xin Wang – Prashant Krishnamurthy – Yijun Mo: Joint Reactive Jammer Detection and Localization in an Enterprise WiFi Network. *Computer Networks,* 57, no. 18 (2013). 3799–3811. Online: https://doi.org/10.1016/j.comnet.2013.09.004

CPE220 2,4 GHz-es 300 Mb/s 12 dBi Kültéri Egység. *TP-Link,* s. a. Online: www.tp-link.com/hu/business-networking/outdoor-radio/cpe220/

Danel, Eve: Wi-Fi 6's OFDMA Challenges Make Verification Crucial. *RF Globalnet,* 02 December 2019. Online: www.rfglobalnet.com/doc/wi-fi-s-ofdma-challenges-make-verification-crucial-0001

Frater, Michael R. – Michael Ryan: *Electronic Warfare for the Digitized Battlefield.* London– Norwood, Artech House, 2001.

Gyányi, Sándor: Informatikai WLAN-hálózatok zavarása. *Bolyai Szemle,* 18, no. 4 (2009). 119–132.

Haig, Zsolt – László Kovács – László Ványa: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Karhima, T. – A. Silvennoinen – M. Hall – S.-G. Haggman: IEEE 802.11b/g WLAN Tolerance to Jamming. *IEEE MILCOM 2004. Military Communications Conference,* 3 (2004). 1364–1370. Online: https://doi.org/10.1109/MILCOM.2004.1495141

Lichtman, Marc – Jeffrey D. Poston – Saidhiraj Amuru – Chowdhury Shahriar – T. Charles Clancy – R. M. Buehrer – Jeffrey H. Reed: A Communications Jamming Taxonomy. *IEEE Security and Privacy,* 14, no. 1 (2016). 47–54. Online: https://doi.org/10.1109/MSP.2016.13

McKee, Caleb: *OFDMA vs OFDM explained.* 04 March 2021. Online: www.minim.com/blog/what-is-wifi-6-ofdma-vs-ofdm-explained

Pirayesh, Hossein – Huacheng Zeng: *Jamming Attacks and Anti-Jamming Strategies. Wireless Networks: A Comprehensive Survey.* 2021. Online: https://doi.org/10.1109/COMST.2022.3159185

QAM modulator and demodulator. *Faststream Technologies,* 28 February 2022. Online: https://faststreamtechblogs.wordpress.com/2022/02/28/qam-modulator-and-de-modulator/

Signal-to-Noise Ratio (SNR) and Wireless Signal Strength. *CISCO,* s. a. Online: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength

What is WiFi Strength and RSSI? *SimpliSafe,* s. a. Online: https://support.simplisafe.com/hc/en-us/articles/360035742191-What-is-WiFi-Strength-and-RSSI-

Wi-Fi 4/5/6/6E (802.11 n/ac/ax). *Duckware,* 03 September 2022. Online: www.duckware.com/tech/wifi-in-the-us.html

Wi-Fi Channels, Frequencies, Bands & Bandwidths. *Electornics Notes,* s. a. Online: www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php

HADMÉRNÖK
FÓRUM
17. évfolyam (2022) 3. szám 153–168.
DOI: 10.32567/hm.2022.3.10

Mészáros István,[1] Bognár Balázs[2]

Üzletmenet-folytonossági tervezés kórházi környezetben II. – Kockázatértékelés és hatékonyságmérés

Business Continuity Planning in a Hospital Environment II – Risk Assessment and Efficiency Measurement

Hazánkban 2016-ban kezdődött meg az egészségügyi ágazatban, azon belül is a fekvőbeteg-ellátás alágazatban a létfontosságú rendszerelemek azonosítása és kijelölése. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény, illetve végrehajtási rendelete a kijelölt rendszerelemek üzemeltetői számára Üzemeltetői Biztonsági Terv készítését írják elő. Az üzemeltetői biztonsági tervezéshez bevált, nemzetközi gyakorlatban alkalmazott ISO 22301 szabvány áll rendelkezésre, amely az üzletmenet-folytonossági menedzsmentrendszerek tervezését írja le. Az egészségügyi ágazatra vonatkozó további előírásokat az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló ágazati rendelet határozza meg. A közigazgatásban és így az egészségügyben a profitorientált, így a „termelés" fenntartására fókuszáló szemléletmód gyakorlati alkalmazása nem megszokott, a profit és a termelés fogalma nehezen alkalmazható. A tanulmány az üzletmenet-folytonossági menedzsmentrendszerek alapjainak, a kockázatértékelés és az üzletmenet-folytonossági tervezés hatékonysága visszamérésének közegészségügyben való alkalmazási lehetőségeit vizsgálja.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: meszaros.istvan.mail@gmail.com
[2] Igazgató, Vas Megyei Katasztrófavédelmi Igazgatóság, e-mail: balazs.bognar@katved.gov.hu

Kulcsszavak: **létfontosságú rendszerelem, kritikusinfrastruktúra-védelem, egészségügy, fekvőbeteg-ellátás, üzemeltetői biztonság, üzletmenet-folytonosság, kockázatértékelés**

In Hungary, the identification and designation of critical infrastructures of the healthcare sector began in 2016, including the subsector of the inpatient care. The Act on the identification, designation and protection of critical systems and facilities and its implementing decree requires operators of designated system components to prepare an Operator Security Plan. The ISO 22301 standard, which is a proven in international practice for operator security planning, is available and describes how professionals can design Business Continuity Management Systems (BCMS). Additional requirements for the health sector are set out in a separated government decree on the identification, designation and protection of health-critical systems and facilities. In public administration and thus in healthcare sector, the practical application of a profit-oriented approach, and the focusing on the maintenance of "production", is not the common practice. The concepts of profit and production are difficult to apply. The study examines the fundamentals of BCM thus the Risk Analysis, and Key Performance Indicators (KPI), as the BCMS efficiency measurement in public health.

Keywords: **critical infrastructure protection, healthcare sector, inpatient care, operational safety, business continuity, Risk Analysis, KPI**

1. Problémafelvetés

Hazánkban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.), illetve végrehajtási rendelete, a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról (Vhr.) szabályozza a kritikus infrastruktúrák, azaz a létfontosságú rendszerelemek azonosításával, kijelölésével és védelmével kapcsolatos feladatokat. A jogszabály a már beazonosított és hatósági határozattal kijelölt létfontosságú rendszerelem üzemeltetője számára többek között Üzemeltetői Biztonsági Terv (ÜBT) készítését és annak folyamatos felülvizsgálatát írja elő. Az ÜBT alapvető tartalmi elemeit az Lrtv. 2. sz. mellékletében határozta meg a jogalkotó. Ezenkívül egyes ágazati jogszabályok további kötelező tartalmi elemeket írhatnak elő. A jelen tanulmányban tárgyalt egészségügyi ágazat fekvőbeteg-ellátás alágazatára vonatkozó további előírásokat az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet határozza meg.

Az ÜBT készítése, a versenyszférában a nemzetközi szakmai terminológia alapján a *business continuity planning* (BCP) tervezési gyakorlatra, azaz az üzletmenet-folytonossági átfogó megközelítésű szemléletre épül, amely alapvetően egy vállalatirányítási, folyamatalapú megközelítés, dinamizmust ad a tervnek és a terv „karbantartásának". Ezt a dinamizmust pedig az alapfolyamatok azonosítása és azok ciklikus igazgatása, azon belül is ciklikus tervezése adja.

Az ilyen típusú tervezési és irányítási feladatokra leginkább a szabványosított minőségirányítási rendszerek alkalmasak. Az üzletmenet-folytonossági tervezés és irányítási rendszer alapjait az MSZ EN ISO 22301:2020 Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek című szabvány írja le.

Jelen tanulmányban a szabvány közegészségügyi, azon belül is a fekvőbeteg-ellátó környezetbe való bevezetésének lehetőségeit kívánjuk megvizsgálni, megalapozni, az üzletmenet-folytonossági szemléletmód rendszerbe illesztésével. Ezen szemléletmód első lépései, a Stakeholderelemzés és az üzleti hatáselemzés alkalmazási lehetőségei után – amelyeket tanulmányunk első részében vizsgáltunk – jelen tanulmányunkban a kockázatelemzés, majd a tervrendszer hatékonyságának visszamérésére alkalmazható KPI-k rendszerbe foglalását elemezzük.

A tanulmány első részében levezetett módon a CITDöVKE (célkitűzés, információszerzés, tervezés, döntés, végrehajtás, koordinálás, ellenőrzés) – igazgatási ciklust is leíró – képlet alapján kezdtük el körvonalazni egy BCP-terv felépítését. Így a „Célkitűzés" során megállapítottuk, hogy a tervrendszeren belül melyik időszakra vonatkozóan melyik tervet készítjük, és egy javasolt Stakeholderelemzési módszertanon keresztül meghatároztuk, hogy a tervezés során az értékgazdákat milyen mélyen és milyen módon tudjuk bevonni a tervezésbe. Ezek után az „Információszerzés" szakaszában azonosítottuk egy fekvőbeteg-ellátó intézmény általános alapfolyamatait, mint az üzleti hatáselemzés (*business impact analysis,* BIA) első lépését, illetve levezettük a maximálisan tolerálható leállás mértéke, a helyreállítási pont és a szükséges helyreállítási idő meghatározásának szükségességét a kockázatértékelés megkezdéséhez.

2. Információszerzés: kockázatértékelés

Az üzleti hatáselemzés során azonosítottuk a betegellátást mint egy kórház/klinika védendő alapfolyamatát, ennek alapvető részfolyamatait és azok kiszolgáló folyamatait.

A következő lépés, hogy információt szerezzünk az e folyamatokat érő kockázatokról, tehát azonosítsuk és értékeljük a lehetséges kockázatokat. Az értékelés célja, hogy meghatározzuk, a tervezési folyamat során tervezzük-e a kockázatot csökkenteni, megszüntetni, vagy együtt élünk vele, így intézkedést sem igényel a folyamatos nyomon követésen kívül.

„Az alapfolyamatok kockázatai megközelíthetők az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételek (melyeket az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről szóló 60/2003. (X. 20.) ESzCsM rendelet rögzít részletesen) és a létesítmény üzemeltetési oldaláról is. Az ÜBT készítése során mindkét megközelítési módot szükséges alkalmazni a valós képességek felmérése érdekében, különös tekintettel arra, hogy a két megközelítés egyes elemei szoros összefüggésben állnak egymással.

Így a minimumfeltételek oldaláról mindenképpen szükséges felmérni és kockázati oldalról elemezni:

- az egészségügyi szakszemélyzet létszámát, rendelkezésre állását;

- a szükséges orvostechnikai eszközök számát, karbantartottságát, felhasználásra alkalmas voltát;
- a gyógyszer-, egészségügyi textília-ellátás és mosatás, illetve élelmezés helyi sajátosságait.

Létesítményüzemeltetési oldalról:

- Víz-, elektromos energia-, gáz-, orvosi gáz-, gőzellátás és csatornaszolgáltatás módját, lehetséges redundanciáit;
- A létesítmény és a benne található, üzemeltetésbe bevont eszközök karbantartottságát, a tervszerű megelőző karbantartás és a hibaelhárítás körülményeit;
- Lifteket, illetve egyéb személy- és anyagmozgató eszközöket;
- Fentiek meghibásodása esetére vonatkozó terveket;
- A hulladékkezelés módját különös figyelemmel a vegyi és fertőző veszélyes hulladékokra;
- A veszélyes anyagok kezelésének módját;
- A szervezet védelmi típusú szabályzatait (munka-, tűz-, vagyon-, környezet- és polgári védelmi, informatikai biztonsági), illetve a minőségirányítási rendszer dokumentumainak elérhetőségét, ismertségét, alkalmazhatóságát.
- Informatikai és egyéb kommunikációs eszközöket és hálózatokat, illetve azok biztonságát.

A külső veszélyeztető tényezők felmérésekor különösen az alábbiak felmérése szükséges.

- A kijelölt létfontosságú rendszerelem működési környezetének bemutatása;
  - földrajzi környezet;
  - a kerület lakossága, hivatalok, közintézmények, szolgáltatások;
- a kijelölt létfontosságú rendszerelem működési környezetének természeti eredetű veszélyeztetettsége;
  - vízjárással összefüggő veszélyeztetettség (talajvíz, belvíz, árvíz);
  - geológiai eredetű veszélyeztetettség;
  - meteorológiai eredetű veszélyeztetettség (jellemző szélirányok is);
- a kijelölt létfontosságú rendszerelem működési környezetének civilizációs, ipari és kommunális eredetű veszélyeztetettsége;
  - közlekedésből, szállításból fakadó veszélyeztetettség;
  - a lakosság alapvető ellátását és a létfontosságú rendszerelem működését biztosító szolgáltatások, infrastruktúrák bemutatása, sérülékenysége;
  - a kerület közmű és energia ellátásának helyzete;
  - infokommunikációs szolgáltatások, hálózati ellátás;
- egyéb eredetű veszélyek;
  - a kijelölt rendszerelem környezetében található, a működésére befolyással bíró veszélyes üzemek, gyárak, erőművek;
  - a kerület katasztrófavédelmi osztályba sorolása."[3]

[3] Kátai-Urbán Lajos – Mészáros István – Vass Gyula: Iparbiztonság, válsághelyzeti tervezés. In Major László: *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai.* Budapest, Semmelweis Kiadó, 2019. 68–69.

Az Országos Katasztrófavédelmi Főigazgatóság (OKF) által 2020-ban a létfontosságú rendszerelemek üzemeltetői részére megküldött általános formadokumentum az alábbi főcsoportokra bontja a felmérendő kockázatokat:

- meteorológiai kockázatok;
- geológiai kockázatok;
- humán kockázatok;
- technikai kockázatok;
- kommunikációs kockázatok;
- tűzeset;
- informatikai kockázatok;
- veszélyes anyagokkal és technológiákkal kapcsolatos kockázatok;
- egyéb, az adott ágazat szempontjából specifikus kockázatok.

Tekintettel arra, hogy ez egy általános formanyomtatvány, ahogy az utolsó sora is említi, szükséges az adott üzemeltető részéről az ágazatspecifikus kockázatok felmérése és értékelése is. Itt van lehetőség a minimumfeltételek és ezek kiszolgáló folyamatainak oldaláról is vizsgálni a kockázatot, így egy fekvőbeteg-ellátó létfontosságú rendszerelem esetében ezek az alábbiak lehetnek:

- hiba az orvostechnikai eszközökben;
- liftek és egyéb betegmozgató eszközök üzembiztossága;
  - liftek (különös tekintettel a számukra és a biztonsági felvonók számára);
  - kézi betegmozgató eszközök (különös tekintettel, azok számára, elérhetőségére és használhatóságára);
- betegélelmezés;
  - normál üzemmenet szerinti;
  - egészségügyi válsághelyzeti;
- egészségügyitextília-ellátás és -mosatás;
- orvosi gázrendszerek;
  - oxigén;
  - vákuum;
  - sűrített levegő;
- légtechnikai rendszerek (különös tekintettel a légszűrők cseréjére, a szükséges légcsereszámra, a csíramentes működésre és ezek mérésére);
- gyógyszerellátás;
- vér, vérkészítmény, laborminta-ellátás, -szállítás;
- egyéb egészségügyi anyagbiztosítás (egyéni védőeszközök, kémcsövek, pelenkák, tápszerek, kötszerek stb.);
- takarítás;
- egészségügyi (fertőző), vegyi veszélyes és kommunális hulladékok (különös tekintettel ezek belső kezelésére, az ezekből adódó munkabalestekre, veszélyeztető tényezőkre).

Az OKF által kiadott formadokumentum a kockázatok értékelésére az alábbi képletet alkalmazza:

A kockázat értéke (KÉ) = kockázat valószínűsége (KV) × (kockázat hatása [KH] + kitettség [KI]).

$$KÉ = KV \times (KH + KI)$$

A fenti képlet összetevőit az 1. sz. táblázat mutatja be, ahol a kockázat valószínűsége a bekövetkezési valószínűségnek, a kockázat hatása pedig a veszélyeztető hatások szintjének felel meg.

1. táblázat: Kockázatértékelés összetevőinek lehetséges értékei

A bekövetkezési valószínűség	Nagyon ritka	1
	Ritka	2
	Alkalmankénti	3
	Gyakori	4
	Nagyon gyakori	5
Veszélyeztető hatások szintje	Elhanyagolható	1
	Alacsony	2
	Közepes	3
	Magas	4
	Katasztrofális	5
Kitettség értékei	Nincs kitettség	0
	Egy fél felé van kitettség	1
	Több fél felé van kitettség	2

Forrás: BM OKF KIV kockázatelemzési formadokumentum. BM OKF, 2021.

A képlet alapján megkapott kockázati érték alapján képes eldönteni az üzemeltető, hogy az adott kockázattal intézkedés nélkül együtt él, vagy intézkedik a szükséges sürgősséggel. A 2. táblázat foglalja össze a képletben szereplő értékek szorzataként megjelenő kockázati értéket, a színkódnak megfelelő intézkedési küszöbértékeket pedig a 3. sz. táblázat mutatja. Ez alapján határozható meg, hogy az adott kockázati értékre milyen reakciót, intézkedést szükséges tennie az üzemeltetőnek.

2. táblázat: A kockázat lehetséges értékei

	Elhanyagolható	**Alacsony**	**Közepes**	**Magas**	**Katasztrofális**
Nagyon ritka	1	2	3	4	5
Ritka	2	4	6	8	10
Alkalmankénti	3	6	9	12	15
Gyakori	4	8	12	16	20
Nagyon gyakori	5	10	15	20	25

BM OKF (2021): i. m.

3. táblázat: Kockázati értékek besorolása

20–25	Azonnali beavatkozást megelőző védelmi intézkedést igénylő kockázat
15–19	Megelőző védelmi intézkedést igénylő kockázat
10–14	Intézkedést igénylő kockázat
5–9	Tervezett, későbbi intézkedést igénylő kockázat
1–4	Elhanyagolható kockázat

BM OKF (2021): i. m.

Fentiek alapján egy adott kockázat értékelése a következőképpen írható le a formanyomtatvány segítségével.

4. táblázat: Példa egy adott kockázat értékelésére BM OKF formadokumentum alapján, 1. rész

Kockázatgazda	**Kockázati főkategória**	**Kockázati alkategória**	**Kockázat részletes leírása**	**Bekövetkezés hatása**	**Bekövetkezés valószínűsége (1–5)**	**Hatás (1–5)**	**Kitettség (0–2)**	**Kontroll**	**Számított érték**	**Jelenlegi kockázat**
A megfelelő felhatalmazással bíró személy	A kockázat eredete	Főkategóriából eredő specifius kockázati alkategória [a 65/2013. (III. 8.) Korm. rendelet 2. mellékletében szereplő sorszámozással]	A kockázati tényező ismertetése	Abban az esetben, ha a kockázati esemény bekövetkezik, milyen hatással jár a vizsgált folyamatra, annak eredményére vonatkoztatva	A „Magyarázat KIV" fülön található táblázatból nyert érték	A „Magyarázat KIV" fülön található táblázatból nyert érték	A „Magyarázat KIV" fülön található táblázatból nyert érték	Módszer, amellyel meg tudjuk előzni a kockázat bekövetkezését, vagy csökkenteni a hatását	Teljes számított érték	Számított (max–25) érték [(kárérték+kitettség) x bek. valószínűség]
Igazgató	Humán	4.2.3.8. humán eredetű járványhelyzet	Humán eredetű járványhelyzet kialakulása, az egészségügyi ellátás olyan mértékű leterhelését eredményezi, ami a működését és alapellátását veszélyezteti	Betegellátás akadályozása, illetve esetleges alapellátások leállása, műtétek és kezelések elhalasztása, humán erőforrás és eszközök hiánya, megnövekedett munkavállalói terhelés	4	4	3	Járványügyi utasítások és eljárásrendek kialakítása, infrastuktúra esetleges átalakításának tervezése, előzetes felkészülés	24	24

Forrás: a szerzők szerkesztése

5. táblázat: Példa egy adott kockázat értékelésére BM OKF formadokumentum alapján, 2. rész

Kockázatcsökkentő intézkedés rövid neve	**Intézkedés részletesebb leírása**	**Az intézkedés státusza**	**Intézkedés felelőse**	**Intézkedés határideje**
Kockázatcsökkentő intézkedés tételes megnevezése	A kockázatcsökkentő intézkedés részletes leírása. Összetett eljárás esetén hivatkozni lehet intézkedési tervre, SZME-re, egyéb szabályozásra	Az intézkedésnek a kitöltés időpontjában aktuális állapota	Felelősök meghatározása („Intézkedést nem igényel” és „Megvalósított” státusznál nem kell kitölteni)	Elfogadott határidő („Intézkedést nem igényel” és „Megvalósított” státusznál nem kell kitölteni)
Járványügyi utasítások és eljárásrendek kialakítása, infrastruktúra esetleges átalakításának tervezése, előzetes felkészülés	Járványügyi utasítások és eljárásrendek kialakítása, szükséges építészeti alkotások, védőfelszerelések és eszközök, berendezések, munkavállalók oktatása	Folyamatban	Igazgató, kórházhigiénés terület, műszaki terület, gazdasági terület	Folyamatos

Forrás: a szerzők szerkesztése

6. táblázat: Példa egy adott kockázat értékelésére a BM OKF formadokumentum alapján, 3. rész

Bekövetkezés valószínűsége (1–5)	**Hatás (1–5)**	**Kitettség (0–2)**	**Megvalósított kontrollok**	**A kontroll helye (dokumentum)**	**A kontroll helye (oldal)**	**Maradványkockázat**	**Kockázatcsökkenés**
A kockázatcsökkentő intézkedések eredményeként várható becsült értékek, illetve a kockázatcsökkentő intézkedések megvalósulásának igazolása							Az intézkedések eredményeként a kockázat csökkentése
4	2	1	Minőségirányítási audit, gyakorlatok, előzetes szakhatósági engedélyek megkötése, járványügyi osztályok állománybiztosításának előzetes tervezése, átprofilozás feladatainak, erő-eszköz szükségleteinek tervezése, biztosítása	Infekciókontroll kézikönyv, Járványügyi utasítások és eljárásrendek, Egészségügyi Válsághelyzeti Terv, Többletfeladatok ellátása Részterv		12	12

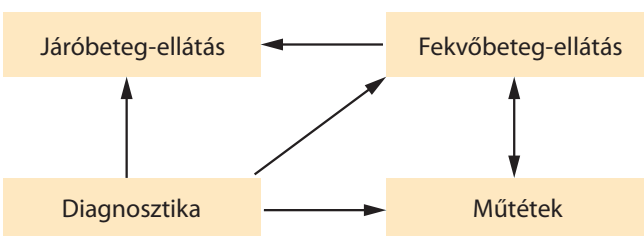
Forrás: a szerző szerkesztése

Az adott kockázat esetében, azt látható módon az adott létfontosságú rendszerelem üzemeltetője nem képes hatáskörén belül elfogadható szintre csökkenteni. Az ilyen esetekben elengedhetetlen a szakhatóság és az ágazati döntőbizottság általi helyzetértékelés és intézkedés. Jelen esetben például az összes rendszerelem kockázatértékelésének elemzése hatással lehet az Állami Egészségügyi Tartalékban lebiztosított eszközökre (járványügyi modul), az országos pandémiás tervezésre, vagy akár az azonosítási eljárás és kijelölés kritériumrendszerére is.

„A létfontosságú rendszerelem által harmadik féltől igénybevett szolgáltatások befolyásolhatják az üzemeltető által nyújtott szolgáltatást, vagy a rendszerelem üzemfolytonos működésére kihatással lehetnek. Ezeket a képlet súlyozottan veszi figyelembe (általánosan elmondható, hogy a fenti metodika mentén, a súlyozás hatására legalább egy kockázati kategóriát emelkedik a kapott érték). A kitettség csökkenthető például megfelelő garanciákat biztosító partneri szerződések (SLA) megkötésével, melyek kockázatcsökkentő intézkedésként a maradványkockázati értéket megfelelő szintre tudják redukálni."[4]

Kitettség azonban nemcsak szerződött partner felé (bár ilyen a közműszolgáltatóként megjelenő dependens kritikus infarstruktúra is), hanem befelé, saját folyamataink interdependenciájából is adódhat. Éppen ezért a folyamatalapú megközelítés során a kitettségi értéket dependeciaértékkel célszerű helyettesíteni.

Véleményünk szerint a fenti kockázatértékelési módszertant nem egyszerre az egész létesítményre szükséges vizsgálni. A tanulmány előző részében, az üzleti hatáselemzés során megállapítottuk a fekvőbeteg-ellátó létfontosságú rendszerelemek alapfolyamatát és fő folyamatait. Mindezt azért, hogy e fő folyamatok esetében legyen megállapítható azok kiesésének maximálisan tolerálható értéke, illetve a legutolsó helyreállítható állapot és a helyreállítási idő. A kockázatokat e folyamatonként egyesével kell értékelni, és figyelembe kell venni a folyamatok interdependenciáit is. Ezek alapján megállapítható az egyes részfolyamatok kockázata egymásra nézve is. Az egészségügyi, fekvőbeteg-ellátó infrastruktúrán belüli fő folyamatok interdependens jellegét az alábbi, 1. ábra mutatja:



1. ábra: Fekvőbeteg-ellátó létfontosságú rendszerelem fő folyamatainak interdependenciái
Forrás: a szerzők szerkesztése

[4] *BM OKF Kockázatelemzés kitöltési útmutató.* BM OKF, 2021.

Az interdependenciák konkrét, kockázatértékelések alapján végzett vizsgálata ágazatokon átívelően is szükséges. Az interdependencia

„kétirányú kapcsolat két infrastruktúra között, amelyen keresztül az egyes infrastruktúrák állapota befolyásolja vagy korrelál a másik állapotával. Általánosabban fogalmazva, két infrastruktúra kölcsönösen függ egymástól, ha mindegyik függ a másiktól. Ez a meghatározás azt sugallja, hogy az egyik infrastruktúra működőképessége függhet egy másik infrastruktúra működőképességétől. Ez azt is jelenti, hogy az infrastruktúrák kölcsönös függőségei növelik az általános strukturáltságot, hozzájárulnak a rendszer összetettségéhez, és alapját képezhetik olyan rendszereknek, amelyek funkcionalitása az egymástól kölcsönösen függő rendszerek összteljesítményétől függ. Ez a felfogás alátámasztja azt az állítást, hogy a közjólét – beleértve az egészségügyet, a gazdaságot és a biztonságot – fenntartásának célja több, egymással szorosan összekapcsolt rendszer bemeneteitől és kimeneteitől függ. Az ilyen infrastruktúrák közötti kapcsolatok nem egy-, hanem többirányúak. Ezért az ilyen infrastruktúrákban a kockázatok megfogalmazásakor figyelembe kell venni a létfontosságú infrastruktúrák közötti kapcsolatok kétirányú jellegét".[5]

3. Tervezés

A tervezés több részből áll, amelyek eredményeként létrejön a komplex Üzletmenet-folytonossági Terv.

Az üzletmenet-folytonossági alapok azonosítása és az üzletmenet-folytonossági megoldások kiválasztása az üzleti hatáselemzésen és a kapcsolódó költségeket figyelembe vevő kockázatértékelésen keresztül kell hogy történjen,[6] így az információszerzés szakaszában megismert fogalmakon keresztül a terv az alábbi részekből áll össze:

- kockázatértékelés intézkedési terve, amely a kockázatok csökkentését hivatott szolgálni;
- rendkívüli események kezelésnek terve;
- katasztrófakörülmények közötti működés terve – Egészségügyi Válsághelyzeti Terv;
- deeszkalációs tervezés, amely során a rendszerelem visszaáll a „békeidei" működésre.

A tervezés célja tehát a kockázatok csökkentése, a szervezet képessé tétele arra, hogy az egyes részfolyamatok csak az üzleti hatáselemzésben meghatározott maximálisan tolerálható időre állhassanak le egy-egy rendkívüli esemény idejére, és a meghatározott ponton visszaállíthatók legyenek, az alapfolyamat pedig a válságegészségügyi ellátás keretein belül ez idő alatt is működőképes maradjon.

[5] Katina Polinpapilinho et al.: Interdependency-Induced Risk with Applications to Healthcare. *International Journal of Critical Infrastructure Protection,* 7. (2014), 1. 12–26.

[6] ISO 22313:2020 Társadalmi biztonság. Üzletmenet-folytonossági irányítási rendszerek. Útmutató az ISO 22301 alkalmazásához. 25.

A központi egészségügyi igazgatás szintjén a tervek összegyűjtésének, elemzésének célja pedig nemzeti szinten a maximálisan tolerálható leállási értékek növelése, a relokáción keresztül a szükséges erők és eszközök létfontosságú rendszerelemek irányába való csoportosítása, mindezek tervezése.

A fenti alapelvek érvényesüléséhez minden üzletmenet-folytonossági tervnek meg kell határozni a rendeltetését, hatályát és céljait olyan formában, amely az azt használók számára egyértelmű. Az üzletmenet-folytonossági tervnek a következőket is tartalmaznia kell:

- aktiválási kritériumok és eljárások;
- végrehajtási eljárások;
- kommunikációs követelmények és eljárások;
- belső és külső kölcsönös függőségek és kölcsönhatások;
- erőforrásigény;
- információáramlási és dokumentációs folyamatok.[7]

4. Döntés

Egyes kockázatok csökkentésére, a válságegészségügyi tevékenység megvalósítási módjára több alternatív lehetőség is szóba jöhet, amelyek prioritási sorrendjét szükséges meghatározni, illetve el kell dönteni, hogy elsősorban melyiket valósítjuk meg. Ez a döntés a költségvetési források, illetve a szakirányító (anyagi, eszköz-, erőallokációs) támogatásának függvénye.

A tanulmány első részében megállapítottuk, hogy az általános üzleti folyamatalapú megközelítés során alkalmazott szemlélet, amely a pénzügyi profit maximalizálását tartja szem előtt, az egészségügyben nem alkalmazható, hiszen az egészségügyi intézmények alapfolyamatainak profitja a beteg egészsége, élete, amely pénzben nem mérhető. Ennek megfelelően a kontrollhatékonysági megfontolások sem klasszikus módon alkalmazhatók, tehát a kockázatkezelés költsége nem vethető össze, így egyensúlyban sem tartható a kockázat kezelésének elmaradása által létrejöhető kárértékkel. A döntés során tehát az egyetlen pénzügyi megfontolás a fekvőbeteg-ellátó intézmény – az évente újra és újra felhalmozódó kórházi adósságállományt látva, egyébként működtetésre is elégtelen – költségvetési kerete.

E döntés, döntések tulajdonképpen fentiek kiadmányozása tervrendszer formájában a létfontosságú rendszerelem üzemeltetője, azaz vezetője által.

A kiadmányozással, így a döntéssel együtt meghatározzák a kockázatcsökkentő intézkedések felelőseit, határidejét, hozzárendelik a végrehajtáshoz szükséges költségvetési forrást. Meghatározzák a rendkívüli események és a válságegészségügyi tevékenység végrehajtásáért felelős vezetőket, törzseket.

[7] ISO 22313:2020 Társadalmi biztonság. Üzletmenet-folytonossági irányítási rendszerek. Útmutató az ISO 22301 alkalmazásához. 40.

5. Végrehajtás

A tervrendszer végrehajtása általánosságban a végrehajtó állomány mint erő, illetve eszközök az adott feladathoz való hozzárendelése, beszerzése, lebiztosítása.

„A szervezet akkor minősül megfelelőnek a veszélyhelyzeti feladatok ellátására, ha rendelkezik egy megfelelően kiválasztott irányítási ponttal és az irányítás technikai infrastruktúrájával (kommunikáció, döntés-előkészítés, dokumentáció stb.).
A végrehajtó szervezet akkor alkalmas feladatainak ellátására, ha:

- az erő-eszköz számítások alapján megfelelő mennyiségben rendelkezésre állnak az erők, és a rájuk bízott feladatokat a terv szerint képesek ellátni,
- rendelkeznek egyéni védőfelszereléssel, speciális eszközzel, kommunikációs eszközzel, anyaggal, és ezek operatív alkalmazásra hozzáférhetőek,
- a rábízott veszélyhelyzet-kezelési feladatok elfogadható időn belül elvégezhetők,
- képzésüket, gyakorlataikat az előírásoknak megfelelően végezték."[8]

Az egészségügyi intézmények tervrendszere alapján a végrehajtás két részre osztható:

- „Békeidei" végrehajtás: leginkább az üzletmenet-folytonossági, tehát kockázatcsökkentő intézkedések végrehajtása, személyzettel és eszközzel való ellátása, a döntés során hozzárendelt költségvetési források biztosítása, beszerzések, közbeszerzések lefolytatása.
- Egészségügyi válsághelyzeti végrehajtás: az egészségügyi válsághelyzeti terv, illetve annak a rendkívüli eseményhez illeszkedő részterveinek alkalmazása, a terveknek megfelelő módon, illetve belső és külső együttműködési rendben.

6. Koordináció

A koordináció a tervek és a végrehajtás összehangolását jelenti. A végrehajtásnak megfelelően szintén két részre bontható.

- „Békeidei" koordináció: jelenti a különböző ágazati fejlesztési programok, intézményfejlesztési tervek és a kockázatkezelési intézkedések, valamint intézményi és központi közbeszerzési tevékenység összehangolását.
- Egészségügyi válsághelyzeti koordináció esetében egyrészt erősebb központi koordináció jelenik meg, hiszen a teljes egészségügyi igazgatás működése és irányítási, együttműködési rendszerei változnak meg, másrészt az intézményi válságegészségügyi tevékenység irányítása is átvált a tervekben kijelölt törzsvezetési rendszerre, amely által a szokásos feladatkiadási és jelentési útvonalak is megváltoznak.

[8] Kátai-Urbán Irina et al.: Risk Management in Population Protection. *Science for Population Protection,* 11. (2019), 2. 1–8.

7. Ellenőrzés

„A biztonságra kiható folyamatokat és tevékenységeket figyelemmel kell kísérni, monitorozni szükséges annak érdekében, hogy a normán aluli teljesítmények közvetlen okait meg lehessen határozni, és azon összefüggéseket fel lehessen tárni, melyek a biztonsági irányítási rendszer működtetésére hatással lehetnek.
A teljesítményeket külön meghatározott normákkal kell összevetni a szükséges változtatások azonosítása érdekében. Az aktív monitoring eljárásokkal megállapítható a biztonsági irányítási rendszer működésének hatékonysága."[9]

Az ellenőrzés során elengedhetetlen:

- az üzleti hatáselemzés felülvizsgálata rendszeres időközönként, amely megvalósulhat a létfontosságú rendszerelemek négyévenként esedékes azonosítási és kijelölési felülvizsgálata során, illetve a válságegészségügyi tevékenység vonatkozásában évente, az egészségügyi válsághelyzeti tervek kötelező felülvizsgálata során;
- a kockázatértékelés felülvizsgálata rendszeres időközönként, amely természetesen minden egyes esetben megvalósítandó, amikor az üzleti hatáselemzés felülvizsgálata után a folyamatok, illetve azok kiesési és visszaállítási értékei változnak, illetve olyan rendkívüli események után, amelyek hatással lehetnek a kockázati értékek egyes összetevőire;
- a munkavállalók tudásának ellenőrzése, ami megvalósulhat éves oktatások és különösen e-learning-rendszerű oktatás során hatékony teszteléssel, illetve gyakorlatokkal;
- az egyik leghatékonyabb és legpraktikusabb módja az ellenőrzésnek – elsősorban a rendkívüli események kezelési, visszaállítás, és egészségügyi válsághelyzeti tervezés esetében – a gyakorlatoztatás, amely során mindhárom fenti ellenőrzési módszerhez kaphatunk adatokat. Amennyiben a gyakorlatnak nemcsak a végeredményét mérjük (sikeres/sikertelen), hanem az egyes részfeladatokat is ellátjuk kvalitatív és kvantitatív mutatókkal, úgy egyén, raj, törzs, illetve intézményi szintű adatokhoz is juthatunk, amely segíti a továbbiakban a tervek komplex, egyes részfolyamatok egymásra hatását is figyelembe vevő módosítását, illetve a szükséges erő-eszköz allokáció finomhangolását is.

Az ellenőrzés lehetséges eszköze lehet a monitoring, mérés, elemzés és értékelés, amely követelményrendszert annak biztosítására hozták létre, hogy megfelelő mérőszámok álljanak rendelkezésre az üzletmenet-folytonossági rendszerek hatékony kezeléséhez, illetve bemenetet biztosít a vezetői áttekintésekhez. Ellenőrzési eszköz a belső audit, amelynek elsődleges követelménye, miszerint az ellenőrzött területért felelős vezetőnek gondoskodnia kell arról, hogy minden szükséges korrigáló intézkedés késedelem nélkül megszülessen az észlelt eltérések és okaik felszámolására. A vezetői felülvizsgálat során pedig tájékoztatást kell nyújtani az audit során feltárt nem

[9] Kátai-Urbán Lajos – Mesics Zoltán: Veszélyes üzemi biztonsági irányítási rendszer működtetése. *Hadmérnök,* 10. (2015), 1. 99–107.

megfelelőségekről és korrekciós intézkedésekről, a monitoring és mérési értékelés eredményeiről és az összefoglaló auditeredményekről.[10]

Általánosan az ellenőrzés során felteendő kérdések:

- Csökkennek a kockázati értékek, összeségében a lehetséges veszteségek?
  - A bekövetkezés valószínűsége.
  - Az okozható kár értéke.
  - A kitettségek.
- Növeltük a maximálisan tolerálható leállási értéket?
- Kitoltuk a visszaállítás még lehetséges utolsó kezdeti időpontját?
- Csökkentettük a visszaállításhoz szükséges időszakot?
- Így összességében tehát az egész rendszer biztonságosabb?

Az ellenőrzés során alkalmazott fő teljesítménymutatók (*key performance indicators,* KPI) segítségével az üzletmenet-folytonossági rendszereink hatékonyságát mérhetővé tudjuk tenni.

Ilyen fő teljesítménymutató a fent meghatározott összes, az ellenőrzés során felteendő kérdésre kidolgozható. Egyesek szerint a hatékony mérés követelménye a mért adatok szélesebb körén alapszik, tehát minél több mérőszám és további információ gyűjtésén, minél több helyről, más szakértők szerint pedig az adatok minősége fontosabb, mint a mennyiség. Ez utóbbi szempont szerint a mérési céloknak egyszerre kell SMART-nak és DUMB-nak lennie, azaz az angol akronimek megfejtéseként a követelmény a mérési célokkal szemben a specifitás *(specific),* a mérhetőség *(measurable),* az elérhetőség *(available),* a relevancia *(relevant)* és az időalapúság *(time-based),* valamint a megvalósíthatóság *(doable),* érthetőség *(understandable),* a kezelhetőség *(manageable)* és a jótékony hatás *(beneficial).*[11]

8. Összefoglalás

Az egészségügyi ágazat és alágazatai létfontosságú rendszereinek és rendszerelemeinek, jogszabály által előírt, üzemeltetői biztonsági tervezésében szemléletmódváltás érhető el, és a tervezés, illetve az üzemeltetés hatékonysága növelhető minőségirányítási rendszerek, azon belül is az üzletmenet-folytonossági menedzsmentrendszerek alkalmazásával.

Tanulmányunk első részében rámutattunk, hogy az üzletmenet-folytonossági rendszerek működtetésének első mérföldköve a tervezés, amelyet azonban a célkitűzésnek és az információszerzésnek meg kell előznie. Ehhez elsődleges fontosságú a menedzsment meggyőzése, az értékgazdák azonosítása, aki a megfelelő információkkal el tudnak látni és a tervezésben is részt vesznek, majd ezen értékgazdákkal közösen azonosítandók az alapfolyamatok és ezek megzavarásának üzleti hatáselemzése, tehát az alapfolyamatra gyakorolt hatásának feltárása.

[10] MSZ EN ISO 22301:2020 Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek. 50–52.
[11] BSI UK: *Measurement Matters – The Role of Metrics in ISO 22301 – A BSI Whitepaper for Business.* 2015. 4.

Tanulmányunk jelenlegi, második részében feltártuk, hogy az üzleti hatáselemzés után kezdődő kockázatértékelésnek minden egyes folyamatra ki kell terjednie, és a megállapított maximálisan elfogadható leállási értékek alapján rangsorolhatók a kritikus nyomvonalak, az egyes kockázatok, fenyegetések. Majd az azonosított kockázatok a kritikusság rangsorolása, az interdependenciák figyelembevétele, illetve a tolerálható leállási és szükséges helyreállítási értékek alapján elkészülhet a komplex intézkedési terv.

A tervezés fázisa után a döntési fázisban vissza kell térni az egészségügyi kritikus infrastruktúrák üzletmenet-folytonossági rendszereinek tervezése során kimondott alapvetésünkhöz, amely során megállapítottuk, hogy az egészségügyi intézmények alapfolyamatainak profitja a beteg egészsége, élete, amely pénzben nem mérhető, tehát a kockázatkezelési döntések során nem alkalmazható a költség-haszon elv pénzügyi értelemben.

Ahhoz, hogy a komplex üzletmenet-folytonossági rendszer, tehát a jogszabályok által előírt Üzemeltetői Biztonsági Terv és Egészségügyi Válsághelyzeti Terv praktikus, a gyakorlatban is alkalmazható legyen, elengedhetetlen a tervrendszer ellenőrzése, hatékonyságának visszamérése. Ennek legcélszerűbb eszköze a jogszabály által is előírt, azonban az üzemeltetői és hatósági gyakorlatban az egészségügyi létfontosságú rendszerek esetében nem alkalmazott komplex gyakorlatok végrehajtása, amelyek részfolyamatai kvalitatív és kvantitatív teljesítménymutatóinak meghatározásával, mérésével a tervrendszer tökéletesíthető.

Felhasznált irodalom

Kátai-Urbán Irina – Cimer Zsolt – Szakál Béla – Vass Gyula: Risk Management in Population Protection. *Science for Population Protection,* 11. (2019), 2. 1–8.

Kátai-Urbán Lajos – Mészáros István – Vass Gyula: Iparbiztonság, válsághelyzeti tervezés. In Major László (szerk.): *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai.* Budapest, Semmelweis Kiadó, 2019. 48–83.

Kátai-Urbán Lajos – Mesics Zoltán: Veszélyes üzemi biztonsági irányítási rendszer működtetése. *Hadmérnök,* 10. (2015), 1. 99–107.

Polinpapilinho, Katina – C. Ariel Pinto – Joseph Bradley – Patrick Hester: Interdependency-Induced Risk with Applications to Healthcare. *International Journal of Critical Infrastructure Protection,* 7. (2014), 1. 12–26. Online: https://doi.org/10.1016/j.ijcip.2014.01.005

Felhasznált szabványok, útmutatók

BM OKF KIV kockázatelemzési formadokumentum. BM OKF, 2021.

BM OKF Kockázatelemzés kitöltési útmutató. BM OKF, 2021.

BSI UK: *Measurement Matters – The Role of Metrics in ISO 22301* – A BSI Whitepaper for Business. 2015.

ISO 22313:2020 *Társadalmi biztonság. Üzletmenet-folytonossági irányítási rendszerek. Útmutató az ISO 22301 alkalmazásához*
MSZ EN ISO 22301:2020 *Társadalmi biztonság, Üzletmenet-folytonossági irányítási rendszerek*

HADMÉRNÖK
FÓRUM
17. évfolyam (2022) 3. szám 169–185.
DOI: 10.32567/hm.2022.3.11

Dóra Molnár,[1] Patrik Szalkai[2]

Could the Arctic Be a New Field of Advocacy for Hungary?

Climate change is driving the discovery of more and more minerals hidden in the Arctic, for which the initial stage of the struggle is already underway. As this process intensifies, so the number of countries interested in the region is expanding. Hungary cannot be left out of this process, but the articulation of Hungarian interests is still in its infancy. The paper examines how the Arctic region is currently reflected in Hungarian strategic documents and how actual cooperation with the Arctic states is developing. Finally, the paper outlines the elements on which Hungarian interests and actions concerning the Arctic can be built in the future.

Keywords: **Arctic region, Hungarian interests, strategy**

1. Introduction

The Arctic is a region that has been significantly valorised in recent decades. Climate change is opening up new shipping routes and new economic opportunities that could bring significant strategic advantages to countries that are able to exploit them. Increasingly, states are engaging with the region which, at first glance, would find it difficult to see that it is worth investing resources and capital in their presence in the region. Among the European countries, Germany and France now have their own Arctic strategy,[3] and states such as Mediterranean Spain and Italy, which have a particularly warm climate and are located in the Mediterranean, and Switzerland, which is located in the middle of the continent with no access to any sea, have also signed up as observers to the Arctic Council.

The question rightly arises as to whether Hungary, like Switzerland or Spain, should be concerned about the Arctic? The paper seeks to answer this question both

[1] University of Public Service, Faculty of Military Sciences and Officer Training, Department of International Security Studies, e-mail: molnar.dora@uni-nke.hu
[2] University of Public Service, Faculty of Military Sciences and Officer Training, International Security and Defence Policy Msc, e-mail: zpatrik141@gmail.com
[3] Ministry of Foreign Affairs and International Development: *The Great Challenge of the Arctic. National Roadmap for the Arctic.* Paris, 2016; Federal Foreign Office: *Germany's Arctic Policy Guidelines. Assume Responsibility, Seize Opportunities.* Berlin, 2013.

theoretically and through examples from today, and proposes the basic elements of a future Hungarian Arctic policy.

2. Hungarian strategic thinking about the North Pole

The analysis of strategies is based on the most up-to-date and valid Hungarian strategy documents in force, and limited to sectors such as foreign policy, security policy, energy policy and climate change. Climate change is of particular importance because it has become a key driver of the security and economic revaluation of the Arctic region, and the impact of environmental processes in the region is not limited to the region, but has global implications.

The first comprehensive strategy document is the *Hungarian Foreign Policy Strategy,* published in 2011. Although the strategy does not specifically mention the Arctic region, the third of its three priorities, global openness, could serve as a basis for future work on the Arctic.[4] Although the focus of the strategy is on the post-Soviet space, Asia, the Middle East, North Africa, Sub-Saharan Africa, the Sahel and Latin America, the very fact that the third priority is to turn Hungarian foreign policy towards regions that have received little or no attention so far offers an opportunity to enhance the value of the Arctic for Hungarian foreign policy. All the more so as the strategy underlines that

"…global attention means our interest in issues that do not necessarily seem to affect our country directly, but are important in global terms and therefore gain in international importance. […] At the same time, we must also be aware that, because of the increasingly interconnected and interdependent nature of world processes, issues that seem to affect us only marginally also have an impact on the circumstances whose development is a priority issue for our domestic development and the foreign policy that is intended to help it".[5]

The message of the strategy is therefore that Hungarian foreign policy must address regions of global importance even if they currently have little direct impact on the country. In addition, the need to monitor global changes in energy policy and geopolitics means that the current foreign policy strategy should already include the Arctic as a third foreign policy priority.

In 2020, the Hungarian Government published a new *National Security Strategy* (NSS), entitled *Hungary in a Changing World.* This strategy also does not attribute much importance to the region, but it is worth highlighting that it recognises the growing role of the Arctic in the great power competition: "The power competition is increasingly extending to the global commons: there is an increasing struggle for

[4] The three main priorities of the strategy are: regional policy (Central and Southeastern Europe); Euro-Atlantic orientation (representation of national interests in the EU and NATO); global opening (highlighting relationships that have been pushed into the background or always lost in recent years). See Ministry of Foreign Affairs of Hungary: *Hungary's Foreign Policy after the Hungarian Presidency of the Council of the European Union.* 2011.

[5] Ministry of Foreign Affairs of Hungary (2011): op. cit. 36–37.

control of international waters and resources, the Arctic and outer space, and the dominance of cyberspace."[6]

Interestingly, the 2012 *National Military Strategy* (NMS) is eerily similar in its approach to the global commons, except that it identifies international airspace as a global commons, but not the Arctic.[7] In contrast, the 2021 NMS no longer includes global public goods as a concept and, like the 2012 strategy, does not address the Arctic, while cyberspace and space will play a larger role than in its 2012 predecessor.[8]

The relationship between the Arctic region and Hungary is given the greatest weight in the *Second National Climate Change Strategy 2018–2030, looking ahead to 2050* published by the Ministry for Innovation and Technology in 2018.[9] The aim of this very long, 251-page strategy is to prepare the country for the challenges posed by climate change. It takes stock of how this process will affect different sectors and then sets out proposals and objectives for the short, medium and long term.

In relation to the Arctic melt, it addresses the issue in the section on "Climate Change Security Implications for Hungary", stating that "[a]n immediate risk factor is that Hungary could become a destination or transit country for global climate migration from the sea areas flooded by melting Arctic ice caps, as well as from prolonged heat waves, droughts and severe water and food shortages in the Middle East, North Africa and possibly the Mediterranean countries".[10] The strategy sets out two long-term lines of action for the security sector. The first is the full integration of climate change into national security policy, and the second is "preparing to prevent and counter direct or indirect economic, political or even armed attacks to control natural resources, in particular drinking water and land".[11]

All this suggests that strategies that address the challenges of the present pay little attention to the region, preferring to see it as an issue for the future. This may be due to the fact that strategies such as the NSS or NMS accepted for 5 to 10 years expect the challenges facing the region to become relevant only after 2030. The 2018 strategy, however, is a clear sign that the long-term security policy implications for the region are already being recognised in Hungary, as well.

This is already clearly visible in political manifestations at senior management level. In 2017, Péter Szijjártó, Minister of Foreign Affairs and Trade, participated in the Arctic Frontier Conference at the invitation of the Norwegian Foreign Minister Børge Brende. In his speech he spoke about the relationship between the Arctic and the European Union (EU) and the future role of the region. He made several arguments in support of his presence. Hungary has recently been granted observer status in the Council of the Baltic Sea States (CBSS), and the minister humorously mentioned the Austro–Hungarian Empire's colonialism in the region, which, although not a real argument in this case, is Hungary's oldest and most important historical relationship

6 1163/2020 (IV. 21.) Government Resolution on the National Security Strategy of Hungary. Point no. 148.
7 Ministry of Defence: Hungary's National Military Strategy. 2012. 10.
8 1393/2021 (VI. 24.) Government Resolution on the National Military Strategy of Hungary.
9 Ministry for Innovation and Technology: 23/2018 (X. 31.) Parliamentary Resolution on the Second National Climate Change Strategy 2018–2030, looking ahead to 2050.
10 Ministry for Innovation and Technology (2018): op. cit. 160.
11 Ministry for Innovation and Technology (2018): op. cit. 187.

with the Arctic. Furthermore, he argued that the biggest challenges of European integration, energy security, security in general and EU–Russia relations all appear in the Arctic, and therefore the European Union and Hungary want to contribute to a long-term Arctic strategy.

In his speech, concerning Hungary's position on the Arctic, he also stated that a balance must be struck between environment, economy, energy and competitiveness. Not enough attention is paid to the fact that the largest hydrocarbon reserves are located in the Arctic, but the current peaceful period of recovery should be used to prepare for the coming hydrocarbon discoveries and exploration by establishing international regulations for the Arctic. After all, an expanding population and economic growth will mean that Arctic energy resources will come to the fore.[12]

Minister Péter Szijjártó attended the conference again in 2018, this time at the invitation of the Norwegian Minister of Foreign Affairs and Terje Søviknes, Norwegian Minister of Petroleum and Energy.[13] At this conference, he again began his speech by explaining why a representative from a country so far from the Arctic was holding a speech. Among the reasons he gave was that what is happening in the Arctic has a global impact, which affects Europe in particular. He then identified three factors that have a strong influence on the development of Hungarian policy and which are also closely linked to the Arctic. He stressed that Hungary has one of the world's largest water resources, including thermal and drinking water, and therefore water management is one of the flagships of Hungarian industry. This makes the country particularly vulnerable to global events affecting sea level change, which can contribute to drinking water shortages. The second aspect is migration, which is predicted to create humanitarian and security challenges in the coming decades due to climate change, in addition to political debates. The third aspect is the economy. Hungary is a very open economy, heavily dependent on foreign direct investment and exports, but a balance needs to be struck between competitiveness and environmental protection. The Foreign Minister then highlighted three areas where Hungary can contribute to the EU and Norway's Arctic policy:

- increasing the use of nuclear energy in electricity generation from 43% to 65% and reducing emissions
- supporting the production and purchase of electric cars in the automotive sector through financial instruments, innovation and research and development
- participation in the Arctic Frontier forum year after year

The Hungarian minister explained the third point in detail. The Arctic has become an integral part of global politics, and is a good example of how major conflicts can only be resolved through dialogue, with the participation of all parties concerned.[14]

It is clear from the two ministerial speeches that, in the Foreign Minister's interpretation, the relationship between Hungary and the Arctic has economic and geopolitical dimensions, and indirectly, Hungary's membership of the EU also means

[12] Arctic Frontiers: Arctic Frontiers 2017 The Arctic in a Global Context. *YouTube,* 25 January 2017.
[13] Ábrahám Vass: Hungarian Oil Company MOL expands further in Norway. *Hungary Today,* 24 January 2018.
[14] Arctic Frontiers: Arctic Frontiers Policy 2018. Speaking Truth to Power. Science Based Policy in a Post-Fact World. *YouTube,* 15 June 2018.

that the region needs to be addressed. It is no less important to note that Hungary has a strong position on the international regime governing Arctic resources, and supports and considers it necessary. These aspects point to strategic interests, all the more so since they have been channelled into the political discourse at ministerial level.

3. The Hungarian Arctic presence

In the light of the above, it is perhaps not so surprising that Hungary cooperates with Arctic states in a number of areas. One such state is Sweden. In 2001, the Hungarian Government signed a contract for the lease of 14 Gripen fighters, making Hungary the third country after Sweden and the Czech Republic to have systematically deployed Gripen C/D variants.[15] This cooperation has been so successful that the two countries signed an agreement in 2022 to upgrade the fighter aircraft fleet with the MS20 Block 2 capability, which will be delivered by SAAB. This upgrade will expand both the combat and communications capability of the Gripen and the range of weapons that can be integrated on the fighters.[16] Another meeting point in the Arctic regarding the Gripen is that pilot training will continue in Canada, as part of NATO's Canadian Air Training Programme. The first phase of the Canadian training, which was successfully completed by 95 Hungarian pilots between 2002 and 2018,[17] will begin in Hungary on Zlin-242 aircraft, followed by a Canadian training course lasting at least two years. Those who successfully complete the Canadian training will be assigned to Gripen after a retraining period in Sweden.[18]

A further result of the Swedish–Hungarian cooperation is that in 2019 it was decided that Hungary will put into service the Swedish SAAB Bofors Dynamics Carl Gustaf M4 recoilless rifle. The order is worth USD 55 million and delivery will take place between 2019 and 2024.[19] Finally, another Swedish company, Volvo, has also been involved in the modernisation of the Hungarian Defence Forces. The first prototype of the Currus Aries bus, produced in Gödöllő, was built on the Volvo B7R chassis in 2013, and from 2017 Volvo has also supplied the Euro6 engine and many other components for the buses.[20] In 2019, the last of the 100 buses ordered was handed over to the Army.[21] (Hungary also came into contact with the Norwegian defence industry when it decided to procure the Norwegian–American NASAMS air defence system in 2020.)[22]

15 Saab: Gripen roars over Hungary for 15 years. *Saab,* 30 March 2021.
16 Saab: Saab to Deliver Upgrade for Hungarian Gripen Fleet. *Saab,* 12 January 2022.
17 Only five people were unable to complete the training.
18 Sándor Galambos: A Griff hangja. *Honvéd,* 8 (2022). 36–45; Gábor Baranyai: Kanadában képezik a Honvédség pilótáit. *Magyar Nemzet,* 24 August 2019.
19 KaliberInfo: 55 millió dollárért vesz Carl Gustaf M4-eseket a Magyar Honvédség. *KaliberInfo,* 08 January 2019.
20 István Dániel Ott: A Currus Aries 01 többfunkciós moduláris jármű kifejlesztése és feladatai a magyar haderőben I. rész. *Haditechnika,* 54, no. 4 (2020). 58–62; István Dániel Ott: A Currus Aries 01 többfunkciós moduláris jármű kifejlesztése és feladatai a magyar haderőben III. rész. *Haditechnika,* 54, no. 6 (2020). 58–63.
21 Gábor Kámánfi: Átadták a századik honvédségi Currus Aries buszt. *Honvédelem,* 28 November 2019.
22 85% of the purchase price (HUF 130 billion) is covered by an export credit provided by Export Credit Norway (ECN) and the Norwegian Export Credit Guarantee Agency (GIEK). See Mfor.hu: Haderő-fejlesztés Magyarországon: 130 milliárdos hitelt kapunk hozzá. *Mfor.hu,* 17 March 2021.

In addition, Sweden is the second largest contributor of hours to the Pápai International Heavy Airlift Regiment, with 550 hours[23] and the other three Arctic states, together with the Arctic states of the United States, Finland and Norway, account for 65.2% of the regiment's flying hours,[24] which also means that these Arctic states contribute a large share of the costs.[25]

From a NATO perspective, it is worth mentioning the Arctic exercises in which Hungary is also participating. In the 2018 Trident Juncture exercise, which involved 50,000 troops, 15 soldiers from the Hungarian Material Supply Depot Base took part, and their task – in cooperation with German soldiers – was to install a field fuel depot and operate it as part of the theatre fuel supply system.[26] Hungary also participated in the 35,000-strong Cold Response 2022 exercise in March–April 2022, which was notable for the fact that not all NATO member states were present (only 23), but Norway was also among the participants.[27]

In the context of the Hungarian presence, it is also important to highlight the expansion of Hungarian Oil and Gas Plc (MOL Group, hereinafter referred to as "MOL") in Norway. In 2015, MOL successfully completed the previously announced acquisition of 100% of Ithaca Petroleum Norge ("IPN") from Ithaca Petroleum Ltd., which is now operating under the name MOL Norge. According to the statement, the transaction includes more than 600 million barrels of unrisk-weighted geological assets, mostly oil, which will double the MOL Group's exploration portfolio. Commenting on the acquisition, Alexender Dodds, Managing Director of Exploration Production, said: "Norway will be a key exploration hub for the MOL Group in the future, helping us to achieve our goal of becoming a marine operator in the North Sea."[28] However, it is also important to note that MOL sold its stakes in two wells in April 2022.[29] Although the specific drilling areas do not fall within the Arctic, they are quite close to the Arctic border in an Arctic state. At the same time, MOL had an Arctic interest in Russia, but the 100%-owned Matyushinsky block in Western Siberia was sold in 2016.[30] In addition to the investment, the parties also agreed to support each other's efforts within the UN, and Hungary in particular will support Norway's candidacy for non-permanent Security Council membership in the 2021–2022 term. Norway has successfully won this membership. In 2017, the two countries agreed to cooperate in the field of health care, whereby Norwegian patients will be treated in Hungary, and Hungary plans to increase agricultural exports to Norway.[31] In the energy sector, Hungary has also entered into strategic partnerships with ExxonMobil, a Texas-based

[23] Swedish Armed Forces: Hungary (HAW). s. a.
[24] USA 32%, Sweden 17.4%, Norway 12.6%, Finland 3.2%.
[25] Strategic Airlift Capability: The Strategic Airlift Capability (SAC). s. a.
[26] Melinda Hovány-Pap – István Háda: Eredményesen zárult a Trident Juncture 2018 gyakorlat. *Honvédelem,* 05 December 2018.
[27] Astri Edvardsen: Cold Response 2022: 35,000 Soldiers from 26 Countries in Northern Military Exercise. *High North News,* 18 January 2022.
[28] MOL Group: A MOL sikeresen lezárta az Ithaca Petroleum Norge megvásárlását. 09 July 2015.
[29] Melisa Cavcic: Norwegian Player Seeks Operatorship as MOL Norge Offloads Two North Sea Discoveries. *Offshore Energy,* 18 April 2022.
[30] MOL Group: Annual Report *2016.* 39.
[31] MTI: Hungary Seeks Closer Ties with Northern Europe, Says Foreign Minister in Norway. *Daily News Hungary,* 25 January 2017.

company that is one of the largest players in Arctic gas and oil exploration, alongside several Swedish, Finnish and Canadian companies.[32]

In the context of Arctic sea routes, the *Hungarian port of Trieste* should be highlighted, as its acquisition was an important aspect of supporting the competitiveness of Hungarian exports.[33] The advantage of the port is its geographical proximity compared to Europe's largest ports: while Rotterdam or Piraeus are around 1,500 km from Budapest, Trieste is only 500 km away. This is important mainly because land transport is orders of magnitude more expensive than sea transport. It is also worth noting that between 2005 and 2019, container traffic in Trieste tripled, so this is presumably an investment that can pay off in the long term.[34]

The port acquisition in 2019 will mainly serve to connect Europe to China via Italy (as well as to facilitate access to the Arab parts of Africa and the Middle East). The One Belt One Road Initiative,[35] which will connect Europe to China, aims to reach Europe via two planned routes.[36] One is the Northern Sea Route, the other is mainly over land and through the Mediterranean. Furthermore, taking into account the Budapest–Belgrade railway line that will be part of it, this also means that Hungary has a counter-interest in this respect in the development of the Northern Sea Route, which bypasses Hungary – although presumably this route will be faster and cheaper to transport under the circumstances.

Another area of cooperation with the Arctic states is *research cooperation*. In 2021, Hungary signed a Memorandum of Understanding on space cooperation with Finland. The agreement creates opportunities for cooperation between companies and higher education institutions in the development of space research, Earth observation and vehicle navigation technologies.[37] In 2022, Hungary signed a Memorandum of Understanding with Russia to continue the bilateral cooperation in space exploration that started in 1999. Three major Hungarian–Russian space research programs have been launched in the last three years, involving Russian and Hungarian research institutes, universities and companies.[38]

There is little attention paid to the Arctic among Hungarian researchers, and no Hungarian has ever undertaken a full expedition to the Arctic. However, given that the climatic conditions are similar to Antarctica and that some Arctic Council observer states (e.g. Spain, India) have used their Antarctic activities as an argument to legitimise their Arctic presence or as a strategy to link the two regions, the Hungarian presence in the Antarctic is worth investigating.[39] Krisztina Kovalcsikné Bátori and

[32] Ministry of Foreign Affairs and Trade of Hungary: *Stratégiai partnerségi megállapodások.* s. a.
[33] András Kovács: Szijjártó Péter a trieszti kikötőről: Ezzel Magyarország erősödik. *Origo,* 26 July 2019.
[34] Agrárszektor: Jó ötlet-e a trieszti magyar kikötő? *Agrarszektor.hu,* 24 July 2019.
[35] Xi originally announced the strategy as the "Silk Road Economic Belt" during an official visit to Kazakhstan in September 2013. Nowadays it is called Belt and Road Initiative (B&B or BRI).
[36] Jana Robinson: Arctic Space Challenge for NATO Emerging from China's Economic and Financial Assertiveness. *Transforming Joint Air and Space Power. The Journal of the JAPCC,* 30 (2020). 35–40.
[37] Government of Hungary: Magyarország és Finnország űripari együttműködésről állapodott meg. *Magyarország Kormánya,* 14 September 2021.
[38] Ferenc Kovács: Aláírták a magyar–orosz űregyezményt. *Index,* 12 February 2022; Ferenc Horvai: Harmincéves kapcsolataink az Európai Űrügynökséggel. *Aero Magazin,* 17 September 2021.
[39] Rajesh Gawande: India's Engagement with Arctic Council. December 2016; Arctic Council: *Spain – Observer Report 2020.*

Zoltán Ács were the first to reach the South Pole in 2004, but they only completed the last stage of 11 km. They also made it to the North Pole, but here they travelled to the 87th parallel by helicopter.[40] In 2019, Gábor Rakonczay became the first Hungarian to walk the 917 km distance between Antarctica and the South Pole.[41]

Hungarian research activity in the Antarctic goes back a long way. The exploration of the region by Hungarians began with an astronomical expedition in 1874, and many Hungarian explorers have subsequently visited Antarctica.[42] After the regime change, the most significant Hungarian research started in 1998 on King George Island on the edge of Antarctica, and by 2003 it had evolved into the first fully Hungarian research expedition, called the "Frozen Oasis" Research and Film Expedition. The ice-free areas at the Antarctic margin are very sensitive to short-term environmental changes and are therefore ideal for studying climate change. The Hungarian researchers then returned to the site in 2005 to investigate how the processes shaping the ice-free areas on the surface have changed over the past two years and the rate at which the topography is changing.[43] From the Hungarian perspective, the importance of the research was justified by the fact that the study of the Arctic climate and the movement of Antarctic ice can help to understand the archaeogeography of the Carpathians and their development during the Ice Age.[44] Due to lack of funding, the expedition was not supported by ministries or academia. The Hungarian Academy of Sciences also supported the expedition only on a technical level.[45] According to one of the participants, Sándor Fira, "we had to admit that Hungarian Antarctic research does not yet feature prominently among the concrete goals of Hungarian science".[46] However, the 2005 expedition[47] was supported by the Zoltán Magyary Postdoctoral Fellowship of the "Foundation for Hungarian Higher Education and Research", the Department of Natural Geography of Eötvös Loránd University, the Geographical Research Institute of the Hungarian Academy of Sciences, the Geochemical Research Laboratory of the Hungarian Academy of Sciences and the Collegium Budapest – Institute for Advanced Study. Other collaborating partners were the Korean Ocean Research and Development Institute[48] and the Chilean Antarctic Institute.[49]

Zsófia Jurányi, a physicist working on the optical properties of aerosols, studied the relationship between aerosol particles and climate change at the German Neumayer III station from December 2016 to February 2018, also at the German Alfred Wegener Institute.[50] Finally, in 2021, the MTA–ELTE Theoretical Physics Research Group and MTA–MTM–ELTE Paleontology Research Group, part of the Eötvös Loránd Research

[40] Index: Magyarok elsőként a Déli-sarkon. *Index,* 16 January 2005; HVG: Két magyar hegymászó is elérte az Északi-sarkot. *HVG,* 20 April 2004.
[41] Sándor Joób: Első magyarként elérte a Déli-sarkot Rakonczay Gábor. *Index,* 08 January 2019.
[42] Kele František – László Fekete: *Jég és föld között. Az Antarktisz (újra)felfedezése.* Dunaszerdahely, Nap Kiadó, 2003. 131.
[43] Origo: Újra magyar kutatók az Antarktiszon. *Origo,* 10 February 2005.
[44] Sándor Fiar – Balázs Nagy: *Olvadó jövő.* Budapest, General Press Kiadó, 2004. 26.
[45] Fiar–Nagy (2004): op. cit. 9, 11.
[46] Fiar–Nagy (2004): op. cit. 11.
[47] Fagyos Oázis Kutatócsoport: Hungarian Scientific Program 2005. *Antarctica.hu,* 2005.
[48] Korean Ocean Research and Development Institute, KORDI.
[49] Instituto Antártico Chileno, INACH.
[50] Attila Károly Nagy: Két hónapos jó éjszakát kíván az Antarktiszon áttelelő magyar kutatónő. *Index,* 20 May 2017.

Network (ELKH), and the Konkoly Thege Miklós Institute of Astronomy of the ELKH Centre for Astronomy and Earth Sciences (CSFK), the ELKH Institute of Geophysics and Space Science (FI) and the Department of General and Applied Geology of ELTE, investigated the adequacy of the widely accepted textbook explanation of the so-called Eocene-Oligocene transition.[51] It is therefore fair to say that over the past twenty years, the importance of Arctic research has greatly increased, with the most prestigious universities and research institutes now taking part.

4. Conclusions based on Hungarian strategies and practice

Based on all these strategic documents and actual practice, we can say that there is a Hungarian presence in the Arctic and that specific Hungarian interests can be identified. These are as follows:

Direct Hungarian interests:

- further increasing economic ties in a spirit of global openness, with a focus on the defence and energy sectors
- participation in the management of Arctic warming as a factor affecting Hungary, because:
  - environmental change reinforces migration
  - from a geopolitical point of view, it increases the country's vulnerability to freshwater supplies and increases the potential for conflict in the Arctic
  - it could be economically disadvantageous because it opens up a route between Europe and China that bypasses Hungary
- supporting dialogue between the major powers in the region, involving all stakeholders
- support for comprehensive international regulation of hydrocarbon exploitation in the region

Indirect Hungarian interests:

- the growing presence of NATO makes it necessary to prepare the Hungarian Defence Forces for these special climatic conditions, so participation in these military exercises is among the national interest
- the European Union also supports the presence in the region with significant resources and programs, participation in which can help to promote direct interests

However, the problem is that the current Hungarian strategy documents do not address the region, or address it only to a limited extent, and Hungary does not have an independent Arctic strategy. A further handicap is that the Hungarian defence industry is not yet present in the region, but this may be due to the fact that industrial capacities are still being built up. In the future, however, the region could become a target for the Hungarian industry, as in other countries. Finally, the fact that Hungary

[51] MTI: Magyar kutatók megfejtették, hogyan jegesedhetett el az Antarktisz. *Origo,* 07 October 2021.

does not have observer status in any regional international organisation is also a major constraint. The latter is a possibility that deserves further discussion.

4.1. Arctic Council as an untapped Hungarian opportunity

International cooperation in the region has seen a significant upsurge since the end of the Cold War, with more than a dozen regional organisations now operating in the region. Their activities cover virtually everything from environmental protection to economics and research. It would therefore greatly facilitate the promotion of the interests already identified if Hungary, following the example of many other non-Arctic states, were to acquire observer status in the organisations best suited to its interests. Although Russia's membership in the largest regional organisations has either been suspended or boycotted by other states (Arctic Council, Barents Euro-Arctic Council, Nordic Council)[52] due to the Russian–Ukrainian war, this should not be interpreted as a permanent breakdown of Arctic cooperation. After the 2014 crisis, there was also some decline in Arctic cooperation, but after a few years, the previous level of cooperation was restored and further progress was made. This was interrupted by the current, much more serious situation, so it is expected that this recovery will take more time, but this is unlikely to have an impact on a possible Hungarian observer status.

The most important regional organisation in the region is the Arctic Council, founded in 1996 by eight states,[53] which have coined the term "Arctic state" for themselves.[54] From Hungary's perspective, the most important are the powers of the observer states. Although this status does not imply decision-making competence, as decision-making at all levels of the Council is the exclusive competence of the eight Arctic states (with the involvement of the permanent participants), observer status does give the right to participate in Council meetings and working groups. In the Council's subsidiary bodies,[55] observers may speak, make written statements, submit relevant documents and express their views on issues under discussion.[56]

Considering that the effects of climate change are most visible in the Arctic, which Hungary considers a long-term security threat, Council participation can contribute to obtaining relevant information for the threat assessment. In addition, an important aspect is the establishment of new informal contacts and the fact that, since a large part of the observer states' time in the Council is spent in working groups, where observers can provide financial, technical and other contributions to programs of interest to the Arctic states, the Arctic states will accept the observer state. For many non-Arctic states, becoming an observer is also a recognition of

[52] Atle Staalesen: Nordic Countries Halt All Regional Cooperation with Russia. *Eye on the Arctic,* 07 March 2022; Gloria Dickie: Russian Officials Call Arctic Council Boycott 'Regrettable'. *Reuters,* 04 March 2022.

[53] The founding countries are Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, Finland, Sweden and the United States. In addition to the eight member countries, the organisation has six indigenous permanent participating organisations.

[54] Arctic Council: Declaration on the Establishment of the Arctic Council. Joint Communique of the Governments of the Arctic Countries on the Establishment of the Arctic Council. Ottawa, 1996.

[55] Working Groups, Task Forces, Expert Groups and other bodies set up by the Arctic Council.

[56] Arctic Council: Arctic Council Observers. s. a.

their Arctic interests and their right to assert them.[57] Considering that most of the Hungarian interests identified in the previous section are directly or indirectly related to climate change, this is even more true from a Hungarian perspective, given that a significant part of the Arctic Council's work is devoted to climate change research, environmental protection and the use of sea routes.

Based on interviews[58] on the Arctic Council's website, "Observer Reports"[59] submitted to the Arctic Council and other publicly available sources (e.g. reports from public institutions or statements from politicians),[60] most observer states legitimise their participation in the organisation by the impacts of climate change. Legitimacy may be based on participation in climate change research, but also on the historical link with the region (the Netherlands) or on the protection of economic interests (Italy, the U.K. and Spain). Many states refer to having an independent Arctic strategy (France, Germany, Italy, China, Switzerland and South Korea) or highlight the number of research programs or conferences they have participated in or organised.

4.2. Elements of the special Hungarian campaign – proposal to obtain observer status

Taking the above into account, a special Hungarian campaign can be set up to obtain Hungarian observer status. The main building blocks of this are outlined as follows:

- In the context of *historical argumentation,* while there is minimal Hungarian presence in the last hundred years, the aforementioned Austro–Hungarian "colony" may be a central element of this argumentation.[61]
- While there is no significant Hungarian minority in most of the Arctic States, the *Hungarian diaspora* in Sweden is estimated at 27,000,[62] 348,000 in Canada in the 2016 census, and 1,348,198 in the United States (although only 1,764 of

[57] Liz Bowman: Observers to the Arctic Council and Their Benefits. *The Polar Connection,* 27 July 2017.

[58] Arctic Council: Interview with Arctic Council Observers: The Netherlands, Japan, United Kingdom, Italy, Poland, Spain, Switzerland. Arctic Council, 2020.

[59] Michael Däumer: Germany's 2016 Observer Review Report. *Arctic Council,* 31 May 2016; Arctic Council: *Germany – Observer Review 2021.* Arctic Council: *France – Observer Report 2020*; Didier Ortolland – Olivia Bellemere: France's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016; Francesco Puccio: Italy's 2016 Observer Activities Report. *Arctic Council,* 24 November 2016; Kazuko Shiraishi: Japan's 2016 Observer Activities Report. *Arctic Council,* 16 December 2016; Arctic Council: *Japan – Observer Report 2020*; Arctic Council: *Netherlands – Observer Review 2021*; Yang Xiaoning: China's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016; Linlin Li: The People's Republic of China 2018 Observer Review Report. *Arctic Council,* February 2019; Galen Lee: Singapore's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016; Arctic Council: *Republic of Singapore – Observer Report 2020*; Arctic Council: *Republic of India – Observer Report 2020.*

[60] Ministère de l'Europe et des Affaires étrangères: Strengthening Our Cooperation to Achieve Our Common Goals. *12th Ministerial Meeting of the Arctic Council – Observer Statement,* 20 May 2021; Federal Foreign Office (2013): op. cit.; Sam Tan: What Is the Connection between Singapore and the Arctic Region? *Today,* 24 May 2016; Tae-yul Cho: 2nd Vice Minister's Opening Remarks at the Seoul International Arctic Symposium. *Ministry of Foreign Affairs,* 11 April 2013.

[61] The expedition had a Hungarian supporter in the person of Count Ödön Zichy, and there was also a Hungarian participant, Dr. Gyula Kepes, a doctor on board. See Tamás M. Tarján: A Ferenc József-föld felfedezése. *Rubicon,* 30 August 1873.

[62] The number of Hungarians in diaspora: Denmark – 5,170, Finland – 2,248, Norway – 8,316, Russia – 2,781. See Krisztián Rákóczi et al.: *Nemzetpolitika.* Budapest, Dialóg Campus, 2017. 37.

them live in Alaska).[63] Even if we only include Alaska, there are approximately 400,000 Hungarians living in the Arctic states. On the one hand, this could be an argument for observer status in the Arctic Council, but on the other hand, it is another reason why more attention should be paid to the region.

- The impact of *climate change* on Hungary is also a compelling reason given that the vulnerability of Hungarian water resources to sea level rise makes the country particularly interested in combating climate change. Similar reasoning can be observed for Singapore and the Netherlands, which are also particularly vulnerable to sea level change due to their specific geographical conditions.
- The active involvement prior to the application could be given less emphasis, as there is not much of a Hungarian presence in the Arctic, but the *participation in the Arctic Frontier conference* in 2017 and 2018 mentioned above can be highlighted.
- Hungary has *research cooperation* with several Arctic states, which is worth highlighting. Although not Arctic, but Antarctic research, Arctic research has a long history in the country, and there is still significant Arctic and climate change research going on in the present. In this context, it would be worthwhile to emphasise space research and space cooperation with Finland and Russia, as there are already international examples of space research being highlighted in relation to the Arctic.
- *Economic interests* can also be discussed, most notably in relation to MOL Norge, but the assertion of such interests would be legitimate after the observer status has been granted, rather than being the basis of the Hungarian argument – especially given the explicit emphasis on environmental protection in the organisation.
- Finally, a unique element of this Hungarian campaign could be to emphasise the *Finnish–Hungarian linguistic affinity*. Hungary's closest linguistic relative is Finland, and no other observer country has such an argument or similar ones, which could provide additional legitimacy.

Taking these shortcomings into account, Hungary may be able to develop a legitimate and serious set of arguments to justify its claim to observer status. And the idea is not unrealistic, as countries further south than Hungary and similarly lacking a sea exit have already campaigned successfully.

5. Conclusions

In the shadow of the crises of recent years, the Arctic has received little attention. However, challenges such as climate change, population growth and energy scarcity face a long future, and this foreshadows a growing role for the Arctic. In the long term, this could certainly justify the creation of an independent Hungarian Arctic strategy,

[63] 2020: ACS 5-year Estimated Detailed Table (B04006 – People Reporting Ancestry). *United States Census Bureau*, 2020.

but in the meantime, it would be necessary to define the country's interests and goals in other strategies. This is also supported by the fact that Hungary cooperates with most Arctic states in the fields of economics, research and the military industry. On this basis, Hungary, as a European state, may (or should) soon embark on the path towards the Arctic.

References

1163/2020 (IV. 21.) Government Resolution on the National Security Strategy of Hungary. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001

1393/2021 (VI. 24.) Government Resolution on the National Military Strategy of Hungary. Online: https://defence.hu/news/national-military-strategy-of-hungary.html

2020: ACS 5-year Estimated Detailed Table (B04006 – People Reporting Ancestry). *United States Census Bureau,* 2020. Online: https://data.census.gov/cedsci/table?q=B04006&g=0400000US02&tid=ACSDT5Y2020.B04006

Agrárszektor: Jó ötlet-e a trieszti magyar kikötő? *Agrarszektor.hu,* 24 July 2019. Online: www.agrarszektor.hu/piac/jo-otlet-e-a-trieszti-magyar-kikoto.15533.html

Arctic Council: *Arctic Council Observers.* s. a. Online: https://arctic-council.org/en/about/observers/

Arctic Council: *Declaration on the Establishment of the Arctic Council. Joint Communique of the Governments of the Arctic Countries on the Establishment of the Arctic Council.* Ottawa, 1996. Online: https://oaarchive.arctic-council.org/bitstream/handle/11374/85/EDOCS-1752-v2-ACMMCA00_Ottawa_1996_Founding_Declaration.PDF?sequence=5&isAllowed=y

Arctic Council: *France – Observer Report 2020.* Online: https://oaarchive.arctic-council.org/handle/11374/2718

Arctic Council: *Germany – Observer Review 2021.* Online: https://oaarchive.arctic-council.org/handle/11374/2693

Arctic Council: Interview with Arctic Council Observer: Italy. *Arctic Council,* 11 March 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-italy/

Arctic Council: Interview with Arctic Council Observer: Japan. *Arctic Council,* 03 July 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-japan/

Arctic Council: Interview with Arctic Council Observer: Poland. *Arctic Council,* 30 March 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-poland/

Arctic Council: Interview with Arctic Council Observer: Spain. *Arctic Council,* 11 March 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-spain/

Arctic Council: Interview with Arctic Council Observer: Switzerland. *Arctic Council,* 06 July 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-switzerland/

Arctic Council: Interview with Arctic Council Observer: The Netherlands. *Arctic Council,* 10 August 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-the-netherlands/

Arctic Council: Interview with Arctic Council Observer: United Kingdom. *Arctic Council,* 11 March 2020. Online: https://arctic-council.org/news/interview-with-arctic-council-observer-united-kingdom/

Arctic Council: *Japan – Observer Report 2020.* Online: https://oaarchive.arctic-council.org/handle/11374/2724

Arctic Council: *Netherlands – Observer Review 2021.* Online: https://oaarchive.arctic-council.org/handle/11374/2702

Arctic Council: *Republic of India – Observer Report 2020.* Online: https://oaarchive.arctic-council.org/handle/11374/2721

Arctic Council: *Republic of Singapore – Observer Report 2020.* Online: https://oaarchive.arctic-council.org/handle/11374/2711

Arctic Council: *Spain – Observer Report 2020.* Online: https://oaarchive.arctic-council.org/handle/11374/2710

Arctic Frontiers: Arctic Frontiers 2017 The Arctic in a Global Context. *YouTube,* 25 January 2017. Online: www.youtube.com/watch?v=AWx2yzWm77Y

Arctic Frontiers: Arctic Frontiers Policy 2018. Speaking Truth to Power. Science Based Policy in a Post-Fact World. *YouTube,* 15 June 2018. Online: www.youtube.com/watch?v=p_VIBqrr49k

Baranyai, Gábor: Kanadában képezik a honvédség pilótáit. *Magyar Nemzet,* 24 August 2019. Online: https://magyarnemzet.hu/belfold/2019/08/kanadaban-kepezik-a-honvedseg-pilotait

Bowman, Liz: Observers to the Arctic Council and Their Benefits. *The Polar Connection,* 27 July 2017. Online: https://polarconnection.org/arctic-council-observers-benefits/

Cavcic, Melisa: Norwegian Player Seeks Operatorship as MOL Norge Offloads Two North Sea Discoveries. *Offshore Energy,* 18 April 2022. Online: www.offshore-energy.biz/norwegian-player-seeks-operatorship-as-mol-offloads-two-north-sea-discoveries/

Cho, Tae-yul: 2nd Vice Minister's Opening Remarks at the Seoul International Arctic Symposium. *Ministry of Foreign Affairs,* 11 April 2013. Online: https://bit.ly/3UizRfP

Däumer, Michael: Germany's 2016 Observer Review Report. *Arctic Council,* 31 May 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1874

Dickie, Gloria: Russian Officials Call Arctic Council Boycott 'Regrettable'. *Reuters,* 04 March 2022. Online: www.reuters.com/world/europe/russian-officials-call-arctic-council-boycott-regrettable-2022-03-04/

Edvardsen, Astri: Cold Response 2022: 35,000 Soldiers from 26 Countries in Northern Military Exercise. *High North News,* 18 January 2022, Online: www.highnorthnews.com/en/cold-response-2022-35000-soldiers-26-countries-northern-military-exercise

Fagyos Oázis Kutatócsoport: Hungarian Scientific Program 2005. *Antarctica.hu,* 2005. Online: www.antarctica.hu/antarctica.php?event=100101&id=326&ord=2

Federal Foreign Office: *Germany's Arctic Policy Guidelines. Assume Responsibility, Seize Opportunities.* Berlin, 2013. Online: www.arctic-office.de/fileadmin/user_upload/www.arctic-office.de/PDF_uploads/Germanys_Arctic_policy_guidelines.pdf

Fiar, Sándor – Balázs Nagy: *Olvadó jövő.* Budapest, General Press Kiadó, 2004.
František, Kele – László Fekete: *Jég és föld között. Az Antarktisz (újra)felfedezése.* Dunaszerdahely, Nap Kiadó, 2003.
Galambos, Sándor: A Griff haragja. *Honvéd,* 8 (2022). 36–45.
Gawande, Rajesh: *India's Engagement with Arctic Council.* December 2016. Online: https://oaarchive.arctic-council.org/bitstream/handle/11374/1869/EDOCS-4033-v1-2016-12-16_India_Observer_activity_report.PDF?sequence=1&isAllowed=y
Government of Hungary: Magyarország és Finnország űripari együttműködésről állapodott meg. *Magyarország Kormánya,* 14 September 2021. Online: https://kormany.hu/hirek/szijjarto-peter-magyarorszag-es-finnorszag-uripari-egyuttmukodesrol-allapodott-meg
Horvai, Ferenc: Harmincéves kapcsolataink az Európai Űrügynökséggel. *Aero Magazin,* 17 September 2021. Online: www.aeromagazin.hu/index.php?option=com_k2&view=item&id=1430:harmincéves-kapcsolataink-az-európai-űrügynökséggel&Itemid=115
Hovány-Pap, Melinda – István Háda: Eredményesen zárult a Trident Juncture 2018 gyakorlat. *Honvédelem,* 05 December 2018. Online: https://honvedelem.hu/hirek/hazai-hirek/eredmenyesen-zarult-a-trident-juncture-2018-gyakorlat.html
HVG: Két magyar hegymászó is elérte az Északi-sarkot. *HVG,* 20 April 2004. Online: https://hvg.hu/itthon/0000000000559C2F
Index: Magyarok elsőként a Déli-sarkon. *Index,* 16 January 2005. Online: https://index.hu/sport/2005/01/16/050115dsark/
Joób, Sándor: Első magyarként elérte a Déli-sarkot Rakonczay Gábor. *Index,* 08 January 2019. Online: https://index.hu/sport/extremsport/2019/01/08/rakonczay_gabor_antarktisz_deli-sark_expedicio/
KaliberInfo: 55 millió dollárért vesz Carl Gustaf M4-eseket a Magyar Honvédség. *KaliberInfo,* 08 January 2019. Online: www.kaliberinfo.hu/hirek/55-millio-dollarert-vesz-carl-gustaf-m4-eseket-a-magyar-honvedseg/
Kámánfi, Gábor: Átadták a századik honvédségi Currus Aries buszt. *Honvédelem*, 28 November 2019. Online: https://honvedelem.hu/galeriak/atadtak-a-szazadik-honvedsegi-currus-aries-buszt.html
Kombrink, Henk: Mol Plans to Exit Norway. *Expronews.com,* 10 November 2021. Online: https://expronews.com/company-news/mol-plans-to-exit-norway/
Kovács, András: Szijjártó Péter a trieszti kikötőről: Ezzel Magyarország erősödik. *Origo,* 26 July 2019. Online: www.origo.hu/itthon/20190725-szijjarto-peter-interju.html
Kovács, Ferenc: Aláírták a magyar–orosz űregyezményt. *Index,* 12 February 2022. Online: https://index.hu/techtud/2022/02/12/orban-viktor-oroszorszag-urkutatas/
Lee, Galen: Singapore's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1863
Li, Linlin: The People's Republic of China 2018 Observer Review Report. *Arctic Council,* February 2019. Online: https://oaarchive.arctic-council.org/handle/11374/2251
Mfor.hu: Haderő-fejlesztés Magyarországon: 130 milliárdos hitelt kapunk hozzá. *Mfor.hu,* 17 March 2021. Online: https://mfor.hu/cikkek/makro/hadero-fejlesztes-magyarorszagon-130-milliardos-hitelt-kapunk-hozza.html

Ministère de l'Europe et des Affaires étrangères: Strengthening Our Cooperation to Achieve Our Common Goals. *12th Ministerial Meeting of the Arctic Council – Observer Statement,* 20 May 2021. Online: https://oaarchive.arctic-council.org/bitstream/handle/11374/2677/MMIS12_2021_REYKJAVIK_Observer-Statement_State_France.pdf?sequence=1&isAllowed=y

Ministry for Innovation and Technology: 23/2018 (X. 31.) Parliamentary Resolution on the Second National Climate Change Strategy 2018–2030, looking ahead to 2050. Online: https://mkogy.jogtar.hu/jogszabaly?docid=A18H0023.OGY

Ministry of Defence: Hungary's National Military Strategy. 2012. Online: https://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf

Ministry of Foreign Affairs and International Development: *The Great Challenge of the Arctic. National Roadmap for the Arctic.* Paris, 2016. Online: www.diplomatie.gouv.fr/IMG/pdf/frna_-_eng_-interne_-_prepa_-_17-06-pm-bd-pdf_cle02695b.pdf

Ministry of Foreign Affairs and Trade of Hungary: *Stratégiai partnerségi megállapodások.* s. a. Online: https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/strategiai-partnersegi-megallapodasok

Ministry of Foreign Affairs of Hungary: *Hungary's Foreign Policy after the Hungarian Presidency of the Council of the European Union.* 2011. Online: https://brexit.kormany.hu/admin/download/f/1b/30000/foreign_policy_20111219.pdf

MOL Group: *A MOL sikeresen lezárta az Ithaca Petroleum Norge megvásárlását.* 09 July 2015. Online: https://molgroup.info/hu/befektetoi-kapcsolatok/befektetoi-hirek/a-mol-sikeresen-lezarta-az-ithaca-petroleum-norge-megvasarlasat

MOL Group: *Annual Report 2016.* Online: https://molgroup.info/storage/documents/publications/annual_reports/2016/ar_2016_book_eng_0606.pdf

MTI: Hungary Seeks Closer Ties with Northern Europe, Says Foreign Minister in Norway. *Daily News Hungary,* 25 January 2017. Online: https://dailynewshungary.com/hungary-seeks-closer-ties-northern-europe-says-foreign-minister-norway/

MTI: Magyar kutatók megfejtették, hogyan jegesedhetett el az Antarktisz. *Origo,* 07 October 2021. Online: www.origo.hu/tudomany/20211007—a-klimavaltozas-dinamikajanak-megerteset-is-segitheti-a-magyar-tudosok-uj-modellje.html

Nagy, Attila Károly: Két hónapos jó éjszakát kíván az Antarktiszon áttelelő magyar kutatónő. *Index,* 20 May 2017. Online: https://index.hu/tudomany/2017/05/20/juranyi_zsofia_antarktisz/

Origo: Újra magyar kutatók az Antarktiszon. *Origo,* 10 February 2005. Online: www.origo.hu/tudomany/20050210ujra.html

Ortolland, Didier – Olivia Bellemere: France's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1855

Ott, István Dániel: A Currus Aries 01 többfunkciós moduláris jármű kifejlesztése és feladatai a magyar haderőben I. rész. *Haditechnika,* 54, no. 4 (2020). 58–62. Online: https://doi.org/10.23713/HT.54.4.12

Ott, István Dániel: A Currus Aries 01 többfunkciós moduláris jármű kifejlesztése és feladatai a magyar haderőben III. rész. *Haditechnika,* 54, no. 6 (2020). 58–63. Online: http://doi.org/10.23713/HT.54.6.12

Puccio, Francesco: Italy's 2016 Observer Activities Report. *Arctic Council,* 24 November 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1857
Rákóczi, Krisztián – Viktória Válent – Péter Varga: *Nemzetpolitika.* Budapest, Dialóg Campus, 2017.
Robinson, Jana: Arctic Space Challenge for NATO Emerging from China's Economic and Financial Assertiveness. *Transforming Joint Air and Space Power. The Journal of the JAPCC,* 30 (2020). 35–40. Online: www.japcc.org/articles/arctic-space-challenge-for-nato-emerging-from-chinas-economic-and-financial-assertiveness/
Saab: Gripen roars over Hungary for 15 years. *Saab,* 15 June 2021. Online: www.saab.com/newsroom/stories/2021/march/gripen-roars-over-hungary-for-15-years
Saab: Saab to Deliver Upgrade for Hungarian Gripen Fleet. *Saab,* 12 January 2022. Online: www.saab.com/newsroom/press-releases/2022/saab-to-deliver-upgrade-for-hungarian-gripen-fleet
Shiraishi, Kazuko: Japan's 2016 Observer Activities Report. *Arctic Council,* 16 December 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1868
Staalesen, Atle: Nordic Countries Halt All Regional Cooperation with Russia. *Eye on the Arctic,* 07 March 2022. Online: www.rcinet.ca/eye-on-the-arctic/2022/03/07/nordic-countries-halt-all-regional-cooperation-with-russia/
Strategic Airlift Capability: *The Strategic Airlift Capability (SAC).* s. a. Online: www.sacprogram.org/en/Pages/The Strategic Airlift Capability.aspx
Swedish Armed Forces: *Hungary (HAW).* s. a. Online: www.forsvarsmakten.se/en/activities/current-international-missions/hungary-haw/
Tan, Sam: What Is the Connection between Singapore and the Arctic Region? *Today,* 24 May 2016. Online: www.todayonline.com/commentary/what-connection-between-singapore-and-arctic-region
Tarján, M. Tamás: A Ferenc József-föld felfedezése. *Rubicon,* 30 August 1873. Online: www.rubicon.hu/magyar/oldalak/1873_augusztus_30_a_ferenc_jozsef_fold_felfedezese
Vass, Ábrahám: Hungarian Oil Company MOL expands further in Norway. *Hungary Today,* 24 January 2018. Online: https://hungarytoday.hu/hungarian-oil-company-mol-expands-norway-28505/
Xiaoning, Yang: China's 2016 Observer Activities Report. *Arctic Council,* 01 December 2016. Online: https://oaarchive.arctic-council.org/handle/11374/1860

HADMÉRNÖK
FÓRUM
17. évfolyam (2022) 3. szám 187–206.
DOI: 10.32567/hm.2022.3.12

Zsákai Zsolt[1]

Az emberi térd, csípő és gerinc biomechanikai jellemzői, valamint terhelés hatására létrejött elváltozásainak áttekintő elemzése

3. rész: A lumbalis gerinc biomechanikája

An Overview of the Biomechanical Characteristics of the Human Hip, Knee and Spine, as well as the Changes Caused by Exercise

Part 3: Biomechanics of the Lumbar Spine

„Annak, aki sebész akar lenni, előbb háborúba kell menni."

Hippokratész

Cikksorozatom harmadik részében a deréktáji gerinc biomechanikai elemzését végzem. Irodalmi példákon fogom bemutatni, hogy a megnövekedett terhelés, a katonai szolgálat során a gerincet ért hatások és egyéb tényezők milyen nagy hatással vannak a gerincpanaszok kialakulására. A kiképzéssel és bevetéssel járó megterhelés ellensúlyozására fontosnak tartom a megfelelő stratégia kiépítését preventív szempontok alapján, növelve ezáltal a kezelés hatékonyságának fokát, végeredményként pedig csökkentve a gerincbetegségek kialakulásának kockázatát.

Kulcsszavak: **lumbalis gerinc, biomechanika, degeneratív betegség, porckorongsérv, derékfájdalom**

[1] Főorvos, Borsod-Abaúj-Zemplén Megyei Központi Kórház és Egyetemi Oktató Kórház, e-mail: zsakaizsolt@zsakaizsolt.com

In the third part of my article series, I perform a biomechanical analysis of the lumbar spine. I will use examples from the literature to show what a significant effect increased load, effects on the spine during military service and other factors have on the development of spine complaints. To counterbalance the burden of training and deployment, I consider building a strategy based on appropriate preventive factors to be important, thereby increasing the effectiveness of treatment and ultimately reducing the risk of developing spine diseases.

Keywords: **lumbar spine, biomechanics, degenerative disease, disc herniation, low back pain**

1. Bevezetés

Cikksorozatom harmadik részében az emberi gerinc biomechanikáját, túlterhelésével járó problémakörét vizsgálom. Írásomban képet szeretnék adni gerincünk bonyolultságáról, összetettségéről, be szeretném mutatni, hogy e rendszer túlterhelése – a katonai szolgálat alatti túlterhelést is beleérve – krónikus gerincpanaszok kialakulásához vezet. Kutatásomban az aktív szolgálatot teljesítő állomány mozgásszervi problémáit, azok előfordulását vizsgálva, a nemzetközi irodalmat áttekintve körvonalazódott bennem a téma fontossága. Az anatómiai részletek és az egyes betegségek elemzése nem tartozik e cikk témájába, így ezekre nem térek ki részletesen, azonban érintőlegesen, a könnyebb érthetőség miatt fontos ezeknek a bemutatása is.

2. A gerinc anatómiája

A gerincoszlop *(columna vertebralis)* 33-35 csigolyából álló vázrész, amelyet jellemzően 7 db nyakcsigolya *(vertebrae cervicales),* 12 db hátcsigolya *(vertebrae thoracicae),* 5 ágyéki csigolya *(vertebrae lumbales),* 5 db összecsontosodott keresztcsonti csigolya *(sacrum)* és 4-6 csökevényes farokcsonti csigolya *(vertebrae coccygeae)* alkot. Régiónként eltérő anatómiai jellemzőkkel rendelkeznek, ezek alapján valódi és álcsigolyákra is felosztható. Az utolsó 9-11 csigolya álcsigolya, az első 24 csigolya pedig valódi. A valódi csigolyákon megkülönböztetünk testet *(corpus vertebrae),* íveket *(arcus vertebrae),* amelyek a csigolyalyukakat *(foramen vertebrae)* fogják közre. Tulajdonképpen a csigolyalyukak alkotják a gerinccsatornát *(canalis vertebralis).* A hátulsó tövisnyúlvány *(processus spinosus),* valamint az oldalsó nyúlványok *(processus transversus),* illetve a felfelé és lefelé irányuló, páros ízületi nyúlványok jellegzetes anatómiai részletek, anatómiarégiónként eltérő sajátosságokkal, amelyek részletezése nem szükséges jelen írás tartalma szempontjából.[2]

A csigolyák közti összeköttetéseket kisízületek, szalagok *(syndesmosis),* összecsontosodások *(synostosis)* és rostos porcos összeköttetések *(synchondrosis)* biztosítják. Tanulmányom és kutatásom szempontjából ezen utóbbinak van nagyobb

[2] Szentágothai János – Réthelyi Miklós: *Funkcionális Anatómia 1 kötet*. Budapest, Medicina Kiadó – Semmelweis Kiadó, 1996. 308–313.

jelentősége, mert a gerincpanaszok kialakulásában a synchondrosisok játszanak nagy szerepet, ugyanis ezen összeköttetések a tulajdonképpeni csigolya közti porckorongok *(disci intervertebrales),* amelynek betegségei, különös tekintettel annak sérvesedését *(discus hernia),* akár markáns, az aktív katonai szolgálatot is lehetetlenné tévő tünetegyüttes kialakulásához vezethetnek. A cikk további részében célzottan, a könnyebb érthetőség kedvéért a megfelelő részbe illesztve, még kitérek anatómiai részletekre.

A probléma megértéséhez sokkal jobb megközelítést ad, ha megértjük a gerincünk biomechanikáját, ezért célom a következő részekben ennek részletesebb kifejtése, természetesen szem előtt tartva mindezek lényegi és érthetőségi szempontjait.[3]

3. A gerinc biomechanikája

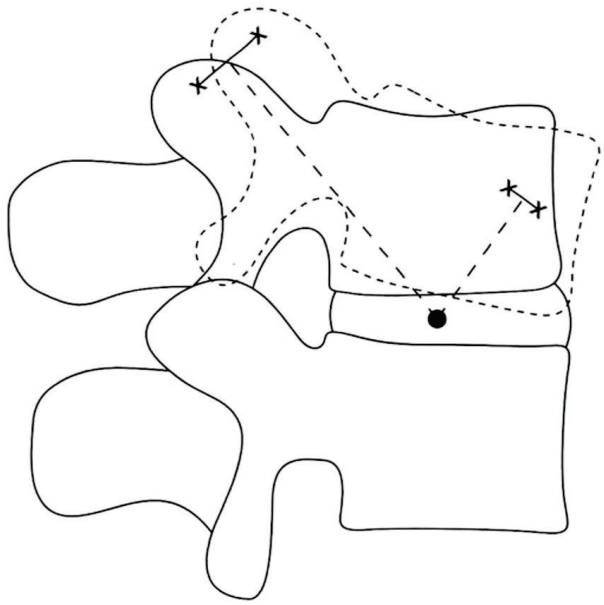
Az emberi mozgás fejlődése során, fokozatosan alakulnak ki a gerinc görbületei. Normál esetben a végső görbületekre a következők jellemzők: a nyaki szakaszon előre irányuló domborulat, a háti szakaszon hátra irányuló, az ágyéki szakasz szintén előre, majd a keresztcsonti szakasz ismét hátra domboruló irányultságot mutat. Az előre domboruló görbületeket *lordosisoknak*, a hátrafelé irányulókat *kyphosisoknak* nevezzük.[4] A görbületek mértéke a *thoracalis kyphosis* esetén megközelítőleg 30 fok, a *lumbalis lordosis* területén 40 fok körüli, a *lumbosacralis* átmenetben pedig 45 fok átlagértéket mutat.[5]

A gerinc mozgásait a csigolyák, a porckorongok, szalagok és izmok biztosítják. Összeségében kijelenthető, hogy a gerinc nagy mozgástartománnyal rendelkezik, azonban síkonként és gerincszakaszonként eltérő hányaddal vesz részt az adott mozgás kialakításában. Főbb mozgásirányai az előre- és hátrahajlás, oldalirányú hajlás, valamint a csavarodás *(torsio)*.[6] A nyaki és ágyéki szakasz jelentős előrehajlást enged, míg a háti szakasz keveset. Hátrahajlásnál a nyaki és ágyéki rész kezdeti része vesz részt leginkább ebben a mozgásban, a háti szakaszon a csigolyanyúlványok összetorlódása miatt ez a mozgás jelentősen kisebb mértékű. Az előre- és hátrahajlás során a rotációs központ a porckorong középpontjának területére esik[7] (1. ábra).

Közelebbről megvizsgálva azonban az előre- és hátrahajlás tulajdonképpen az elemi mozgásszegmentumot alkotó felső *(cranialis)* csigolya rotatiója és hátra vagy előre elcsúszása a szegmentumot alkotó alsó *(caudalis)* csigolyához képest. Az elcsúszás mértéke egészséges, degeneratív elváltozásokat nem elszenvedő szegmentum esetén körülbelül 2 mm.[8] Természetesen ez az elcsúszó effektus a forgásközpontot a centrumból kissé a szegmentumot alkotó alsó csigolya felé helyezi át. Frobin és munkatársai munkájukban mérték meg új, pontosabb módszerrel az elcsúszás mértékét. A mérés

[3] Szentágothai–Réthelyi (1996): i. m. 313–316.
[4] Szentágothai–Réthelyi (1996): i. m. 318–320.
[5] Szendrői Miklós (szerk.): *Ortopédia*. Budapest, Semmelweis Kiadó, 2005. 216.
[6] Paul Brinckmann – Wolfgang Frobin – Gunnar Leivseth: *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002. 105.
[7] Brinckmann–Frobin–Leivseth (2002): i. m. 105.
[8] Brinckmann–Frobin–Leivseth (2002): i. m. 105.

újdonsága az volt, hogy a szomszédos csigolyák testének középpontját vették alapul.[9] Mintegy 2%-os eltérést találtak, és azt állapították meg, hogy ez a csigolyatest méreteiből vonatkoztatva kifejezhető mm-ben is. Tehát egy 35 mm-es csigolya esetén 0,7 mm-nek adódik ez az érték, ami nagymértékű pontosságra engedett következtetést a mérések során.[10]



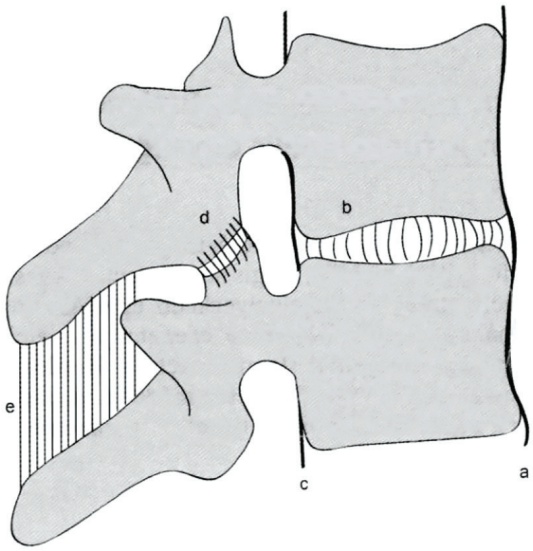
1. ábra: A gerinc rotációs központja előrehajlás esetén
Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 105.

Megjegyzés: Előrehajlás során az elemi mozgásszegmentum rotatios központja megközelítőleg a porckorong középpontjába esik.

Oldalirányú hajlás során szintén a fent említett szakaszok jellemzői érvényesülnek. A gerinc tengelyirányú csavarodása mintegy 45 fokos. Ebben a nyaki gerinc vesz részt leginkább, majd a háti gerinc, az ágyéki csigolyák esetén pedig nem beszélhetünk effektív torsióról.[11]

Fontos fogalom az elemi mozgásszegmentum fogalma, amelyet ismernünk kell a gerinc biomechanikai sajátosságainak szempontjából. Elemi mozgásszegmentumnak nevezzük a gerinc alapvető funkcionális egységét, amelyet a 2. ábra szemléltet.

[9] Wolfgang Frobin et al.: Precision Measurement of Segmental Motion from Flexion-Extension Radiographs of the Lumbar Spine. *Clinical Biomechanics,* 11. (1996), 8. 457–465.
[10] Brinckmann–Frobin–Leivseth (2002): i. m. 106.
[11] Szentágothai–Réthelyi (1996): i. m. 318–320.

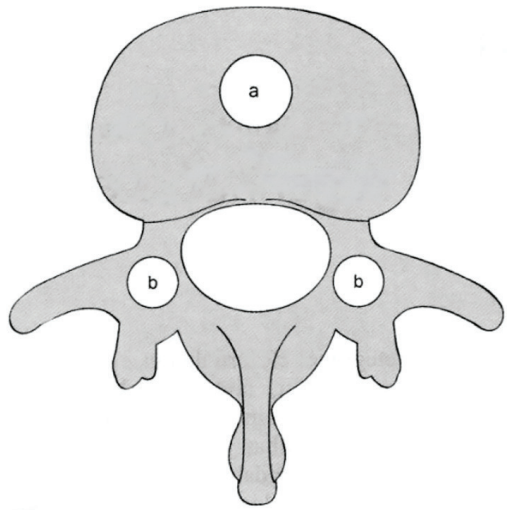


2. ábra: A gerinc elemi mozgásszegmentuma
Forrás: Szendrői (2005): i. m. 214.

Megjegyzés: a) elülső hosszanti szalag (ligamentum longitudinale anterius); b) porckorong (discus intervertebralis); c) hátulsó hosszanti szalag (ligamentum longitudinale posterius); d) kisízület; e) tüskenyúlvány közti szalag (ligamentum intersinosum)

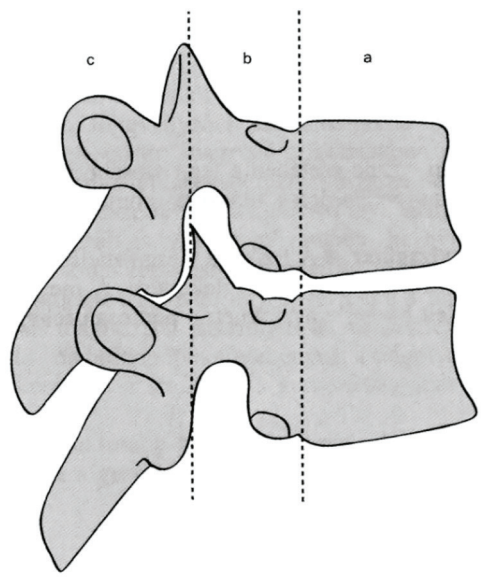
A gerinc fontos feladatait úgy kell elvégezze, hogy stabilitása, merevsége mellett a hajlékonyságát és rugalmasságát is megőrizze. Ezt a kettős és egymásnak ellentmondó biomechanikai tényt az elemi mozgásszegmentumok és a három oszlop elméletével összefoglalt jelenség révén tudja elérni. Az elemi mozgásszegmentum két egymást követő csigolyából és az azokat összekötő minden anatómiai alkotóból áll (2. ábra). A három oszlop elméletet horizontális (3. ábra) és sagittalis (4. ábra) síkra vonatkoztatva kell értelmezni. Horizontális síkban az elülső oszlopot a csigolyatestek, discusok és szalagok, míg a hátulsó oszlopokat a kisízületek alkotják. Sagittalis síkban a csigolyatest elülső kétharmada a discus egy része, valamint a *ligamentum longitudinale anterius* alkotja. A csigolyatest hátulsó harmada, a *ligamentum longitudinale posterius* és a pediculusok egy része a középső, a pediculusok hátulsó része, a kisízületek, valamint a csigolyanyúlványok pedig a hátulsó oszlopot alkotják. Az elemi mozgásszegmentum vizsgálatakor kitűnik, hogy a két csigolya kétkarú emelőnek fogható fel, ahol az alátámasztási pont a kisízületeknél helyezkedik el. Ez a kétkarú emelő elv segíti a csigolyákra ható nyomási erőt aktív és passzív módon is eliminálni.[12]

[12] Szendrői (2005): i. m. 214–215.



3. ábra: A horizontális síkra vetített 3 oszlop elmélet
Forrás: Szendrői (2005): i. m. 214.

Megjegyzés: a) elülső oszlop; b) hátulsó oszlop



4. ábra: A sagittális síkra vetített 3 oszlop elmélet
Forrás: Szendrői (2005): i. m. 217.

Megjegyzés: a) elülső oszlop; b) középső oszlop; c) hátulsó oszlop

A teljesség igénye nélkül a gerincoszlop feladatait, annak mechanikai szerepét a következőképpen lehetne jellemezni:

- A test stabilitásának biztosítása.
- A test egyensúlyának biztosítása.
- A test központi vázát alkotja.
- A központi idegrendszer védelmét biztosítja.
- A koponya tartása, térbeli orientációjának biztosítása.
- A törzs térbeli hajlékonyságának biztosítása.
- Részt vesz a bordakosár alkotásában.
- Kapcsolatot biztosít a vállövvel.
- Kapcsolatot biztosít a medenceövvel.

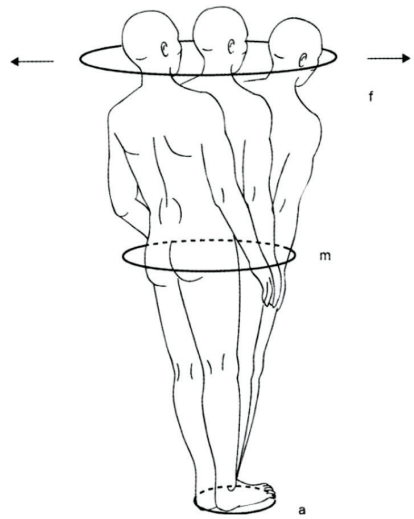
A gerinc biomechanikája szempontjából a stabilitás és egyensúly-biztosítás problémájára érdemes megfelelő mértékben kitérni, hiszen e fogalmak mögé rendezett funkció – illetve annak eltérése, főleg fokozott terhelés esetén – jelentheti a tünetek akár korai kialakulását és a panaszok megjelenését.

A gerinc stabilitása szintén az elemi mozgásszegmentum vizsgálatával határozható meg: az ezt alkotó, két szomszédos csigolya egymáshoz képest, a fiziológiás értékeken túl nem elmozdítható. Ebből könnyen következhetne, hogy instabilitáson pedig ennek az ellenkezőjét lehet érteni, azaz, hogy az elemi mozgásszegmentumot alkotó két csigolya egymáshoz képest, a fiziológiástól eltérő mértékben, kórosan elmozdítható. Az instabilitás fogalmát azonban árnyalja a *potenciális instabilitás* meghatározása, amelynek jelentése az, hogy bár objektív, dinamikus vizsgálómódszerekkel nem kimutatható az aktuális instabilitás, azonban jelen van olyan betegség vagy trauma következtében kialakult elváltozás vagy fejlődési rendellenesség, amely magában hordozza az abnormális elmozdulás veszélyét.[13]

Sajnos a potenciális instabilitás okainak nagy része akár fedve is maradhat, pedig azoknak diagnosztizálása esetén preventív intézkedésekkel, odafigyeléssel a panaszok kialakulását is elkerülhetjük, vagy elodázhatjuk. Különösen igaz ez nagyobb megterhelés fennállása esetén, így a szolgálatot teljesítő, aktív állományban lévő katonák esetében is.

A másik fontos funkciója gerincünknek a test egyensúlyi helyzetének biztosítása. Egyensúlyi helyzet akkor adódik, ha a gravitációs tengely és a súlypont vetülete az alátámasztási felszín közepén marad, egy tengelyen elhelyezkedve. Testünk jellemzője, hogy minden irányban ugyanolyan amplitúdójú mozgásokkal próbálja fenntartani az egyensúlyi helyzetét, mindezt pedig minimális izommunkával teszi. Álló helyzetben az alátámasztási pontot lábaink alkotják, és ettől a medence és fej azonos amplitúdójú, a tér minden irányába mutató mozgást végez (5. ábra), amelyet a térben egy szelvényként tudjuk értelmezni: ez a gazdaságos munka kúpja.

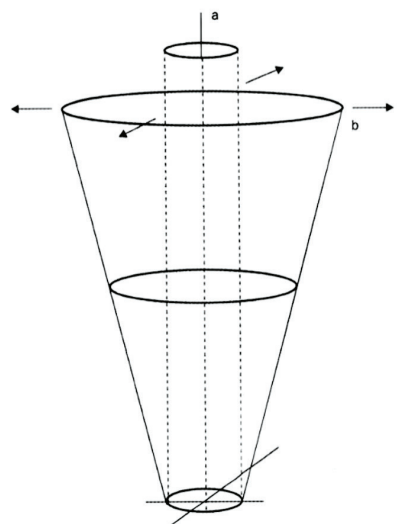
[13] Szendrői (2005): i. m. 216.



5. ábra: A test egyensúlyi helyzete
Forrás: Szendrői (2005): i. m. 217.

Megjegyzés: a) alátámasztási terület; m) a medence mozgássíkja; f) a fej mozgássíkja

Az egyensúly fenntartásához szükséges maximális izommunka felhasználásával kialakított térbeli szelvényt a maximális munka kúpjaként definiálhatjuk[14] (6. ábra).



6. ábra: Az egyensúlyi helyzetben megjelenő mozgáskúpok
Forrás: Szendrői (2005): i. m. 217.

Megjegyzés: a) gazdaságos munka síkja; b) maximális munka síkja

[14] Szendrői (2005): i. m. 216–217.

Ekkor a gravitációs tengelyen elhelyezkedő súlypont nem esik kívül az alátámasztási felszín területén. Ha a gravitációs tengelyre illeszkedő súlypont kívül esik az alátámasztási felszín területén, akkor nagyobb izomerőre, ezáltal pedig nagyobb energiára is van szükség az egyensúlyi helyzet fenntartásához.

Az eddig írottakból is tapasztalhattuk, hogy a gerinc biomechanikája rendkívül összetett és bonyolult összefüggésekből és jellemzőkből álló tulajdonsága központi támasztórendszerünknek. Természetesen a mozgás mellett a terhelési viszonyok is fontos hatáskülönbségek, amelyek a gerincünket érhetik, hiszen a mindennapi életvitel során, különösképpen pedig a nagy fizikai megterhelések esetén gerincünkre is nagyobb terhelés jut. A katonai szolgálat során fellépő megnövekedett terhelés túlterhelés formájában jelenik meg, a megnövekedett izomtevékenység, mozgásfokozódás és a gerincet érő erőbehatások miatt. A test súlyának cipelése önmagában is hatással van mozgásszervrendszerünkre, azonban a plusz tömeg, mint például a fegyver, málha, testpáncél, öltözet viselése ezt a hatást felerősíti, és túlterheléses betegségek kialakulására is hajlamosít. Ezt a túlterhelést a gerincoszlop derékszakasza biomechanikájának összefüggésében többen is vizsgálták.

A tömeg emelésekor fellépő erők, amelyek tulajdonképpen az emelés közbeni egyensúlyi helyzetet biztosítják, és kiegyensúlyozzák a gravitációs erőt, a gerinc két oldalán elhelyezkedő izmok erejének összeadódásából tevődnek össze.[15] A gerincre ható erő az aktuális testhelyzettől is függ, az erre vonatkozó összefüggéseket a későbbiekben tárgyaljuk. Természetesen az egyensúlyi helyzetet adó, összeadódó izomerő nemcsak a tartott tömeg súlyát, hanem a test súlyát is ellensúlyozza. Ha ugyanezt vizsgáljuk nemcsak tartott, hanem gyorsulással mozgatott esetben, akkor azt tapasztaljuk – és a vizsgálatok eredménye is ezt mutatta –, hogy a statikus helyzetet összehasonlítva a dinamikus helyzettel, ezen utóbbinál nagyobb erő szükségeltetik az egyensúlyi helyzet megtartásához, következésképpen a gerincre is nagyobb erő hat.[16]

Itt szeretnék megemlíteni egy kevésbé egyértelmű, de annál érdekesebb összefüggést mutató tényt: az emelő munkavégzés közben megnövekedett hasűri nyomás tényét. A hasi izmok *(musculus obliquus internus abdominis, musculus obliquus externus abdominis, musculus transversus abdominis)* működése biztosítják a hasüregben megjelenő nyomás emelkedését. Ennek eredményeként a lumbalis gerincszakasz stabilizációját feltételezzük, bár vannak olyan elméletek, amelyek mintegy melléktermékként megjelenő jelenségnek írják le a megnövekedett hasi nyomást.[17] Érdekesség, hogy számos nagy erőkifejtéssel járó sport vagy tevékenység közben elterjedt bizonyos széles övek használata, noha az erre vonatkozó vizsgálatok bebizonyították, hogy ezek sem az izomerőre, sem a lumbalis gerincsérülés elleni védelemre szignifikánsan nem hatnak.[18] Használatuk értelme abban rejlik, hogy legalább a törzs flexiójának

[15] Brinckmann–Frobin–Leivseth (2002): i. m. 106–108.
[16] T. P. J. Leskinen et al.: A Dynamic Analysis of Spinal Compression with Different Lifting Techniques. *Ergonomics,* 26. (1983a), 6. 595–604.; T. P. J. Leskinen et al.: The Effect of Innertial Factors on Spinal Stress When Lifting. *Engineering in Medicine,* 12. (1983b), 2. 87–89.
[17] Brinckmann–Frobin–Leivseth (2002): i. m. 108–110.
[18] J. R. Reyna et al.: The Effect of Lumbar Belts on Isolated Lumbar Muscle. Strength and Dynamic Capacity. *Spine,* 20. (1995), 1. 68–73.

lehetőségét csökkentik mozgásbeszűkülést okozó hatásukkal, ami pedig valóban csökkenti a sérülések kockázatát.[19]

Természetesen az utóbbi három fejezetben tárgyalt összefüggéseket tovább lehet finomítani, és ennek megfelelően érdekes gyakorlati következtetéseket lehet levonni. Eddig egy eredő izomerő esetén vizsgáltuk annak hatását, azonban, ha tetszőleges testtartás és tetszőleges külső erővektor hatását vesszük alapul, akkor nyilvánvaló, hogy nem ezen egy eredő izom működésével lehet megfelelően modellezni a szituációt. Több vizsgálat is történt nyolc,[20] vagy akár tíz[21] izom külön vonatkozásában is, beleépítve többek közt a testtömeg, nem, alkat szerepét is modelljeikbe.[22] Ezek a vizsgálatok megfelelő javaslatok irányába mutattak, elkerülendő a lumbalis gerinc túlterhelődését. Dieen munkája például azt az érdekes eredményt hozta, hogy a gerinc túlterhelése nem feltétlenül következik be nagyobb mértékben akkor, ha a sagittalistól eltérő, aszimmetrikus testhelyzetben (például oldalirányban hajlott törzzsel) történik az emelés, mert az obliqus izomzatnak nagyobb erőkarja van, mint a hátizmoknak, ezért ez csökkenti a gerincre ható erőket, így annak terhelődését.[23]

Általános elvként mutatkozik, hogy minden testhelyzetben a lumbalis gerinc terheltsége a mindenkori emelt vagy hordozott tömegtől függ. Ebből az következik, hogy a túlterhelés elkerülését vagy a súly nagyságának megválasztásával, vagy pedig a gerinc és az emelt tömeg gravitációs centrumának közelítésével tudjuk megoldani. Ezért nagyobb súly emelésekor, amennyire lehet a tömeg a gerinchez legközelebbi tartásával kell megoldani, sőt kissé hátrahajlott törzzsel ugyanezt kivitelezve tovább csökkenthető a gerincre ható megterhelés. Számos szerző vizsgálatát összehasonlítva juthatunk erre a következtetésre. A vizsgálatok során az egyenes hát/hajlított térd, előredöntött törzs/kissé hajlított térd és a teljesen előrehajolt törzs/egyenes térd vonatkozásában végeztek méréseket.[24] A háton való teherhordozás az erőkart 10 cm alá csökkenti, ami szintén csökkenti gerincre ható erőt, és igaz ez a ventralis (has felőli) emeléssel összehasonlítva is. A vizsgálatokból kiderült, hogy a deréktájéki gerincszakaszon fellépő nyíró erők nagyobbak előrehajlott testhelyzetben, mint nyújtott törzs esetén, azonban általános szabályszerűségként lehet kijelenteni, hogy az erőkar lecsökkentése esetén (azaz, ha a tárgyat közel emeljük a törzsünkhöz), a derékra ható erők is lecsökkennek. A nyújtott törzzsel való emeléshez általában hajlított helyzetű térdekkel való mozgásmintával járulunk hozzá. A vizsgálatokból kiderült, hogy az emelő saját súlya és az emelni kívánt tömeg összefüggésében is

[19] K. Miyamoto et al.: Effects of Abdominal Belts on Intra-Abdominal Pressure, Intra-Muscular Pressure in the Erector Spinae Muscles and Myoelectrical Activities of Trunk Muscles. *Clinical Biomechanics,* 14. (1999), 2. 79–87.

[20] Matthias Jäger: *Biomechanisches Modell des Menschen zur Analyse und Beurteilung der Belastung der Wirbelsaeule bei der Handhabung von Lasten*. Düsserdorf, VDI Verlag, 1987. Fortschritt-Bericht 17/33. Matthias Jäger – A. Luttmann: Entwicklung eines biomechanischen Modells zur Bestimmung der Belastung der Wirbelsäule. *Biomedizinische Technik,* 38. (1993), 393–394.

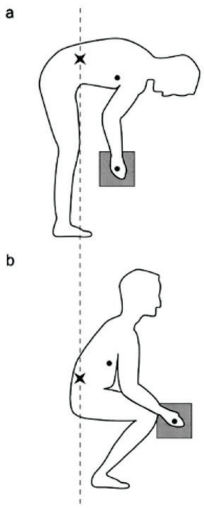
[21] J. C. Bean – D. B. Chaffin – A. B. Schultz: Biomechanical Model Calculation of Muscle Contraction Forces. A Double Linear Programming Method. *Journal of Biomechanics,* 21. (1988), 1. 59–66.

[22] S. M. McGill – R. L. Hughson – K. Parks: Changes in Lumbar Lordosis Modify the Role of the Extensor Muscles. Clinical Biomechanics, 15. (2000), 10. 777–780.

[23] J. H. Dieen – I. Kingma: Total Trunk Muscle Force and Spinal Compression are Lower in Asymmetric Moments as Compared to Pure Extension Moments. *Journal of Biomechanics,* 32. (1999), 7. 681–687.

[24] Richard C. Nelson – Chauncey A. Morehouse (szerk.): *Biomechanics IV*. Baltimore, Maryland, Macmillan Education, 1974. 37–43.

lehet megállapításokat tenni. A saját test tömegének erőkarja és az emelni kívánt test erőkarja közt ugyanis testtartástól függően fordított viszonyulás van. A testtömegerőkar előrehajlott törzsnél nagyobb, míg a tárgy súlyának erőkarja a gerinchez viszonyítva hajlított térd és egyenes törzs mellett nagyobb[25] (7. ábra).



7. ábra: A test és az emelni kívánt tömeg súlypontjának viszonyulása
Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 116.

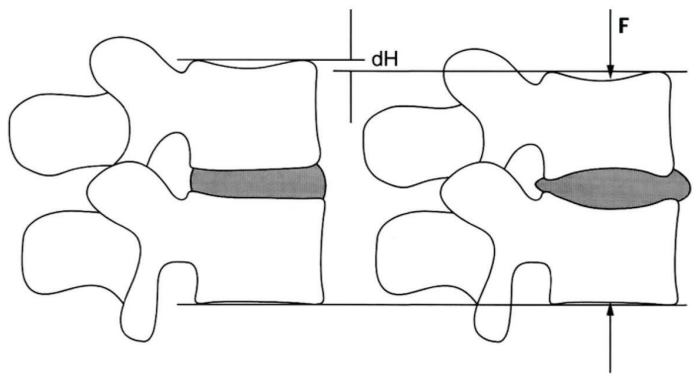
Hajlított törzs esetén a külső tömeg gravitációs erejének erőkarja kisebb (a), mint hajlított térd és egyenes törzs esetén (b), valamint a törzs gravitációs erejének erőkarja hajlított törzs esetén nagyobb (a), egyenes törzs és hajlított térd esetén kisebb (b).

Ebből az az érdekes megállapítás tehető, hogy azokban az esetekben, amikor a testsúly kis mértékű, vagy nagy az emelni kívánt tömeg, akkor az előrehajolt testtartás, míg nagy testtömeg és könnyű súly esetén az egyenes törzs hajlított térd a kíméletesebb megoldás. Sajnos nem lehet általános érvényű javaslatot tenni annak érdekében, hogy mindig a helyes testtartással történjen az emelés. Idősebb korban a hajlított térdel való emeléskor a térdre eső nagyobb terhelés miatt a nem megfelelő porcviszonyok, illetve akár a porckopás jelentős panaszokat tud az ízületben okozni. Arról nem is beszélve, hogy rendszeres hajlított térdből végzett ütemes, ismétlődő fizikai munkavégzés során a szervezet energiatartalékának kimerülésével is számolni kell.[26]

A gerincünk vonatkozásában van még egy nagyon fontos rész, amiről beszélni kell akkor, ha központi támasztórendszerünk funkcióját meg kívánjuk érteni. A gerincbetegségek kialakulásának egy részéért ugyanis a porckorongok megbetegedése felelős, illetve ennek a következtében kialakult egyéb elváltozások. Ez abból a biomechanikai sajátosságból következik, hogy nyomás alatt a porckorongok és a csigolya teste

[25] Brinckmann–Frobin–Leivseth (2002): i. m. 116.
[26] Brinckmann–Frobin–Leivseth (2002): i. m. 113–116.

deformálódik (8. ábra). Következésképpen a csigolyatest véglemezei a test belseje felé, míg a porckorongok a korong síkjából kifelé irányulva nyomódnak. A csigolyatest zárólemezek benyomulásának mértéke, anélkül, hogy törés alakuljon ki, körülbelül 0,5 mm.[27] Ennél nagyobb bedomborodás már a törés kockázatával jár. A porckorong kitüremkedése pedig komoly tüneteket okozhat különösen akkor, ha az ideg nyomás alá kerül az anatómiai csatornájában, amelyben elhagyja a gerincoszlop ezen részét. Érdemes megjegyezni, hogy a kiboltosulás mértéke nagyban függ a lumbalis lordosis mértékétől és a törzs hajlított vagy egyenes helyzetétől. Ennek megfelelően nyújtott törzs mellett a hátulsó kiboltosulás, míg hajlított törzs mellett az elülső a nagyobb mértékű.[28]



8. ábra: A nyomás alatt lévő csigolya és porckorong deformálódása
Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 117.

Megjegyzés: F: nyomóerő; dH: a deformáció mértékéből adódó magasságvesztés nagysága

Porckorongunk nagyon érdekes szerepet tölt be a csigolyák közt elhelyezkedve. Fő feladata, hogy a nyomóerőket egyenletesen vigye át a csigolyára. Ezt meg is teszi egészséges szöveti viszonyok közt, vagy csekély degeneráció esetén, azonban előrehaladott degeneratív folyamatoknál ez az egyenletesség megborul, és oldalra, előre vagy hátra hajlás során a csigolyák véglemezénél, az egymáshoz közelítő részeken megnő az ide eső terhelés és nyomás[29] (9. ábra).

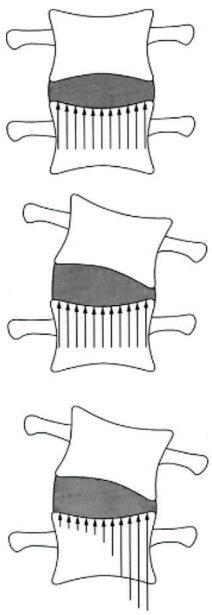
A porckorongban lévő nyomás kiszámítható, és ezt már az 1960-ban meghatározta Nachemson. Az általa javasolt képlet a $p = 1.5 \times F/A$, ahol az F nyomóerő,

[27] Paul Brinckmann et al.: Deformation of the Vertebral End-Plate under Axial Loading of the Spine. *Spine,* 8. (1983), 8. 851–856.; Paul Brinckmann – Manfred Horst: The Influence of Vertebral Body Fractures, Intradiscal Injection, and Partial Discectomy, on the Radial Bulge and Height of Human Lumbar Discs. *Spine,* 10. (1985), 2. 138–145.

[28] Paul Brinckmann – R. W. Porter: A Laboratory Model of Lumbar Disc Protrusion. Fissure and Fragment. *Spine,* 19. (1994), 2. 228–235.

[29] Manfred Horst – Paul Brickmann: Measurement of the Distribution of Axial Stress on the End-Plate of the Vertebral Body. *Spine,* 6. (1981), 3. 217–232.

az A pedig a discus keresztmetszeti területe.[30] Az arányossági faktor kortól, anatómiai elhelyezkedéstől, illetve a degeneráció mértékétől függ. Anatómia szempontból az *intervertebralis discus* (porckorong) két részből áll: a belső, folyékonyabb, *nucleus pulposus* és a külső kötőszövetes *anulus fibrosus* rétegéből és ez az anatómia szerkezet biztosítja a rá jellemző, itt is taglalt biomechanikát.

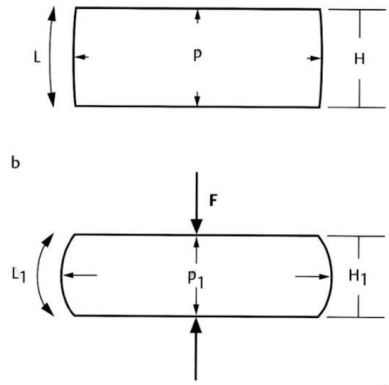


9. ábra: Nyomáseloszlás sematikus ábrázolása
Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 118.

A nyomáseloszlás sematikus ábrázolásán látható, hogy a állandónak tekinthető normál állapotú vagy kevésbé degenerált elemi mozgásszegmentum esetén előre hajlás (felső képrész), vagy akár oldalra hajlás esetén is (középső képrész), míg jelentős nyomáseltolódás következik be súlyosan degenerált esetben (alsó képrész).

Fontos tulajdonsága porckorongunknak, hogy vizet képes megkötni diffuzió útján. Éjszakánként, amikor a gerincre és így a porckorongra nem esik terhelés, akkor víz diffundál a *nucleus pulposusba,* ezáltal a porckorong magassága növekszik. Terheléskor a nyomás hatására a víz eltávozik a discusokból, ezáltal magasságuk csökken, kidomborodásuk fokozódik, és bennük a nyomás nő, aminek segítségével ellensúlyozza az egyenletben is szereplő változásokat (10. ábra).

[30] Alf Nachemson: Lumbar Intradiscal Pressure. Experimental Studies on Post-Mortem Material. *Acta Orthopedica Scandinavica,* 31. (1960), Suppl. 43. 1–104.



10. ábra: Sematikus modell a terhelés következtében fellépő porckorongváltozásokra
Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 88.

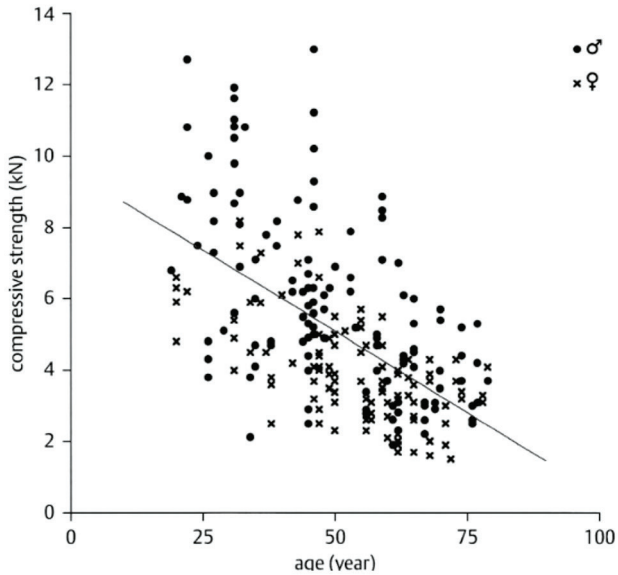
Megjegyzés: L: a porckorong membránjának hossza nem terhelt esetben; L_1: a porckorong membránjának hossza terhelt esetben; F: nyomóerő; H: a porckorong magassága nem terhelt esetben; H_1: a porckorong magassága terhelt esetben; p: a porckorongon belüli nyomás nem terhelt esetben; p_1: a porckorongon belüli nyomás terhelt esetben

Az összenyomódás során a porckorong a várhatónál kisebb mértékben boltosul ki. A várttól elmaradt különbség az *anulus fibrosus* külső rétegének megfeszülése miatt adódik. A terhelés hatására fellépő nyomás, körkörösen, minden irányba hatva okoz feszességet a discus rétegeiben. A csigolyatestek véglemezének területe – ahol a porckorong érintkezik a csigolyával – nagyobb, mint a nem érintkező terület, amelyek a discusok oldalán körkörösen helyezkednek el. A nyomás tartja fel tulajdonképpen a csigolyák közti távolságot, ezáltal csökkentve a kiboltosulás mértékét is.[31] Ez a modell jól szemlélteti, hogy minden olyan változás, amely ezen integritást megbontja – mint a csigolyatest törése, discus hernializálódása, egyes sebészeti beavatkozások –, egyben megváltoztatja porckorongunk működését is, ami pedig a panaszok kialakulásában meghatározó lehet.[32]

A csigolyatest nyomószilárdsága egy másik fontos fogalom, amely a gerinc biomechanikájának megértése szempontjából elengedhetetlen. Vizsgálatok szerint a deréktájéki csigolyák nyomószilárdsága 2 kN és 12 kN között mozog.[33] A szakítószilárdság jellemzésében szerepet játszik a trabecularis csont állományának jellegzetessége is. Vizsgálatok azt mutatták ki – nem meglepő módon –, hogy trabecularis csont állapota korfüggő, és 20-30 éves kor között éri el a maximumát[34] (11. ábra). A csigolya csontszerkezeti minősége szignifikáns nemi különbséget nem mutat, azonban vizsgálatok megállapították, hogy a csigolyák a nemek közt fellelhető, méretbeli különbségéből adódóan – ami férfiban és nőben különböző – megjelenik eltérés a mérésekben. Adott életkorban a nők esetén csökkentebb a csigolyák nyomószilárdsága,

[31] Brinckmann–Frobin–Leivseth (2002): i. m. 119–120.
[32] Paul Brinckmann – Henk Grootenboer: Change of Disc Height, Radial Disc Bulge and Intradiscal Pressure from Discectomy. An In Vitro Investigation on Human Lumbar Disc. *Spine,* 16. (1991), 6. 641–646.
[33] Brinckmann–Frobin–Leivseth (2002): i. m. 121.
[34] D. Felsenberg et al.: Quantitative computertomographische Knochenmineralgehalts Bestimmung. *Fortschr Röntgenstr,* 148. (1988). 431–436.

azonban ez hangsúlyozottan nem nemi összefüggés, hanem másodlagosan, alaki összefüggés miatt tapasztalható.[35]



11. ábra: A nyomószilárdság eloszlása életkor szerint

Forrás: Brinckmann–Frobin–Leivseth (2002): i. m. 88.

Megjegyzés: Az adatok a TH_{12}-L_5 mozgásszegmentum vizsgálatából adódnak. A férfiak értékeit pont, a nőkét x jelzi. Látható, hogy az évek előrehaladtával a nyomószilárdság mértéke csökken, valamint az is kitűnik, hogy a nőknél jellemzőbb módon. Más tanulmányból tudjuk, hogy ez a csökkenés a csont denzitásmértékével van összefüggésben.[36] *A függőleges tengely: nyomóerő KN-ban kifejezve; vízszintes tengely: kor években kifejezve.*

Nyilvánvaló, hogy e bonyolult rendszert megváltoztató minden tényező – mint például az ismétlődő traumatikus hatások, a túlterhelés, törés – panaszok kialakulását okozza. A probléma bonyolultságát fokozza, hogy sok esetben a gerincnél kialakult degeneratív elváltozás nem jár markáns tünetekkel, valamint ennek az ellenkezője is igaz, azaz jelentős panaszok hátterében sem áll egyértelmű, nagymértékű elváltozás. Ha figyelembe vesszük a fájdalom szubjektív voltát, akkor valóban nehéz is megítélni és okot keresni bizonyos esetekben. Az nyilvánvalónak tűnik, hogy nagy teher mozgatása, bizonyos testhelyzetekben végzett munka, ismétlődő, krónikus terhelés nagyobb valószínűséggel alakít ki derékpanaszokat.[37] Az is evidenciának tűnik, hogy a lelki háttér, tehát a biomechanikai faktorokon kívül eső pszichológiai tényező is derékpanaszokat okozhat egyeseknél.[38] Látható, hogy a derékpanaszok fellépte esetén komplex, nem csak biomechanikai értelmezésben lehet és kell vizsgálódni. Jelen írás

[35] Brinckmann–Frobin–Leivseth (2002): i. m. 123.
[36] Paul Brinckmann – M. Biggemann – D. Hilweg: Prediction of the Compressive Strength of Human Lumbar Vertebrae. *Clinical Biomechanics,* 4. (1989), Suppl. 2. 1–27.
[37] Brinckmann–Frobin–Leivseth (2002): i. m. 125.
[38] Brinckmann–Frobin–Leivseth (2002): i. m. 125.

keretei közé nem fér bele a biomechanikai hatásoktól eltérő, más tényezők részletes elemzése, komplex vizsgálata, azonban említésüket érdemesre méltónak gondolom.

Véleményem szerint a téma fontossága komplex elemzést igényel, ezt mutatja a nemzetközi irodalomban fellelhető vizsgálatok szép száma is.

Bader és munkatársai munkájukban kimutatták, hogy az USA aktív katonai állományában az egyik leggyakoribb mozgásszervi panasz a gerincszakasz alsó részének, azaz a deréktájéki gerincnek a fájdalma. Az incidenciát 40,5/1000 személy/év-nek mérték.[39]

Koreerat és munkatársa írásából kiderül, hogy a Security Force Assistance Brigade tagjai közt a deréktájéki gerinc sérüléseinek prevalentiája bevetés előtt, alatt és után vizsgálva is vezető értéket mutatott.[40]

Thoolen és szerzőtársa az F-16-os pilóták esetén vizsgálták a nyaki és háti gerincnél jelentkező fájdalmak megjelenését, és azt találták, hogy 2007–2014 között nőtt az incidencia. Ennek okát az életkorban, a repülési idő növekedésében, az éjjellátó szemüveg megnövekedett idejű használatában látták.[41]

Orsello és munkatársai helikopterpilótáknál vizsgálták a testmagasság és a repülés közben fellépő gerincfájdalom közti összefüggést. Azt találták, hogy nagyobb testmagasság esetén szignifikánsan megnövekedett mértékben fordulnak elő deréktájéki fájdalmak. Tanulmányuk szerint minden 1 inches növekedés (1 inch = 2,34 cm) 9,3%-kal növeli a panaszok kialakulásának valószínűségét.[42]

Nagai és szerzőtársai vizsgálatában a korábban már derékfájdalom tünetét mutató, valamint a tünet nélküli helikopterpilóták vizsgálatában állapították meg, hogy a törzsizomzatot erősítő gyakorlatok, a deréktájéki gerinc mozgástartomány megőrzése megakadályozhatják a derékproblémák kialakulását, sőt fontosnak is tartják ezek további vizsgálatát, hogy még komplexebb képet kapjunk ezen összefüggésekről.[43]

Mattila és munkatársai azt kutatták, hogy a katonai szolgálat alatti deréktájéki fájdalom elővetíti-e az élet későbbi szakaszában is az ebben a régióban meglévő panaszokat, és úgy találták, hogy az arra hajlamos egyéneknél várhatók az életük későbbi szakaszában fellépő derékfájdalmak, illetve panaszok, ha ezek a katonai szolgálat alatt is jelen voltak.[44]

Qu és szerzőtársai vizsgálták, hogy a terhelésnek kitett katonák esetén milyen, a gerincet érintő változások következnek be. Vizsgálták többek közt a paravertebralis (gerinközeli) izmok, a deréktájéki intervertebralis rés méretének, a lumbosacralis szög, a deréktájéki lordosis változását. Ezen értékeknél szignifikáns eltéréseket tapasztaltak.[45]

---

[39] Christine E. Bader et al.: Musculoskeletal Pain and Headache in the Active Duty Military Population: An Integrative Review. *Worldviews on Evidence-Based Nursing,* 15. (2018), 4. 264–271.

[40] Nicholas R. Koreerat – Christina M. Koreerat: Prevalence of Musculoskeletal Injuries in a Security Force Assistance Brigade Before, During, and After Deployment. *Military Medicine,* 186. (2021), Suppl. 1. 704–708.

[41] Stijn J. J. Thoolen – Marieke H. A. H. Van Den Oord: Modern Air Combat Developments and Their Influence on Neck and Back Pain in F-16 Pilots. *Aerospace Medicine and Human Performance,* 86. (2015), 11. 936–941.

[42] Christopher A. Orsello – Andrea S. Philipps – George M. Rice: Height and In-Flight Low Back Pain Association among Military Helicopter Pilots. *Aviation, Space, and Environmental Medicine,* 84. (2013), 1. 32–37.

[43] Takashi Nagai et al.: Lumbar Spine and Hip Flexibility and Trunk Strength in Helicopter Pilots With and Without Low Back Pain History. *Work,* 52. (2015), 3. 715–722.

[44] Ville M. Mattila et al.: Low Back Pain during Military Service Predicts Low Back Pain Later in Life. *Plos One,* 12. (2017), 3. 1–10.

[45] Hao Qu et al.: Spine System Changes in Soldiers after Load Carriage Training in a Plateau Environment: A Prediction Model Research. *Military Medical Research,* 7. (2020), 63. 1–11.

Knox és munkatársai írásából tudhatjuk, hogy a katonai szolgálatot teljesítő sofőröknél kis mértékű, de szignifikáns növekedés van a derékfájdalmak kialakulásának vonatkozásában, a kontrollcsoporthoz képest.[46]

Sturdy és szerzőtársai a katonai hátizsák viselése közbeni hatásokat vizsgálták csak a váll- és a csípőövvel is kiegészített hátizsákformák esetén. Azt találták, hogy a deréktájéki 4-es, 5-ös gerincre és a csípőkre is nagyobb erők hatnak mind a két esetben, mint a terhelés nélküli csoport esetén. További vizsgálatokat javasoltak a járás, illetve a hátizsák tömegeloszlás-vizsgálatát illetően.[47]

Kang és munkatársai kutatásukban azt vizsgálták, hogy milyen összefüggés van a deréktájéki gerinc fájdalmának és a porckorongjának sérvesedése, valamint a katonai rang és az iskolázottság között. Úgy találták, hogy az iskolázottsági fok és a betegség kialakulása közt nincs szignifikáns különbség, azonban a rang fordított arányban, de szignifikánsan összefüggést mutat a deréktájéki fájdalmak kialakulásának vonatkozásában.[48]

Yi és szerzőtársa azt vizsgálták, hogy a pszichoszociális faktorok, a fizikális állapot befolyásolják-e a mozgásszervi panaszok kialakulását. Arra a következtetésre jutottak 415 résztvevő bevonásával, hogy a kiképzés során fellépő stressz és megterhelés, valamint a korábbi mozgásszervi sérülések szignifikánsan megnövelik a panaszok kialakulásának valószínűségét. Azt javasolták, hogy több figyelmet kell fordítani a mozgásszervi kórtörténet felvételére.[49]

Ezen irodalmi példákból is látszik, hogy a téma nagyban érinti az aktív állományt világszerte. Véleményem szerint megfelelő szűréssel, illetve a megelőzésre helyezett nagyobb hangsúllyal, az időben elkezdett kezeléssel és minden rizikótényező megfelelő mérlegelésével a kockázat csökkenthető, a szövődmények súlyossága mérsékelhető, ezáltal pedig a szolgálatba való visszaállíthatóság, valamint a szolgálati időt követő panasz súlyosbodása valószínűségének alacsonyabb szintre helyeződése várható.

Felhasznált irodalom

Bader, Christine E. – Nicholas A. Giordano – Catherine C. McDonald – Salimah H. Meghani – Rosemary C. Polomano: Musculoskeletal Pain and Headache in the Active Duty Military Population: An Integrative Review. *Worldviews on Evidence-Based Nursing,* 15. (2018), 4. 264–271. Online: https://doi.org/10.1111/wvn.12301

Bean, J. C. – D. B. Chaffin – A. B. Schultz: Biomechanical Model Calculation of Muscle Contraction Forces. A Double Linear Programming Method. *Journal of Biomechanics,* 21. (1988), 1. 59–66. Online: https://doi.org/10.1016/0021-9290(88)90192-3

[46] Jeffrey B. Knox et al.: Occupational Driving as a Risk Factor for Low Back Pain in Active-Duty Military Service Members. *The Spine Journal,* 14. (2014), 4. 592–597.

[47] Jordan T. Sturdy – Pinata H. Sessoms – Anne K. Silverman: A Backpack Load Sharing, Model to Evaluate Lumbar and Hip Joint Contact Forces during Shoulder Bone and Hip Belt Assisted Load Carriage. *Applied Ergonomics,* 90. (2021). 1–10.

[48] Suk Hyung Kang et al.: Military Rank and the Symptoms of Lumbar Disc Herniation in Young Korean Soldiers. *World Neurosurgery,* 82. (2014), 1–2. 9–14.

[49] Jeong Min Yi – Gwang Suk Kim: Factors Influencing Musculoskeletal Symptoms in Military Personnel during Basic Combat Training. *Journal of Korean Academy of Nursing,* 46. (2016), 4. 523–533.

Brinckmann, Paul – Henk Grootenboer: Change of Disc Height, Radial Disc Bulge and Intradiscal Pressure from Discectomy. And In Vitro Investigation on Human Lumbar Disc. *Spine,* 16. (1991), 6. 641–646. Online: https://doi.org/10.1097/00007632-199106000-00008

Brinckmann, Paul – M. Biggemann – D. Hilweg: Prediction of the Compressive Strength of Human Lumbar Vertebrae. *Clinical Biomechanics,* 4. (1989), Suppl. 2. 1–27. Online: https://doi.org/10.1016/0268-0033(89)90071-5

Brinckmann, Paul – Manfred Horst: The Influence of Vertebral Body Fractures, Intradiscal Injection, and Partial Discectomy, on the Radial Bulge and Height of Human Lumbar Discs. *Spine,* 10. (1985), 2. 138–145. Online: https://doi.org/10.1097/00007632-198503000-00005

Brinckmann, Paul – R. W. Porter: A Laboratory Model of Lumbar Disc Protrusion. Fissure and Fragment. *Spine,* 19. (1994), 2. 228–235. Online: https://doi.org/10.1097/00007632-199401001-00019

Brinckmann, Paul – Wolfgang Frobin – Eberhard Hierholzer – Manfred Horst: Deformation of the Vertebral End-Plate under Axial Loading of the Spine. *Spine,* 8. (1983), 8. 851–856. Online: https://doi.org/10.1097/00007632-198311000-00007

Brinckmann, Paul – Wolfgang Frobin – Gunnar Leivseth (szerk.): *Musculoskeletal Biomechanics.* Stuttgart – New York, Thieme, 2002.

Dieen, J. H. – I. Kingma: Total Trunk Muscle Force and Spinal Compression are Lower in Asymmetric Moments as Compared to Pure Extension Moments. *Journal of Biomechanics,* 32. (1999), 7. 681–687. Online: https://doi.org/10.1016/S0021-9290(99)00044-5

Felsenberg, D. – W. A. Kalender – D. Banzer – G. Schmilinsky – M. Heyse – E. Fischer – U. Schneider: Quantitative computertomographische Knochenmineralgehalts Bestimmung. *Fortschr Röntgenstr,* 148. (1988). 431–436. Online: https://doi.org/10.1055/s-2008-1048225

Frobin, Wolfgang – Paul Brinckmann – Gunnar Leivseth – Martin Biggemann – Olav Reikerås: Precision Measurement of Segmental Motion from Flexion-Extension Radiographs of the Lumbar Spine. *Clinical Biomechanics,* 11. (1996), 8. 457–465. Online: https://doi.org/10.1016/S0268-0033(96)00039-3

Horst, Manfred – Paul Brinckmann: Measurement of the Distribution of Axial Stress on the End-Plate of the Vertebral Body. *Spine,* 6. (1981), 3. 217–232. Online: https://doi.org/10.1097/00007632-198105000-00004

Jäger, Matthias: *Biomechanisches Modell des Menschen zur Analyse und Beurteilung der Belastung der Wirbelsaeule bei der Handhabung von Lasten.* Düsserdorf, VDI Verlag, 1987.

Jäger, Matthias – A. Luttmann: Entwicklung eines biomechanischen Modells zur Bestimmung der Belastung der Wirbelsäule. *Biomedizinische Technik,* 38. (1993), 393–394. Online: https://doi.org/10.1515/bmte.1993.38.s1.393

Kang, Suk Hyung – Jin Seo Yang – Yong Jun Cho – Seung Won Park – Kwang Pil Ko: Military Rank and the Symptoms of Lumbar Disc Herniation in Young Korean Soldiers. *World Neurosurgery,* 82. (2014), 1–2. 9–14. Online: https://doi.org/10.1016/j.wneu.2013.02.056

Knox, Jeffrey B. – Joseph R. Orchowski – Danielle L. Scher – Brett D. Owens – Robert Burks – Philip J. Belmont Jr.: Occupational Driving as a Risk Factor for Low Back Pain in Active-Duty Military Service Members. *The Spine Journal,* 14. (2014), 4. 592–597. Online: https://doi.org/10.1016/j.spinee.2013.06.029

Koreerat, Nicholas R. – Christina M. Koreerat: Prevalence of Musculoskeletal Injuries in a Security Force Assistance Brigade Before, During, and After Deployment. *Military Medicine,* 186. (2021), Suppl. 1. 704–708. Online: https://doi.org/10.1093/milmed/usaa334

Leskinen, T. P. J. – H. R. Stålhammar – I. A. A. Kuorinka – J. D. G. Troup: A Dynamic Analysis of Spinal Compression with Different Lifting Techniques. *Ergonomics,*. 26. (1983a), 6. 595–604. Online: https://doi.org/10.1080/00140138308963378

Leskinen, T. P. J. – H. R. Stålhammar – I. A. A. Kuorinka – J. D. G. Troup: The Effect of Inertial Factors on Spinal Stress When Lifting. *Engineering in Medicine,* 12. (1983b), 2. 87–89. Online: https://doi.org/10.1243/EMED_JOUR_1983_012_023_02

Mattila, Ville M. – Heikki Kyröläinen – Matti Santtila – Harri Pihlajamäki: Low Back Pain during Military Service Predicts Low Back Pain Later in Life. *Plos One,* 12. (2017), 3. 1–10. Online: https://doi.org/10.1371/journal.pone.0173568

McGill, S. M. – R. L. Hughson – K. Parks: Changes in Lumbar Lordosis Modify the Role of the Extensor Muscles. *Clinical Biomechanics,* 15. (2000), 10. 777–780. Online: https://doi.org/10.1016/S0268-0033(00)00037-1

Miyamoto, K. – N. Limua – M. Maeda – E. Wada – K. Shimizu: Effects of Abdominal Belts on Intra-Abdominal Pressure, Intra-Muscular Pressure in the Erector Spinae Muscles and Myoelectrical Activities of Trunk Muscles. *Clinical Biomechanics,* 14. (1999), 2. 79–87. Online: https://doi.org/10.1016/S0268-0033(98)00070-9

Nachemson, Alf: Lumbar Intradiscal Pressure. Experimental Studies on Post-Mortem Material. *Acta Orthopedica Scandinavica,* 31. (1960). Supplementum 43. 1–104. Online: https://doi.org/10.3109/ort.1960.31.suppl-43.01

Nagai, Takashi – John P. Abt – Timothy C. Sell – Karen A .Keenan – Nicholas C. Clark – Brian W. Smalley – Michael D. Wirt – Scott M. Lephart: Lumbar Spine and Hip Flexibility and Trunk Strenght in Helicopter Pilots With and Without Low Back Pain History. *Work,* 52. (2015), 3. 715–722. Online: https://doi.org/10.3233/WOR-152192

Nelson, Richard C. – Chauncey A. Morehouse (szerk.): *Biomechanics IV.* Baltimore, Maryland, Macmillan Education, 1974. DOI: https://doi.org/10.1007/978-1-349-02612-8

Orsello, Christopher A. – Andrea S. Philipps – George M. Rice: Height and In-Flight Low Back Pain Association among Military Helicopter Pilots. *Aviation, Space, and Environmental Medicine,* 84. (2013), 1. 32–37. Online: https://doi.org/10.3357/ASEM.3425.2013

Qu, Hao – Ling-Jia Yu – Ju-Tai Wu – Gang Liu – Sheng-Hui Liu – Peng Teng – Li Ding – Yu Zhao: Spine System Changes in Soldiers after Load Carriage Training in a Plateau Environment: A Prediction Model Research. *Military Medical Research,* 7. (2020), 63. 1–11. Online: https://doi.org/10.1186/s40779-020-00293-1

Reyna, J. R. – S. H. Leggett – K. Kenney – B. Holmes –V. Mooney: The Effect of Lumbar Belts on Isolated Lumbar Muscle. Strength and Dynamic Capacity. *Spine,* 20. (1995), 1. 68–73. Online: https://doi.org/10.1097/00007632-199501000-00013

Sturdy, Jordan T. – Pinata H. Sessoms – Anne K. Silverman: A Backpack Load Sharing, Model to Evaluate Lumbar and Hip Joint Contact Forces during Shoulder Bone and Hip Belt Assisted Load Carriage. *Applied Ergonomics,* 90. (2021.). 1–10. Online: https://doi.org/10.1016/j.apergo.2020.103277

Szendrői Miklós (szerk.): *Ortopédia.* Budapest, Semmelweis Kiadó, 2005.

Szentágothai János – Réthelyi Miklós: *Funkcionális anatómia 1 kötet.* Budapest, Medicina Kiadó – Semmelweis Kiadó, 1996.

Thoolen, Stijn J. J. – Marieke H. A. H. Van Den Oord: Modern Air Combat Developments and Their Influence on Neck and Back Pain in F-16 Pilots. *Aerospace Medicine and Human Performance,* 86. (2015), 11. 936–941. Online: https://doi.org/10.3357/AMHP.4303.2015

Yi, Jeong Min – Gwang Suk Kim: Factors Influencing Musculoskeletal Symptoms in Military Personnel during Basic Combat Training. *Journal of Korean Academy of Nursing,* 46. (2016), 4. 523–533. Online: https://doi.org/10.4040/jkan.2016.46.4.523

Tartalom