



LUDOVIKA
EGYETEMI KIADÓ

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY
AND PUBLIC MANAGEMENT SCIENCE

Volume 19 (2020)
Issue 1

ISSN 2498-5392 (print)
ISSN 2498-5392 (online)

AARMS is a peer-reviewed international scientific journal devoted to reporting original research articles and comprehensive reviews within its scope that encompasses the military, political, economic, environmental and social dimensions of security and public management.

AARMS is published in one volume of four issues per year by the National University of Public Service, Budapest, Hungary, under the auspices of the Rector of the University.

Articles and other text material published in the journal represent the opinion of the authors and do not necessarily reflect the opinion of the Editors, the Editorial Board, or the Publisher.

All correspondence should be addressed to Prof. Dr. PADÁNYI József, Editor-in-Chief,
National University of Public Service
P. O. Box 15, H-1581 Budapest 146 Hungary
aarms@uni-nke.hu

AARMS

ACADEMIC AND APPLIED RESEARCH IN MILITARY
AND PUBLIC MANAGEMENT SCIENCE

Volume 19
Issue 1
2020

An International Journal of Security, Strategy, Defense Studies,
Military Technology and Public Management

Published by the National University of Public Service

PADÁNYI József (Chair of the Editorial Board)

SOLYMOSI József (Honorary Chair of the Editorial Board)

Editorial Board:

BLAHÓ András	Pavel MANAS
Vasile CĂRUȚAȘU	NÓGRÁDI György
Erich CSITKOVITS	ONDRÉK József
Boris DURKECH	Boguslaw PACEK
HAIG Zsolt	Harald PÖCHER
HALÁSZ Iván	SZENES Zoltán
KENDE György	TAKÁCS Péter
Ulrike LECHNER	TAMÁS András

TÖRÖK Gábor

Editorial:

PADÁNYI József (Managing Editor)
GAZDAG Ferenc (Editor)
HALÁSZ László (Editor)
GŐCZE István (Editor)
ORBÓK Ákos (Editorial Assistant)

Publisher:

Ludovika University Press Non-Profit Ltd.
Responsible for Publishing:
KOLTÁNYI Gergely, Managing Director

Proofreader:

ORBÁN Áron

Typeset and print by Ludovika University Press Non-Profit Ltd.

ISSN 2498-5392

Contents

Gábor BENCSIK Are We Really Lacking the Effectiveness of Financial Resource Management in the Defence Sector?	5
Tamás BEREK, László FÖLDI, József PADÁNYI The Structure and Main Elements of Disaster Management System of the Hungarian Defence Forces, with Special Regard to the Development of International Cooperation	17
Mihály BODA Erasmus and István Magyarai on the Justification of War	27
Stefany CEVALLOS Public Service Management in Ecuador.....	37
Tamás HÁBERMAYER, Péter HORVÁTH Voluntary Rescue Service in Hungary: The HUSZÁR Team.....	45
Gergely HERCZEG, Ágoston RESTÁS Solutions for the Accessibility of Water Sources for Fire Extinguishment	55
Ferenc KOCZKA Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment.....	65
TAMÁS SZÁDECZKY Governmental Regulation of Cybersecurity in the EU and Hungary after 2000.....	83
Szilveszter SZELECZKI Outlining a Set of Theory-based Requirements for the Future Digital Soldier.....	95
Tomáš ZEMAN Soft Targets: Definition and Identification.....	109
Authors' Guide.....	121

Are We Really Lacking the Effectiveness of Financial Resource Management in the Defence Sector?

Gábor BENCSIK¹

Recently, the increase of spending in the sector of defence has opened up larger and larger spaces for the development / modernisation potential of individual countries. However, in this “resource overflow”, the effectiveness of the use of financial resources for defence is undermined. This study takes a look at the dangers of the ever-decreasing defence budget share (dangers well known in economics and well known in the field of defence sphere in the recent past) and the “free-rider effect” observed in different members states of the NATO (related to e.g. NATO Article 5) and reviews the effectiveness of financial resource management.

Keywords: *defence spending, financial resource management, threats-security, cost-effectiveness, efficiency testing.*

“If mathematics, including everything that rests on it, were somehow suddenly to be withdrawn from our world, human society would collapse in an instant.”
(Ian Nicholas Stewart)²

Introduction

The American economist and mathematician George Bernard Dantzig (1914–2005) is considered one of the pioneers, explorers and legendary figures of operations research. [1: 159–161] During the period of WWII, he spent a considerable time in the Pentagon (as the leader of Combat Analysis Branch of Statistical Control and later as the mathematical adviser of the Department of the U.S. Air Force [1]) and contributed to the explosive development of operations research as a complex branch of applied mathematics. The simplex method and algorithms to deal with transport problems have attracted the attention of contemporary scientists, especially Roland Neely McKean (1917–1993) and Charles J. Hitch (1910–1995). McKean and Hitch published their work in 1960 entitled *The Economics of Defence in the Nuclear Age*, in which they identify economically—as an economic problem of defence—basically three interrelated factors: the quantity and quality of national resources (1), the

¹ Ph.D. student, National University of Public Service, Doctoral School of Military Engineering; Senior Financial Officer in the Ministry of Defence, Defence Economic Bureau; e-mail: bencsik.gabor@hm.gov.hu; ORCID: <https://orcid.org/0000-0002-1394-6765>

² 1945–, British mathematician. Source: [10].

share of national resources dedicated to defence (2) and the effectiveness of the use of these dedicated resources (3). [2: v]

The extent of each nation’s resources (1) used for defence purposes (2) is highly dependent on social support within the nation and on the political will. In addition to the scarcity of resources available in the complex system, we could observe a more pronounced downward trend in defence spending in the past (over several decades), which was steadily plummeting in recent years, but has taken a sluggishly rising path. [3]

Further narrowing the statistics we can observe the negative impact of the 2008 global economic and financial crisis on GDP-related defence spending world-wide, both within NATO and in many countries besides NATO [3]—despite the fact that in 2006, NATO member states accepted to spend 2% of their gross domestic product (GDP) on defence and armed forces to cope with the forthcoming challenges of the time. Relying on the collective defence established by Article 5 of the NATO Statute, [4] only a few member states are merely “beneficiaries” of the system, and this current situation is described in classical economics as an economic problem called “free-rider effect”. (cf. [5: 7])

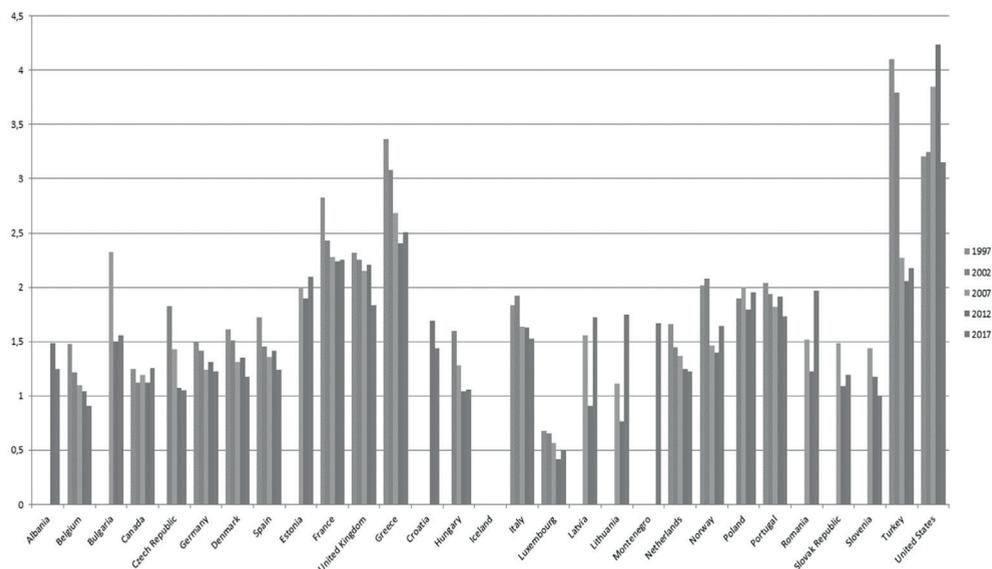


Figure 1. NATO member states’ GDP-related defence expenditure over the last two decades. (Edited by the author based on [3].)

Keith Hartley also attaches considerable and particularly worrying consequences to the declining defence budget. Hartley noted in his writing of December 2016, *The Economics of European Defence*: “Falling or constant defence budgets in real terms and continued cost escalation mean difficult defence choices cannot be avoided: something has to go. Some nations have already confronted such choices and have abandoned a major capability.” [11: 2]

These processes, the significantly deteriorated security situation and the decreasing GDP-related defence expenditures in recent times have highlighted the need to re-monitor and further investigate a previous problem, namely how we can provide the best possible “end product” (solution) to the “customer” from a “unit of money (UoM)”.

The Still Unresolved Issue of Optimal Financial Resource Management

“Defence and security are controversial public goods. [...] Of course, the ‘force-orientation’ of the defence economy also depends on how strong a country’s army is, how much it consumes, and how much it contributes to the GDP, the role it plays in implementing the country’s foreign policy, and maintaining the country’s internal security.”
Zoltán Szenes³

As we read in the introduction, Hitch and McKean’s 1960 publication [2] paid particular attention to the efficient use of resources dedicated to defence, which was identified as a key issue in defence management.

The limitations of defence resources (in the general sense, including material resources and services) can be traced back to the extent of the availability of financial resources. That is why the continuous, up-to-date examination of the optimal resource management of the financial resources devoted to the maintenance of security as a public good is particularly important. In Hungarian context, a study was published in 2003 by the Center for Security Policy and Defence Research (in Hungarian: Biztonságpolitikai és Honvédelmi Kutatások Központja Alapítvány – BHKK Foundation) entitled *Designing the efficient use of resources in the defence sphere, with particular regard to financial resources*. [7] The study – as its title suggests – attaches particular importance to the examination of the use of financial resources, especially those available to the defence sector. However, if we observe more thoroughly, the study, which processes historical data and procedures, can be dated several years back, when the budget share, which had been reduced in relation to the GDP until 1999, was for a short term on a rising trend.⁴ Apart from all these, the period defined by defence spending on the rising trend is characterised by the following statement: “In the course of economic planning, feasibility studies as well as cost and effectiveness analyses are not prepared with the required level of detail.”⁵ [7: 50]

The Background of Cost- and Effectiveness Analysis (Threat and Security)

“There is no clear vision about what kind of defence economics would serve the most the nation’s interest in the circumstances of market economy, in the changing security situation.”
Zoltán Szenes⁶

The performance of economy is crucial for the defence power of a country. In a well-operating economy, it is possible to raise other important capabilities, such as military capabilities, to the competent (expected) level. However, with increasing defence spending, there is increasing pressure on responsible and efficient financial resource management as well.

³ Former Chief of the General Staff of the Armed Forces of the Republic of Hungary (2003–2005). Source: [6: 10, 12]. Translated by the author of this article.

⁴ Note: Subsequently, following our accession to the European Union in 2004, a decline in the share of GDP was again observed. Cf.: [5: 7].

⁵ Translated by the author of this article.

⁶ Source: [6: 6]. Translated by the author of this article.

Numerous scholarly works offer in-depth knowledge of cost and effectiveness analysis. The 2003 BHKK study refers to the cost-effectiveness of defence spending as follows: “In planning and decision-making work, the cost-effectiveness approach (more for less principle) results in improved organisational performance.”⁷ [7: 5]

The management of this era (both at the level of military tactics management and military strategy management) was primarily determined by the cost-effectiveness approach (“more for less” principle). We should not be surprised by this: as mentioned before, the Hungarian army has undergone significant decommissioning in the few decades preceding that period.

At the moment, however, we are in the midst of another military reform,⁸ which intends nothing more than a correspondence with the requirements mentioned in many other previous articles, taking into account necessity and timeliness. We could see that the rise in defence expenditures to the proportion of 2% of the GDP was formulated as an international and national priority, the target date of which was set by the Hungarian government in 2024. [8: point 1] The planned increase in financial resources can be measured in hundreds of billions of HUF, because of which the opportunity has now come for the real development of national defence. However, the objective of the actual development concerns not only the absolute use of the available resources, but also the importance of efficient financial resource management and, if necessary, the reconsideration of management procedures/methods.

The reconsideration of military management procedures/methods is not only a military matter but also a national requirement. Optimal use of the defence budget can be compared to the perfect market in the economy, which, as is known, only exists in theory. In addition to the homogeneity of goods, perfect information, rational decisions, temporal and spatial identities, and the absence of immediate reactions, we have to reckon with various national security factors that complicate even more the complex mathematical models. We often mention the importance and role of effective financial resource management in the 21st century as a “trendy and fashionable way”, but how does this work in the practice? How effective is the financial resource management of the defence sector (both within and outside Hungary)? How do we calculate/measure the efficiency of the financial resource management?

In order to answer the questions raised, let’s start with the basics, that is, first of all, we need to examine why we need protection. What is protection and how much is it needed?

According to the *Explanatory Dictionary of the Hungarian Language* [12] issued in 1959–1962 by the Academic Press, the defence is an “active preservation, defence, protection, and protection of the physical integrity, life and integrity of someone”, and “the

⁷ Translated by the author of this article.

⁸ Note: a military reform provides an excellent opportunity to rethink and develop the functionality and methods of the army. The mentioned study by the BHKK Foundation highlights: “In the context of military development, all structural, management and operational transformations that ensure the most efficient management and use of forces and assets must be implemented. However, the first pace of the transformation is not in the exchange of applied military equipment and weapon systems, but in the re-thinking of applied organisational and management procedures.” [7: 88] The referenced military reform is the Zrínyi 2026 Defence and Military Development Program, which is referred to by various organs as the largest defence and military development program of the past 26 years.

defence activities and operation of armed forces, protecting organisations against (military) attack”⁹.

Based on all these, defence is generally expressed as a response to a particular threat or its prevention. With the application of protection, we have no other purpose than to reduce the level of threat, to create security, or to increase the existing security level. The relationship between threat and security is illustrated in Figure 2 below:

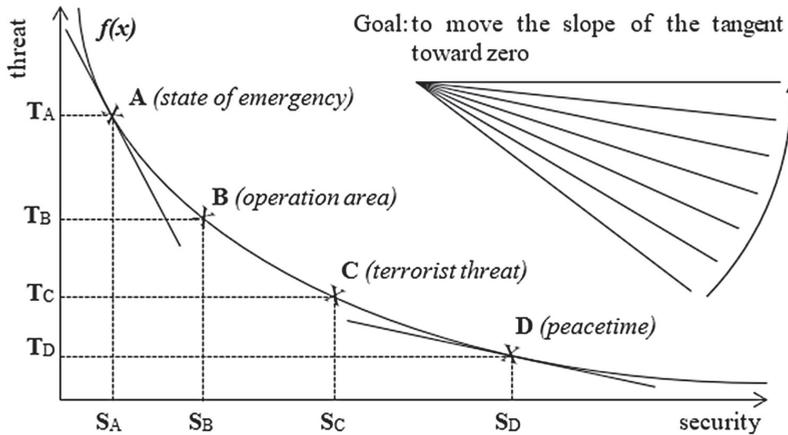


Figure 2. *The relationship between threat and security [f(x)].*
 [Edited by the author.]

Figure 2 shows four alternative options that not only illustrate the relationship between security and threat, but will help us to understand how the efficiency of financial resource management can be interpreted in different cases. The four alternatives shown are:

- **A:** during a special legal period, in case of the state of emergency;
- **B:** in a high-risk operation area;
- **C:** during a special legal period in case of a terrorist threat;
- **D:** in peacetime.

In the four alternative options outlined, we can discover a number of common points, such as all four points are on the common curve between threat and security, and in all four cases, the threat level is reduced, leading to an increase in the level of security. However, this objective can be achieved by different methods and procedures at different points. We only need to think about how much IT security development reduces the threat at “A” or how the same development contributes to the increase of the level of security at point “D”. It is clear and obvious that this kind of development in peacetime (“D”) can contribute much more to an increase of the level of security, since it can provide adequate security against a possible cyberattack. However, the same development is not likely to show the same level of security increase in an emergency situation (“A”) where the rules of direct combat contact dominate. Here, we can immediately be attentive to the “time” factor, which

⁹ Translated by the author of this article.

is why it is essential that we have the time to respond to the (response) challenges we face. On the basis of these, it can be seen that efficient management with the available resources is rather complex and in different cases it is at a different level. We can consider as our primary objective to create a function describing curve, after which the approximation to optimal financial resource management can be achieved by applying differential geometry.

Taking into account this example (defence IT development), and returning to the correlation and relationship system outlined in Figure 2, it can be concluded that the management of defence budget resources can be considered effective if it can reduce the threat level, thereby increasing the level of security. The higher the rate of this change, the better we approach the level of optimal (non-existent) financial resource management. In general terms: *in the field of financial resource management, the efficiency of the management process can be measured by the—indirect or direct—result of measures aiming at the reduction of the level of measurable threat, using the “unit of money (UoM)” for measurement.*

Concerning the notion “efficiency of financial resource management of defence resources”, the efficiency of this management process is the aggregate rate of the efficiency factor of each sub-process. On the basis of these, the implementation of the sub-processes of financial managing should seek to maximise the contribution of management to a positive shift in the threat-security curve (to an increase of the safety level). However, it can be noticed that the aggregate value/level must represent a continuously calculated value/level (see Figure 3). Based on these, constructive sub-processes with added value in the field of efficient management can be considered as if the effect of their threat-reducing/safety-increasing value on the threat-safety curve led to a positive shift. Determining this property is independent of the actual aggregate efficiency value, which means that a subprocess can be considered effective even if it involves an aggregate efficiency level decrease but also a safety level increase, and can be considered ineffective if its aggregate efficiency level is increased, but has a safety-reducing effect (see Figure 2).

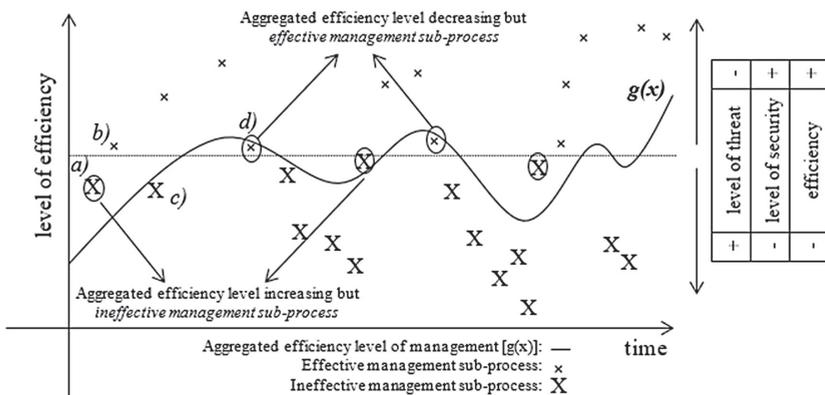


Figure 3. The illustration of the role of decisions affecting the financial resource management processes in supporting/enhancing their effectiveness.

[Edited by the author.]

The decision points shown in Figure 3 illustrate the role of each decision in the effects on the threat and security level, taking into account their status in relation to the aggregated efficiency level. The figure clearly shows that although the large X indicated in a) reduces the level of security (and simultaneously increases the threat level), its contribution to the aggregate efficiency level is constructive. If we consider our earlier statement that “the implementation of the sub-processes of financial managing should seek to maximise the contribution of management to a positive shift in the threat-security curve,” it can be stated that although the value indicated in a) has a positive effect on the aggregate efficiency level, at the same time, it is not constructive concerning the safety level, and does not increase efficiency. Accordingly, the decision value in a) is not considered effective. This statement is also supported by the value in c), the effect of which is to increase the level of threat to be equal to the value in a), except that the effect of this value on the aggregate efficiency level is also negative.

However, the values in b) and d) are already the result of an efficient management process based on their positive impact on the level of safety. The difference between the two points on the same level can be seen in their effect on the aggregate efficiency level. It can be seen that while the level of the effective management decision in b) has a positive effect on the aggregate value, the same property can no longer be attributed to the value indicated in d). Regardless of all these, both points have the same efficiency factor as they are capable of increasing the level of security with the same degree.

In the periods shown in Figure 2, all of the management decision alternatives can be found at almost all levels of financial resource management. Taking into account the correlations of Figure 3, we can conclude that the effectiveness of individual financial resource management processes are determined by their impact on threat and safety levels, and this result is independent of the aggregate value of the efficiency level.

The Impact of the “High Level” Protection Budget and the Importance of the Decision Duration

As mentioned earlier, in different periods of time (cf. Figure 2), there are different time intervals for managers to make decisions. As is often the case with leadership theory education, there is no wrong decision, all decisions are adequate at the given time, and our idea of judging the decision can be changed as time goes by. Therefore, the importance of the time-factor in explaining the problem is quite pronounced.

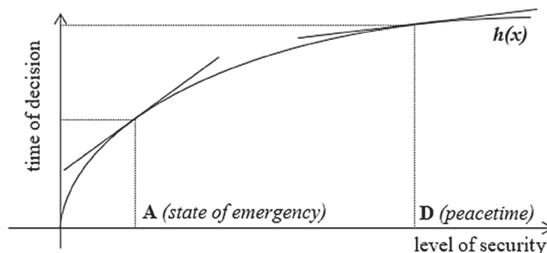


Figure 4. The relationship between security level and time of decision making $[h(x)]$.
[Edited by the author.]

From the context shown in Figure 4, we can see that the higher the security level of a country, the more time it takes for leaders to make defence decisions (cf. “peacetime” and “state of emergency”). Here, it is apparent that our aim is to reduce the first derivative value of the function $h(x)$, which represents the relationship, to the level 0, by which convergence can be achieved towards the maximum-security level and the corresponding high-value time factor.

On the other hand, however, it can be stated that the lower the amount of (financial) resources available to military leaders, the more they are forced to make their decisions in favour of a cost-effectiveness approach (“more for less”). However, low (financial) resources have low effects. That is why the issue of effective financial resource management is placed in the background and the role of the above-mentioned “more for less” approach is maximised. In this case, in the short term, one of the goals is “as much as possible to get more”. The problem arises only if we apply our existing methods based on this approach and, in the event of a possible increase in resources, we stick to the “well-known” procedures, ignoring the characteristics of the various factors of the descriptive function(s) that are currently being described, and their values. In this case, the impact of the increase in defence spending is in many cases less than expected:

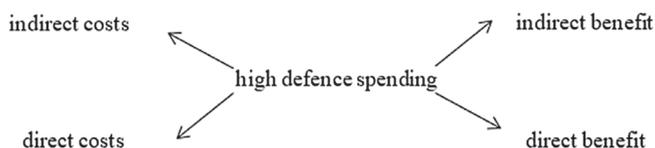


Figure 5. *Illustration of the effects of defence spending.*
(Edited by the author based on [2: vi–vii].)

The level of protection expenditure shown in Figure 5 may have a number of impacts also beyond the direct defence sphere. Accordingly, the efficient use of defence resources—both the direct and the indirect uses—affect the entire national economy (as well as its actors). Considering these relationships, it can also be concluded that the level of defence spending is nothing other than the amount of money spent by a given player (economy) on security. We can define how this “purchase” is carried out, how efficient it is, by the methods used by the actors involved (with defence spending), and by the quantifiable results of the methods and procedures applied.

From the methods described above the primary and most important is the specification of the descriptor variable, and the exact determination of its components. After the definition of the functions of the components—if it is a hypothetical function as outlined—our primary goal is to move the slope of the tangent to a given point of the functions toward 0. This displacement can be carried out by differential calculus, if necessary, using a partial derivation method. However, we must be careful that while in some decisions our primary goal is the reduction of the slope of the affected function (Figure 4), in other cases the goal is to increase this value (Figure 2). If the decision to be taken supports the shift to these directions, then we can talk about an efficient management sub-process. In all other cases, the result falls below the decision criterion level, so it is advisable to reject them (see the large X’s in Figure 3).

The Problem of Resource Limitation and the Defence Economics Conundrum

Our recent developments in military technology, demanded by the dynamics of the era, the information warfare in our world, the modern telecommunication systems and tools have greatly transformed our vision of today's warfare. However, one thing is permanent: the security of a nation is mainly determined by the nature and rational amount of equipment used by its military—among other technical and economic factors—and thus the extent of the national resources dedicated to the realisation of these developments and the utility of developments.

Of course, the development of a nation is determined by its core capacities, in particular the proportion of national resources (material, technical, manpower, etc.) made available for the determined purpose. At the same time, we need to deal with the determination of the proportion of these resources with caution, leaving sufficient margin for the development of security. However, the size of the resources dedicated to defence management has been strongly influenced. These influences depend not only on the performance of a particular nation, but on the political will representing the nation's interest and will, the international pressure and other threats present.

The amount of resources devoted to defence management is primarily represented by the total of approved budget appropriations for ministries involved in defence. However, the margin for budgetary appropriations is sufficiently flexible to determine the proportion of personnel, operational and development expenditure, which plays a key role in budgetary planning. Analysing these ratios, we can rightly assume that we have a good view of a country's defence economy, because if the share of personal costs is high compared to the other two, then it can be rightly argued that the defence structure of that country is based on obsolete, less automated military technology. At the same time, Hitch and McKean, in their work *Economics of Defense in the Nuclear Age* published in 1960, highlight the impact of the acquisition of military equipment on budget planning. They point out: "The prices of goods to be bought in the future are uncertain. One course of action may itself drive up the price of particular weapons or materials, and it is not possible to predict these effects with complete accuracy. The characteristics and cost of some exceptional items may literally be fixed, or nearly fixed, even if we are looking several years ahead. Nonetheless, imperfect as it is, the money cost of a future program usually shows the sacrifice that would be required of the Department better than other measures." [2: 26]

At the same time, Hartley, outlining the shortcomings of the European defence policy, sets out general economic principles to promote more efficient use of resources for defence management. [11: 2–4] In his writing he highlights:

- the benefits of pure competition against monopoly, oligopoly and monopolistic competition, reflects its high value adding role of innovation, ensuring a market price;
- the role and importance of specialisation based on the comparative advantages of each country;
- the role of economies of scale, international projects and R&D;
- the importance of the role of club goods (public goods typical of the defence industry);
- the role of substitute products;
- and last but not least, the priority of the effect of output of the defence, which is described as below: „Major reviews of defence usually focus on inputs rather than defence outputs.

Inputs in the form of the numbers of military personnel and numbers of combat aircraft, tanks and warships dominate debates. This is the wrong method – the focus should be on the contribution of inputs to defence output in the form of peace, protection and national security. Admittedly, there is an absence of money values for defence output, but the output focus is economically correct. Moreover, there should be an additional focus on the effects of small changes in inputs on defence outputs. For example, what are the effects of a smaller or larger air force on defence output; similarly, for a smaller or larger army and navy?” [11: 4]

Conclusion

In recent times, with the increase of economic performance that broke the downward trend following the global crisis in 2008, we can see an increasing level of aggregate defence spending. The United States is ranked first among the countries with the highest defence spending in the world (2016: \$ 611 billion [1.7% growth compared to 2015]) excluding China, Russia, and India who can count 5.4%–8.5% rise in defence spending by looking at data from 2015 to 2016. [3]

However, it can be observed that increasing military spending from 2014 is not necessarily consistent with the development needs of the defence industry required by nations/economies. This is explained by the fact that in individual countries the “threat factors” present are observed as a “military problem” and they often ignore the issue of an efficient resource allocation of defence resources that are closely related to it. Alas, this is by the fact that in the recent past an exact mathematical model was not revealed and the correction of the previously created models was not realised.

The poetic question raised in the title does not require any particular explanation. It can be seen that in the current security environment, the companies—with their over-appetite for profit—do not address the issue of national defence as a primary issue. Summarising the above, it is clear that all factors affecting (civilian and military) management must be a matter of defence (and must be planned at all levels and for each portfolio) as a priority issue.

We can say that developing the domestic defence industry is of key importance. The Hungarian Defence Forces Modernisation Institute established on 1st January, 2019 provides an excellent opportunity for Hungary, as well as the Zrínyi 2026 Defence and Military Development Program launched in the recent period, which in terms of volume is simply a huge set of opportunities. However, exploiting these opportunities should be based on scientific principles, taking into account the limitations of resources, increasing the efficiency of defence financial resource management, while maximising the usefulness for society. Following the creation of the necessary theoretical foundations, a possible microsimulation model—including mathematical methods, especially operations research results and graph theory—could be used to map the aggregate effects of the planned measures, which would provide an opportunity to carry out a complex, multi-dimensional analysis, and thus an impact study, making up for the lack of necessary feasibility studies and cost-effectiveness analyses, the lack of which affected economic planning. All these “needs” are confirmed by the words of the president of the Hungarian Academy of Sciences (in Hungarian Magyar

Tudományos Akadémia, MTA), László Lovász, who has told in May 2018, at the 189th General Assembly of this institute, the following: “Scientific questions of public interest should be answered by a scientific method based on internationally accepted standards.” [9]

References

- [1] PRÉKOPA A.: George Dantzig (1914–2005). *Alkalmazott Matematikai Lapok (Az MTA Matematika Tudományok Osztályának Közleményei)*, 24 1 (2007), 159–161.
- [2] MCKEAN, R. N. – HITCH, C. J.: *The Economics of Defence in the Nuclear Age*. Santa Monica, The RAND Corporation, 1960.
- [3] *Military expenditure (% of GDP)*. Washington, D.C., The World Bank – Data, 2019. <https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS> (Downloaded: 26.02.2019)
- [4] *The North Atlantic Treaty*. Washington, D.C., 1949. NATO. www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=hu (Downloaded: 27.02.2019)
- [5] BALLA T. – BOROS I. – BENCSIK G.: A biztonság iránti kereslet, avagy a védelmi kiadások másik oldala. *Költségvetés, Pénzügy, Számvitel (a HM Védelemgazdasági Hivatal tudományos-szakmai kiadványa)*, 2 (2017), 4–15.
- [6] SZENES Z.: A védelemgazdaság helyzete Magyarországon. *Katonai Logisztika*, 2 (2015), 5–52. http://epa.oszk.hu/02700/02735/00080/pdf/epa02735_katonai_logisztika_2015_2_005-052.pdf (Downloaded: 27.02.2019)
- [7] *Az erőforrások hatékony felhasználásának tervezése a védelmi szférában, különös tekintettel a pénzügyi erőforrásokra*. [Study] Budapest, BHKK Alapítvány, 2003. www.mta.hu/hu/Publikaciok/BHKK_OTKA.pdf (Downloaded: 27.02.2019)
- [8] *A honvédelmi kiadások és a hosszú távú tervezés feltételeinek megteremtését szolgáló költségvetési források biztosításáról szóló 1273/2016. (VI. 7.) Korm. határozat*.
- [9] *Az Akadémia a tudományos módszer mellett állt ki – Lovász László elnöki beszámolója*. <https://mta.hu/kozgyules2018/az-akademia-a-tudomanyos-modszer-mellett-all-ki-lovasz-laszlo-elnoki-beszamolaja-108702> (Downloaded: 28.02.2019)
- [10] STUART, I.: *Nature’s numbers: The unreal reality of mathematics*. New York, Basic Books, 1995.
- [11] HARTLEY, K.: *The Economics of European Defence*. Paris, Armament Industry European Research Group, 2016. www.iris-france.org/wp-content/uploads/2016/12/ARESGroup-Economics_of_European-Defence-d%C3%A9c2016.pdf (Downloaded: 28.02.2019)
- [12] *A magyar nyelv értelmező szótára*. Budapest, Akadémiai, 1959–1962.

The Structure and Main Elements of Disaster Management System of the Hungarian Defence Forces, with Special Regard to the Development of International Cooperation

Tamás BEREK,¹ László FÖLDI,² József PADÁNYI³

The use of military forces in disaster relief activities is indispensable. It is a human and technical resource that can carry out special tasks quickly and professionally. One of the negative consequences of the global climate change is the increasing number and intensity of natural disasters, where the role of the military is more and more appreciated. For Hungary, as a small country and a member of the NATO, it is important to have a compact but capable military, which is able to work in a wide range of different scenarios of crisis management from peace support to disaster operations, especially in a multinational environment. This study introduces the disaster management capabilities of the Hungarian Defence Forces, focusing on the existing and planned international cooperations.

Keywords: Hungarian Defence Forces, climate change, disaster management, use of military force.

Introduction

There are plenty of hazard sources in Hungary which can cause disasters. Some of them immediately, and others by activating a series of secondary hazards. We can categorise them from several points of view. One way of grouping them is the following: [1: 118]

¹ Ph.D., associate professor, Department of Operations and Support, Faculty of Military Science and Officer Training, National University of Public Service; e-mail: tamas.berek@uni-nke.hu, ORCID: <https://orcid.org/0000-0001-8358-6139>

² Ph.D., professor, Department of Operations and Support, Faculty of Military Science and Officer Training, National University of Public Service; e-mail foldi.laszlo@uni-nke.hu, ORCID: <https://orcid.org/0000-0001-7575-7188>

³ DSc, professor, Department of Military Strategy, Faculty of Military Science and Officer Training, National University of Public Service; e-mail padanyi.jozsef@uni-nke.hu; ORCID: <https://orcid.org/0000-0001-6665-8444>

Hazards of civilisational origin:

- nuclear hazards (e.g. domestic nuclear energy installations, transportation of nuclear or radiological materials and consequences of nuclear accidents abroad);
- hazards of production, storage and use of dangerous goods (e.g. dangerous industrial infrastructure and hazardous waste);
- hazards of transportation of dangerous goods (on roads, railways, rivers and seas, by air, or direct or indirect effects of space technology).

Hazards of natural origin:

- hydrological hazards (floods, inland waters or droughts);
- geological hazards (earthquakes, different soil and rock movements);
- meteorological hazards (from extreme weather situations).

Hazards of human or ecological origin

- diseases (epidemic or pandemic situations);
- migration;
- proliferation of weapons of mass destruction and their delivery means;
- terrorism;
- ecological disasters (e.g. animal epidemics, forest- and wildfires)
- Practically, there is no such part of Hungary where hazards would not exist. Moreover, there are many areas where more than just one type of disasters can happen. Good examples are the industrial territories, where different types of dangerous materials are in use and at the same time the local population is dense. [2] The chance for disasters is further increasing due to more and more extreme weather events originating from global climate change.

Legal Background

In Hungary, the constitution guarantees the right of citizens to the safety of their life and wealth. From this, it is obvious that any organisations which can take part in disaster relief activities have the obligation to play an active role in it. It is true for the military, too. The history of military forces prove that every country needs this human and technical resource in disaster prevention and relief. On the one hand, the help from the military does matter in cases when local disaster management forces cannot handle the situation because of its severity. On the other hand, military involvement can be essential during disaster situations when special or customised capabilities and tools are needed to solve unique problems.

In Hungary, the *Act 128/2011. on the protection against disasters* and its related acts, together with some special departmental regulations (including those referring to the Hungarian Defence Forces [in the following: HDF]) essentially regulates domestic disaster management tasks and responsibilities and creates the legal base of the so-called “national disaster management system”. At the same time, continuous development of legal regulations concerning disaster prevention, relief and restoration, fine tuning of tasks and responsibilities, organisational and command structures are essential.

Concerning our military, disaster management tasks and responsibilities of the HDF are formulated in the *National Defence Departmental Disaster Management Plan*. [3]

Cooperation Issues

The complexity of disaster situations and the number of involved relief organisations demand significant cooperation on both command and execution levels. While planning and organisations are the main areas of cooperation in the phase of disaster prevention, efficient phasing of the on-site activities during disaster relief is the most important objective. Though particular tasks of cooperation can vary in different disaster scenarios, there are some basic principles. One of them is that it is practical to organise and maintain cooperation on the same level between the stakeholders. Another significant feature of cooperation is the utilisation of mutual benefits in prevention or relief of disasters. This requires continuous and timely exchange of information and synchronisation of tasks in time and space to avoid parallel (and thus redundant) work of partners.

Cooperation can be successful if it works proactively, that is, stakeholders should specify its purpose, location, time, involved forces, tasks, order of subordination and way of command in time, at the phase of prevention. It must be clear that cooperation is not a standalone, separate task, but a comprehensive approach for the whole defence. It is an integral part of the commandeering of troops because this can only be successful with joint, aligned actions of all stakeholders in disaster management.

Opportunities of the HDF

It is obvious that the primary tasks of our military force are the protection of the country's independence and compliance with alliance obligations. The constitution of Hungary clearly states that the Hungarian military takes part in disaster protection activities as a contributor, in other words, the HDF is a part of the national disaster management system. This is not an extraordinary obligation, almost every country uses this kind of human and technical resources. Of course, preparation for this task in organized manner is controlled by the regulations of the *National Defence Departmental Disaster Management Plan*. [4]

The *Defence Departmental Disaster Management System* (in the following: DDDMS) is a decisive element of the national disaster management system, it describes the details for planning, organisation, command and execution of the military's disaster management tasks. It contains all functions that the military provides during disasters. This continuously improving document lists all the temporarily generated, designated subunits which, based on the HDF's present capabilities, have the task to contribute in disaster protection inside (or, if it is necessary, outside) our national borders.

It is important to emphasise that there are many other tasks among the basic duties, so not the participation in disaster management is the primary function of the HDF. In a disaster situation, in a given time and place they take part in disaster relief operations, that is why these tasks are called "temporary services".

When situation is declared as “disaster danger”, these forces and equipment will be on standby. This means that they are prepared and also preparing their subunits and equipment to be capable to move onto the disaster site and start the assigned defence activities immediately in case of need. The military subunits involved in the DDDMS take part in thematic trainings and exercises regularly.

Let us see what kind of military units the DDDMS contains and what are their capabilities. [5: 4] We did not narrow down our investigation only to flood protection, because the majority of the subunits are multi-purpose, they can be alarmed and used in different types of disasters. This can be advantageous, as we know that disaster situations can be sometimes very complex. There is often not just one type of danger on the site, mainly because of the so-called “domino effect”. This means that a disaster can cause a series of other hazards (e.g. at Fukushima on 11th March 2011 the primary disaster was an earthquake, that raised a tsunami which caused a serious nuclear accident).

- *CBRN⁴ Area Control Centre (CBRN ACC) and CBRN Zone Control Centre (CBRN ZCC)*: They are to be established at national commands. CBRN ACC has to observe the CBRN Area of Observation, the borders of which are the national borders. In peacetime, the Area of Observation may be sub-divided into Zones of Observation in case of a natural or humanitarian disaster, and HDF Command appoints one or more CBRN ZCCs to assume responsibilities. Their main tasks include:
 - *Information Fusion*: The gathering of the information by sensors, observers and other CIS, which detect, identify and monitor CBRN incidents. The fusion of this information is expected to provide accurate and timely picture of CBRN incidents within the battle space.
 - *Analysis and Assessment*: The display, modelling and simulation of these CBRN incidents for the prediction of consequences for CBRN Defence. The use of these conclusions for the adoption of appropriate physical protection, risk assessment, hazard management, and medical countermeasures and support.
 - *Reporting*: The timely exchange of CBRN information/output between National CIS, National Control Centres (static and deployed) and NATO CIS in order to warn and report about CBRN incidents and their consequences.
 - *Filtering*: The filtering of information should result in processing and display of CBRN Defence situation that they have to be appropriate to the users at both tactical, operational and strategic levels. [6]
- *CBRN Survey Group*: Its tasks are reconnaissance of chemically or radiologically contaminated areas on land, checkup of chemical or radiological contamination of personnel, objects, materials and equipment, and proposals to determine methods of eliminating the consequences of the disaster.
- *CBRN Decontamination Group*: It has the task to perform thorough/operational personnel and material decontamination missions – including dress and individual equipment, vehicles, sensitive optical/electrical material –, and conduct fixed-site and terrain/road decontamination missions.

⁴ CBRN: This abbreviation stands for Chemical, Biological, Radiological and Nuclear (previously: NBC) issues in armed forces. Generally, it means the defence against Weapons of Mass Destruction (WMD).

- *Nuclear Early Warning System (NEWS) Support Group*: Its mission is to install mobil NEWS subsystems in directions of interest for increasing station density and/or support critical objects.
- *SCUBA Diving Group*: Its missions are:
 - Reconnaissance, strengthening and insulation of dams from the direction of the water in case of floods.
 - Underwater survey of damaged flood protection structures.
 - Participation in removal of damaged flood protection structures (demolition tasks).
 - Participation in life and wealth rescue operations during water transportation accidents.
- *Biological Diagnostics Group*: Its mission is to analyse biological samples collected and sent from the site to detect possible causative agents. It includes a Mobile Biological Laboratory Complex with complete staff and equipment.
- *Lifting Machinery Group*: It has the mission to load and unload transport vehicles with the necessary flood protection materials (sandbag, gabion, straw bale, etc). It also participates after earthquakes in ruin removal operations and personnel rescue missions when people are trapped under ruins, restoration of public utilities and wrecking works. It provides assistance in loading and unloading military transport railway trains and lifting heavy objects and materials.
- *Epidemiologic Group*: Its task is the epidemiologist work on site under the supervision of the military chief epidemic officer. On-site control and survey, necessary countermeasures and sample taking in case of need.
- *Medical Group*: Its main task is to provide primary life-saving and professional on-site medical first aid.
- *Electric Power and Lighting Supply Group*: Its mission is to support disaster relief forces providing electric power and lighting.
- *HAVARIA Laboratory*: Its mission is to recon chemical or radiological contamination in case of industrial disasters, to measure the range of contamination and its borders, and qualitative and quantitative analysis of released hazardous chemical or radiological materials. Its experts give proposals to determine complex methods of eliminating the consequences of the disaster.
- *Light Geoworks Machinery and Ruin Removal Group*: Its task is to perform different soil mobilisation works.
- *Delivery Group*: Its main task is to transport personnel.
- *Light Water Transporter/Medic and Waterways, Water Area Locking Support Group*: Its mission is to perform and assist in transportation and rescue tasks on water.
- *Air Support Group*: Its mission is to perform air reconnaissance and survey of disaster sites, rapid transportation of the wounded to hospital, support closed or occluded areas with food and medication, airborne search and rescue from occluded or life threatening sites, dam strengthening from the air and participation in firefighting.
- *Airborne Radiological Reconnaissance Group*: It has the mission of fast reconnaissance of radiologically contaminated area in case of nuclear disaster, including reconnaissance of large contaminated areas (with the effectiveness of ca. 300 km²/h), searching for separated radioactive sources and limited identification of radioactive isotopes.

- *Mobile Medical Group*: Its mission is to give medical attendance with their professional equipment to the wounded and make them transportable from the disaster site.
- *Heavy Geoworks Machinery and Ruin Removal Group*: Its task is to perform different soil mobilisation works.
- *Heavy Amphibious Rescue Group*: Its mission is to carry out transportation and rescue on heavy terrain and on water during floods.
- *Vaccination Group*: Its task is the immunisation of the designated personnel with its equipment and giving certificate of inoculation under the supervision of the military chief epidemic officer.
- *Medical Support Group, Hospital Bed Capacity*: Its task is to provide special medical care on a detached 100-bed hospital capacity.
- *Psychologist Advice Group*: Its mission is to provide psychological support to the military personnel involved in disaster relief and prevention against Post Traumatic Stress Disorder (PTSD).
- *Military Police Group*: Its mission is to provide police support and convoy escort to and from the accident site in case of the use of a larger military force.
- *Demolition Group*: Its mission is to carry out demolition works (in ice, soil, objects and buildings) and cutting with explosives.
- *Radiation Health Protection Laboratory*: Its mission is to carry out radio-medical control, give proposals to decision-makings and to the necessary countermeasures.
- *Personnel Transport Group*: It consists of five buses with drivers.
- *Transport Towing Group*: Its mission is to transport materials and valuables and tow damaged vehicles.
- *Land Area and Road Closing Support Group*: Its task is to close or secure areas or roads on disaster sites, extremely important for defence and unobstructed movement.
- *Field Support Group*: Its task is to give full logistic support on field for 200–250 persons involved in disaster relief (meal, bed, electricity).
- *Winter Emergency Response And Rescue Group*: Its mission is to rescue lives and valuables in case of extreme weather emergencies during wintertime, including rescue of public transport vehicles and cars with passengers stucked in snow, cleaning of important road crossings, transportation of wounded or sick persons to hospital and support of closed or occluded areas with food and medication.
- *Manual Defence and Wrecking Working Group*: Its task is to strengthen dams and remove ruins and wreckages with hand tools, fill-up of soil and sandbags and their hand delivery, participation in lookout service, rescue of lives and valuables under the supervision of the on-site commander. It includes 50 persons and 3–4 all-terrain vehicles. The group is capable to fill sandbags with a performance of 800 pieces/hour and deliver sandbags within 5 metres to vehicles with a performance of 2500 pieces/hour.
- *Water Transportation Group*: Its mission is to support the strengthening and insulation of dams from the direction of the water in case of floods, delivery of materials, support of rescue operations on areas flooded by water, and the operation of cargo ferry.
- *Water Purification Group*: Its mission includes water retrieval, water purification and to provide both the disaster relief forces and the population with drinking water.

- *Tracked Winter Emergency Response and Rescue Group*: Its mission is to rescue lives and valuables in case of extreme weather emergencies during wintertime in areas impassable for wheeled vehicles. Its tasks include rescue of public transport vehicles and cars with passengers stucked in snow, cleaning of important road crossings, transportation of wounded or sick persons to hospital and support of closed or occluded areas with food and medication.
- *CIMIC and PSYOPS Group*: Its main task is to inform both the disaster relief forces and the population about the current disaster situation. It includes seven persons (four officers, three NCOs) and three MG G270 cross-country vehicles (one of them is the PSYOPS multimedia car). The group is capable to make CIMIC databases and analyses on their area of responsibility, and to provide and hand over their connection network and database to the experts of on-site disaster relief subunits.
- *Non-conventional Transport and Escort Group*: Its mission is to transport special personnel and technical equipment, escort convoys and oversized vehicles.
- *Airborne Radiological Reconnaissance Patrol*: Its mission is to carry out airborne radiological reconnaissance with its regular equipment.
- *CBRN Casualties Decontamination Group*: Its task is to decontaminate and attend civil and military casualties rescued from territories contaminated with hazardous chemicals, radioactive or biological agents.
- *Salvager and Transloader Group*: Its task is to transload liquid hazardous chemicals on site from damaged containers to elastic tanks.
- *Water Sucking and Pumping Group*: Its mission is to participate in cleaning terrain elements covered by water (roads, ditches, tunnels, buildings, houses) by sucking and pumping water.

We can see that military troops can provide such a large-scale assistance during disaster relief activities as no other rescue organisations in our country. They can operate with full logistic support capability, which means that involved military forces can supply themselves, so their application does not generate any need of subsequent capacities. Rapid mobilisation, special equipment, skilled personnel together with full logistic support capabilities increase their value even further.

The “Tisza” Multinational Engineer Battalion

The tasks of the joint Hungarian–Romanian–Slovakian–Ukrainian subunits of the “Tisza” battalion are:

- prevention of floods or other natural disasters, ecological catastrophes on the catchment area of River Tisza;
- direct intervention to help the local population;
- taking part in disaster relief operations (damage reduction and/or elimination).

The staff of this temporary military organisation consisting of four engineer companies holds exercises every year. The battalion and its equipment is specially organised and shaped in order that in case of floods the capabilities effectively intervene, save lives and

strengthen damaged dams. Every time, the commander comes from the effected country where the exercise is held or the disaster relief works are done. [7]

The Hungarian company of the “Tisza” battalion consists of 154 persons. Its decisive subunits are:

- *Sapper Platoon*: It is capable to provide reconnaissance data or refine existing data, operate cargo ferry or rescue lives and valuables with its assault-boats. Its water purification section is capable to support both the forces involved in the disaster relief and the affected local population with potable water in case of the damage of public utility services. With their bagging equipment the potable water can be packed and dispensed without any risk of infection.
- *Assault Water Crossing Platoon*: It is capable to rescue 840 persons or 60 tons of materials at a time or transport 1200 sandbags to the defence site.
- *Pontoon Platoon*: Its mission is to rescue and transport heavy materials and technical equipment on water.

Additional subunits coming from other nations’ armed forces into “Tisza” battalion are the following:

- *Slovakian Engineer Company*: It has two sapper platoons, a pontoon platoon, a road building platoon and a logistics platoon with 150 soldiers.
- *Romanian Engineer Company*: It consists of a bridge building platoon, a pontoon platoon, an assault water crossing platoon, a road building platoon and a logistics platoon with 168 soldiers.
- *Ukrainian Engineer Company*: It has an engineer platoon, a bridge building platoon, a road building platoon and a logistics platoon with 163 soldiers. [8]

Developments

Capability development of the Hungarian Defence Forces is continuous even in the field of disaster management. An important phase of this procedure is the latest procurement of disaster relief equipment carried out with an almost 6 million EUR financial support from the European Union.

Thanks to the support of the European Union Cohesion Fund and the Hungarian government as co-financer, this development will help the Hungarian Defence Forces to provide assistance in disaster management on higher standards in prevention and elimination of natural disasters including floods. The project will be realised with a total budget of 2.215 billion HUF (6.5 million EUR) with a 100% of EU support of 2.005 billion HUF (5.9 million EUR). With this investment, the Hungarian Defence Forces carries out a large-scale equipment modernisation needed for its participation in disaster management activities, mainly in flood protection.

With this development, the Hungarian Defence Forces will be able to maintain all of its previous contribution capabilities in disaster management and to increase their performance. Besides this, the Hungarian Defence Forces contributes to the development of the capabilities of the National Disaster Management System with its enriched performances. [9: 7] The modernisation of its command and control system and the infocommunication capabilities

of its intervening subunits will make the field cooperation with other organisations' units easier and better.

Development of informatics and office technical equipment, procurements of digital radio transmitters and portable field chemical identification devices will be carried out in the project. Besides the individual protective gears used in flood protection, high delivery pumps, field camp lighting systems, dinghies and outboard motors will be put into service. Renewal of old amphibious vehicles used in flood protection, suitable for the rescue of the population, will be carried out to improve their capabilities of food and drinking water supply. In addition, modification and modernisation of the fuel supply system and capability improvement of field tent quartering are to be realised.

Procurement of technical devices includes the following:

- high delivery gasoline-powered portable sloop pump and high delivery gasoline-powered portable drinking water pump;
- field camp lighting system mounted on truck trailer;
- industrial diving suit;
- light diving suit;
- dinghy with outboard engine;
- outboard engine (four strokes engines with 30 BHP);
- average performance universal engineer geoworks machine;
- life vest and life-ring.

In addition to these, renewal of eight PTS-M (PTS stands for Plavayushchij Transportyer – Sryednyj = medium amphibious transport vehicle) tracked amphibious vehicles has been started, that can be involved not only in flood protection but also in extreme winter weather emergency relief activities. The newly procured heavy transport trailer is perfectly suitable to their transport to the disaster site. Another result of the development is the renewal of a fuel transport truck and eight trailers with one cubic meter of water tanks.

Conclusions

The described system has been continuously developed for years, but it is obvious that there are still some areas that should be improved. Monitoring of international results is important to gain opportunity to implement new solutions, for example in the command and control system, in special equipment, or training and exercise.

One thing is for sure: protection against disasters cannot be privatised either by organisational or individual ambitions. This task can be successfully and effectively solved only in cooperation, systematically using all of the resources that we altogether have, and utilising existing synergies.

We can be sure that hazards of serious floods will increase due to the consequences of global climate change. Not the yearly amount of precipitation will be higher, but the precipitation pattern is changing, including more and more extremities recently. Longer dry periods are predicted followed by shorter but more intensive rainy periods, often with extreme rainstorms and thunder showers. Meteorological experts forewarn us of increasing chance of supercell

formation. [10] All of these can cause higher flood peaks on any of our rivers. We cannot raise the altitude of our dams higher and higher every year, so the risk of floods will increase and useful capabilities of intervening relief forces will become more valuable.

References

- [1] SCHWEICKHARDT, G.: *A katasztrófavédelem rendszere*. [System of disaster management.] Budapest, Dialóg Campus, 2018. https://akfi-dl.uni-nke.hu/pdf_kiadvanyok/web_PDF_EKM_A_katasztrofavedelem_rendszere.pdf (Downloaded: 19.02.2020)
- [2] HORNYACSEK J. – KESZELY L.: A katonai erők, képességek alkalmazása katasztrófák esetén. [Application of military forces and capabilities during disasters.] *Hadmérnök*, 8 2 (2013), 191–209. www.hadmernok.hu/132_18_hornyacsekj_kl.pdf (Downloaded: 25.01.2020)
- [3] 62/2014. (IX. 26.) HM utasítás a Honvédelmi Katasztrófavédelmi Rendszer Szervezeti és Működési Szabályzatának kiadásáról. [Decree of the Minister of Defence No. 62. on 26th September, 2014 about the Regulation of Operation of the Defense Departmental Disaster Management System.] <https://net.jogtar.hu/jogszabaly?docid=A14U0062.HM&txreferefer=00000003.TXT> (Downloaded: 24.01.2020)
- [4] Megújul a Honvédelmi Katasztrófavédelmi Rendszer eszközparkja. [Equipment of the Defence Departmental Disaster Management System is renewing.] *Honvedelem.hu*, 2016. https://honvedelem.hu/cikk/59555_megujul_a_honvedelmi_katasztrofavedelmi_rendszer_eszkozparkja (Downloaded: 26.01.2020)
- [5] CSURGAI, J.: The New Disaster Management System of the Hungarian Defense Forces in the Light of Climate Change with Special Emphasis on Nuclear Accidents. In KRULÍK, O. – PADÁNYI, J. – RATHAUSKÝ, Z. – ŠESTÁK, B. eds.: *Climate Change and its Security Impacts: Proceedings from the International Scientific Conference*. 18th and 19th September 2019. Prague, Policejní Akademie České Republiky v Praze.
- [6] *ATP-45(D) – Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Reference Manual)*. NATO NSO STANAG 2103.
- [7] PADÁNYI, J. – FÖLDI, L.: Tasks and Experiences of the Hungarian Defence Forces in Crisis Management. *Bilten Slovenske Vojske (Contemporary Military Challenges)*, 17 1 (2015), 29–46.
- [8] SOMLAI-KISS A.: A TISZA Többnemzeti Műszaki Zászlóalj bemutatása különös tekintettel az árvízvédelmi szerepére. [Introduction of the TISZA Multinational Engineering Battalion with special emphasis on its role in flood protection.] *Műszaki Katonai Közlöny*, 21 Special editions (2011), 992–1006.
- [9] PADÁNYI, J. – FÖLDI, L.: Military Technical Developments in Hungary in the Frame of ZRINYI 2026 Program. In KŘIVÁNEK, V. ed.: *2019. International Conference on Military Technologies (ICMT)*. Brno, IEEE, 2019. 1–7. DOI: <https://doi.org/10.1109/miltechs.2019.8870061>
- [10] HALÁSZ, L. – FÖLDI, L.: New tendencies in global climate change and their effects on the climate of Hungary. *Hadmérnök*, 14 1 (2019), 99–107. www.hadmernok.hu/191_09_halasz.pdf (Downloaded: 18.02.2020)

Erasmus and István Magyari on the Justification of War¹

Mihály BODA²

Warfare ideologies in Europe basically changed in the Early Modern period. This period is the age of Reformation, of which Desiderius Erasmus was one of the earliest prominent thinkers. Concerning warfare, Erasmus can be understood as a representative of pacifism, but at the same time, it can be argued that he was the first reformer with a specific theory of justification of war. In this respect, Erasmus had several followers from every part of Europe, including Hungary. This Hungarian “apprentice” was István Magyari, who was also the first representative of Hungarian military science. This paper uncovers and examines the common points of Erasmus and Magyari in their theory of justification of war, and Magyari’s divergence from Erasmus’ thinking.

Keywords: *justification of war, just war theory, Erasmus, István Magyari*

Introduction: Just War Theory in the Middle Ages

In order to examine reformers’ warfare ideologies I will build on a specific theory, the just war theory in the form crystallised and systematised by the 13th century by Thomas Aquinas. [1: 171–177] Although, this theory is characteristically Catholic in its content, I can set aside this Catholic content and focus exclusively on the formal features of the theory. The reformers themselves knew and employed the same features within the framework of the theory without accepting the claims of Thomas Aquinas or other Catholic thinkers.

The formal features, steady-state by the period of the reformers (by the turn of 15th–16th centuries), are the following: the thinkers of the Early Modern period more or less accepted that there is significant difference between the lawfulness of initiating a war on the one hand, and the lawfulness of waging a war on the other hand. Since the middle of the 20th century specific terms—*ius ad bellum* and *ius in bello*—have been applied for these forms of justice. Thomas Aquinas listed three rules as *ius ad bellum* rules: the rule of legitimate authority, according to which only the prince was authorised to initiate war; the rule of just cause, according to which war is permitted to initiate only for punishing the breakers of peace and hence to defend peace; and the rule of right intention. The latter rule has two interpretations for Aquinas, the first concerns the extension of Christian peace as the further

¹ This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

² Ph.D., associate professor, University of Public Service; e-mail: Boda.Mihaly@uni-nke.hu; ORCID: <https://orcid.org/0000-0003-3037-3644>

purpose of war, and the second considers the right intention rule as the rule of waging a war with charity (and not, for example, hatred or anger). Only the former interpretation of the right intention rule fits into the requirements of *ius ad bellum*, the latter one is a rule of *ius in bello*.

Erasmus on the Justification of War

Many different standpoints can be supported on the question “What is the moral value of war in general?” One is the theory of realism, according to which war is good as a tool if it helps to satisfy the interest of the state. A completely different point of view is pacifism, according to which war cannot be good at all, because it always goes hand in hand with several deaths and serious suffering of human beings. Erasmus, contrary to his contemporaries Machiavelli and Gentili, is often shown as a representative of pacifism; his work principally referred to is *Dulce bellum inexpertis* (*Against war*, 1515). [2] However, the content of Erasmus’ other works suggests a not completely pacifist standpoint, because these works take the point of view of justifying defensive and offensive wars.

Erasmus deals with the problem of justification of war in detail in his *Querela pacis* (*A Complaint of Peace*, 1517), [3] *Consultatio de bello turcico* (*On the War against the Turks*, 1530), [4] and *Institutio principis christiani* (*The Education of a Christian Prince*, 1532). [5] In justifying war he draws a distinction between defensive and offensive wars on the one hand, and between wars of one Christian prince against another, or the wars of Christian prince(s) against non-Christians, on the other hand. Erasmus takes defensive wars justified if the just cause is the protection of the community against another Christian prince (which is a form of law enforcement), or against a non-Christian prince – actually against the Turks (which is defending Christianity. [3: 314] The ideas in both cases are based on the argument that the prince serving the Christian peace and community has the right to punish those who committed something wrong against the community, and hence he has the right to defend the community against internal and external dangers, which one can find in Aquinas as well. [6: 221–224] Erasmus, however, dealt much more with the frameworks of justifying offensive wars than defensive ones. In the following I examine Erasmus’ ideas on offensive war between Christian princes, and between Christian and non-Christian princes.

Erasmus, starting from the practice of his contemporary princes’ wars against each other, and the humanist warfare ideologies, considers that wars of Christian princes against each other are totally unacceptable and forbidden. What was the specific princely ability of *virtus* with the objective of satisfying interest of the state, was for the humanist thinkers the example of princely ambition and satisfaction of princely self-interest. Erasmus writes: “One [prince] discovers or invents some mouldering, obsolete title to support his claim [...] Another pleads some trifling omission in a treaty covering a hundred clauses, or has a personal grievance against his neighbour over the interpretation of an intended spouse or a careless word of slander. Most criminally wicked of all, there are rulers who believe that their authority is undermined by harmony amongst their people and strengthened by discord, so they use their despotic power to suborn persons who will set about stirring up war; [...] There the worst sort of criminals, men who thrive on the sufferings of the people, and in time of peace find little to do in society.” [3: 305–306]

That is, princes do not have any worthy aims for which one is morally permitted to unleash a war. Erasmus, setting aside this problem, emphasises that breaking peace in accordance with any—just or unjust—cause or aim has very serious consequences. In the opening paragraph of *A Complaint of Peace*, the “Peace” complains that men take peace as a source of every human happiness, but contrary to this, princes too easily turn to war, which “is a kind of encircling ocean of all the evils in the world”. [3: 293] War is basically antihuman for two reasons: because it is contrary to human nature, and because it destroys human civilisations built up in peace.

According to Erasmus, independently of how we define human essence, taking men as members of nature, or subjects of Christ, war in both cases is contrary to human essence. In nature, harmony characterises the relationships within the species of wild animals, and of the planets, so men, too, should live in harmony with each other. Men, with the help of their naturally given reason, can understand that their essence predestined them to lead a peaceful life based on agreement. Nature did not give to human beings abilities (natural weapons) by which they can manage their life alone, but from the very beginning of their life, they are in the need of help. [3: 294–296]

We should draw the same conclusion from the supposition that men’s Christian features are more important than their natural endowments. Since Jesus Christ is the prince of peace, and the Christian God is god of peace, the purpose of Christian princes should be to live in a Christian way, and to build and sustain the peace in their countries and in the relations with their potential enemies. [3: 299] Hence, the further aim of every truly Christian politics is to establish the communion of every Christian men and to progress on the way to the eternal salvation and immortality, which is the “indefinable communion of happy spirits”. [3: 320]

Therefore, war is antihuman in nature for it is contradictory with the essence of men, and for another reason, too: war demolishes the fruits of peace. However, the purposes of wars are the princes’ selfish purposes, every devastating consequences of wars are incumbent on the people and the country. War demolishes the laws, inner discipline and religious purity of citizens, moral chastity of the country, and the villages, the cities and the temples; it makes the fields of the country being desolated, and releases crimes and outrage of mercenaries in the country. [3: 316–317] According to Erasmus, these consequences are independent of the prince’s moral stance, or of the just or unjust nature of the cause of war. The “war is by its nature such a plague to man [...] results in almost more evil than good”. [4: 318]

According to Erasmus, wars between Christian princes have only natural causes—foolishness, anger and ambition—, [3: 305, 310] and never have just causes. It is a real possibility, however, for the prince to consider whether he should initiate a war or not. In this consideration, the prince should take into account such features, according to Erasmus, which did not gain much attendance in the Middle Ages. These features are the modified rule of legitimate authority, the rules of proportionality, of last resort, of reasonable chance of success, of declaration, which the previously already acknowledged rule of right intention joins. These rules constitute the rules of the Erasmian *ius ad bellum* of offensive war, with the absence of the rule of just cause. These two conditions, i.e. the lack of the just cause and the presence of other rules, show that war is always wrong from moral point of view (because war never has a just cause); some wars, however, can be justified as “lesser evil” (because rules other than just cause can morally vindicate them).

A part of these rules, particularly the rules of extended legitimate authority, of proportionality, of last resort, and of declaration, became important in the Early Modern period for Erasmus and for others, because the religious justification of war receded by that time. While the content of the just cause was defined with the help of purposes, commands, and intentions of God, these other rules were relatively uninteresting, because God's aims are incomparable with human casualties, so the war could not be for example disproportional. Since, however, causes of war were redefined in terms of human purposes, the prince should have made good decisions with the help of the potentially affected people, and by comparing the alternative ways of conflict management.

With the help of the rule of legitimate authority, Erasmus wants to emphasise that a Christian prince should consider the possibilities and make a wise decision before he initiates a war, and the prince should not pay attention to his passions. That means, Erasmus supposes that the prince has the right to start a war, [3: 282–288] however, he acknowledges the limits of this right as well. The prince should ground his decision on the wise advice of those who are old enough to give advice (because younger people usually like the idea of war), who are respected by the common people, but who are not interested in the turmoil caused by war. [3: 313]

Erasmus gives another restriction of legitimate authority with the rule of declaration. He thinks the causes of war should be made public immediately in order that perhaps somebody can give an “excuse” for avoiding war. [3: 313] The wise advice or the excuse coming from the advisers or the common people are in connection with the loss and gain of the war and so the general rule of proportionality of *ius ad bellum*.

The rule of general proportionality includes three different rules. These are the rules of reasonable chance of success, of last resort, and of particular proportionality. All these rules contain some element of proportionality, so the prince and his advisors considering them should think about the following: whether the purpose of war can be reached at all or there is no chance; if it can, then whether it can be reached only by war or by other, more peaceful means, too, which results in less losses; and if not, then whether the suffering brought about by war is proportional to the positive value of the cause of war (whether it results in more good than bad consequences, supposing the success).

The rule of reasonable chance of success requires the prince and the advisors to consider the possible ends of the war before the attack, and whether the reasonable possibility of winning the war exists or not. [5: 282–283] If one cannot suppose such a possibility in a reasonable way then the war can be heroic or self-sacrificing, but it cannot be justified because there are not any good consequences over against the caused suffering and deaths, it is extremely disproportional.

The rule of last resort demands the prince and his advisors to take into consideration all the means which can be applied in conflict management, by which the war can be avoided, and not just the possibility of war. Erasmus mentions two such alternative possibilities: appointing arbiters, [3: 310–311] and buying the peace. [3: 313] By considering these possibilities, the prince and the advisors should compare the good and bad consequences of these possibilities with those of war. For example, thinking about buying the peace for a sum of money should be taken into account (the former is the gain and the latter is the loss for the country), and the good and bad consequences of buying the supposedly successful war expressed in a specific sum of money, which sum may be more advantageous to be chosen.

The rule of particular proportionality has its own significance, because it requires the prince to think about and compare the good and bad consequences of bringing about the war. According to Erasmus, the bad consequences affecting the people who do not have influence on starting the war (the peasants and the poor) should be weighted. [3: 312] One extreme case can be that in which there is no chance to attain the purpose of the war, because in this war even a minimal loss makes the war disproportionate.

Finally, before initiating a war, the prince and his advisors should consider the further purpose of war which can be reached by the war. This is the rule of right intention, which has a very specific position in the theory of Erasmus. Since the purpose of Christian princes cannot be other than to build and sustain the empire of Christ and peace in the created world, Christian princes are not morally permitted to wage a war against each other. The rule of just cause is missing from Erasmus' theory for this reason, due to the Christian rules of right intention.

Offensive wars against non-Christians, however, constitute another sort of wars, because according to Erasmus, Christian princes are morally permitted to start a war against non-Christians, particularly the Turks. What is the reason for initiating a war against the Turks? Erasmus writes: "But perhaps it is the fatal malady of human nature to be quite unable to carry on without wars. If so, why is this evil passion not let loose upon the Turks? Of course it used to be thought preferable, even in their case, to win them over to the religion of Christ by teaching and by the example of good deeds and a blameless life rather than by mounting an armed attack. But if war, as we said, is not wholly avoidable, that kind would be a lesser evil than the present unholy conflicts and clashes between Christians." [3: 314]

At first sight, this text takes conflicts, and wars specifically, as an integral part of human life, and perhaps Erasmus thinks that wars are unavoidable, so wars should be started against the Turks and not against other Christian princes.

However, some arguments can be put forward against this interpretation. We saw earlier how Erasmus defines the nature of human beings with the help of the concepts of harmony, cooperation, and peace. This definition does not include conflict and war as natural phenomena, so the above text cannot be interpreted contrary to this.

Furthermore, I mentioned above that according to Erasmus the princes in fact initiate wars for their self-interested purposes, for example, when a prince behaving as a tyrant unleashes a war to keep his subjects busy. Erasmus condemns this practice and such cause of war. On the basis of the cited text Erasmus may be supposed to suggest something similar to exhorting against the Turks. I do not think so.

The text, I claim, should be interpreted in the light of Erasmus' specific view on the Turks. According to Erasmus the Turks are more inferior people than Christians. Turks are naturally lovers of luxury, and for this reason self-indulgent people, who are inclined to robbing lifestyle (for taking others' property arbitrarily), to avarice, envy, ambitiousness, greed for power, anger, and hatred. [3: 324] However, Turks are still better and more superior than Jews and black Africans, because Turks in their religious believes are close to Christians, so they are "half-Christians". [3: 317; 7]

For this reason it can be supposed that Erasmus exhorts for an offensive religious war against the Turks for conversion, which war would be a "lesser evil". I think the cited text of *A Complaint of Peace* can be explained in this way. This interpretation is supported by another work of Erasmus, *On the War against the Turks*.

According to Erasmus, there are preconditions for conversion. The conversion of the Turks to Christianity can be successful if Christians take Christianity seriously, practice it and set an example for Christian life to the Turks. Conversion can be successful in this case only. Of course, it is possible that the princes of the Turks do not want to respect Christianity and resist to peaceful conversion. This time Christians can convert the Turks to Christianity by force. But for Erasmus, peaceful attempt of conversion is a precondition of forced conversion, which in this way can be initiated as last resort.

Erasmus writes in 1530, after the Turkish siege of Vienna in 1529: “It is no longer a case of sharing these disasters because of our common religion, but because there is a danger now that we may soon share them in reality. ‘When your neighbour’s wall is in fire it becomes your business’; in fact, it becomes the business of the whole city, whenever a single house catches fire. Therefore we must give assistance if we are truly anxious to rid ourselves of this peril; but assistance of two kinds. Of course, we must make all the preparations necessary for such an arduous war, but before that we must make the preparations without which military strength will be in vain.” [4: 316]

Christians, for initiating war, need military preparation; for military preparation, however, they need to be prepared in faith. Preparation in faith means taking seriously, purifying and reforming the practice of religion, and together with this, settling the conflicts of Christian princes. In *A Complaint of Peace* Erasmus supports this claim by demanding reform of the practice of religion as a necessary condition of peaceful conversion. In *On the War against the Turks* he argues on another track. The change in the argument is due to the changes in the political circumstances of his time: the Turks defeated the Hungarian king on the battlefield in 1526, and then sieged Vienna in 1529.

According to the second argument, the cause of the successes of the Turks, for example that they reached the capital of the Habsburg Empire, is the sins of the Christians, and not the Turks themselves. God punished Christians for their inner conflicts by having allowed the Turks to win over the Christian armies. [4: 316–317] Hence, the military preparedness alone is not enough against the Turks. If it is not complemented with preparedness in faith, then the Turks will defeat the Christian army again. Therefore reforming the practice of religion is a necessary condition of the successful fight against the Turks, and at the same time the necessary condition of their (peaceful or forced) conversion. By this, the rule of right intention can be completed as well. [4: 324]

To sum up Erasmus’ position on the problem of justifying an offensive war we can state that the starting point of Erasmus is the understanding of the concept of Christian peace, and that this peace should be secured in Europe among the Christian princes, and as far as possible, in the Ottoman Empire as well. Erasmus accepts the “just war” position of his predecessors regarding defensive wars, but he determines new claims concerning one part of offensive wars. Referring to the wars among Christian princes, Erasmus emphasises that wars are unjust and so cannot have just causes, but can be morally permitted under other rules, so wars can be justified as a “lesser evil”. The other part of offensive wars are the wars of conversion whose justification depends on whether Christians can suit themselves to the principles of Christianity by living a peaceful life, setting an example of Christian life to the Turks. If this example does not have any outcome on the side of the Turks, then, as a last resort, Erasmus regards offensive wars of conversion against the Turks morally acceptable.

Erasmian Elements in István Magyari's Theory of Justification of War

István Magyari (1565–1605) was a Hungarian military scientist, baron Ferenc Nádasdy's court chaplain, then deacon in Sárvár (Hungary), who dealt with the problem of justification of war in his book *Az országokban való sok romlásoknak okairól* (1602, *On the causes of the many decays of the countries*). One can find in the focus of his book the idea that the attack and success of the Turks (in Hungary in the 16th century) are God's punishment on the Christians for their sins. According to Magyari these sins are the clear consequences of the Catholic lifestyle, among others idolatry. Magyari lists protractedly the examples of Catholic idolatry, like respecting molded and carved pictures, reclusory, nunship, specific masses, clothes of priests, or the ostentatiously furnished temples. [8: 32–33] Magyari, however, has the remedy for the decays of the country, on which he writes in the fourth chapter of his book.

Considering the nature of the remedy for decays, Magyari is a disciple of Erasmus: he refers to Erasmus *expressis verbis*, and the structure of Magyari's book is similar to that of *A Complaint of Peace*. Apart from the many similarities, however, there are some differences as well.

Magyari thinks that the promotion of selfish aims is the main motivation of warfare in his age, by which hence princes do not intend to protect the common good of the community. Since the good of the community has greater value than selfishness and it can be promoted first of all in peace, Magyari condemns warfare. [8: 154, 157] The condemnable character of war emanates from the nature of human beings, and the harms caused by wars.

According to Magyari, God created human beings for fellowship, which can be seen from the fact that men, similarly to wild animals, do not have natural weapons. Men are naked, without weapons, and so helpless, unless they receive assistance from others. [8: 157] This one train of thought includes Erasmus' ideas on the natural and Christian essences of men together. As far as the harms caused by war are concerned, Magyari thinks laws lapse in war, so the extent of unlawfulness increases, and people and their property decay. The community suffers a lot of harms, and becomes impoverished. [8: 158–159]

So far Magyari has strictly followed the ideas of Erasmus, however, here he comes to the discussion of the just and unjust causes of war and takes the position of just war theory, in which he somewhat dissents from the point of view of Erasmus. [8: 153]

Magyari defines just causes indirectly, by defining the cases of unjust causes: it is unjust if the prince initiates a war but does not defend the faith or the country, or does not help the neighbor to defend his country. [5: 159] This implies the just causes of war, which is called by Magyari "worthy" and "necessary" causes, namely defending the Christian faith, defending one's own country, or helping to defend the neighbouring country.

Just and "necessary" causes include principally the self-defence of a community (the Christian community, or the country), or as it is said nowadays, the protection of the rights of the community. This perspective on just war theory is very different from the medieval form of the theory, according to which just wars are first of all a form of law enforcement and not right-protection. Therefore, Magyari dissents from Erasmus' theory of justifying defensive wars, because Erasmus grounds his theory on the medieval theories (primarily the theory of Thomas Aquinas).

Comparing Magyari's list of just causes to that of Erasmus, the lack of offensive causes is conspicuous, first of all the conversion of the Turks. This is because while Erasmus wrote at the beginning of the 16th century when the Turks had just conquered a great part of Hungary, Magyari worked at the end of that century, during the Fifteen Years War (or Long Turkish war) (1591–1606). This war had escalated from skirmishing activities on both sides, and developed to a defensive war of the Habsburg Monarchy. So, the corresponding warfare ideology was not offensive, e.g. converting the Turks, but a defensive one.

According to Magyari, the prince has legitimate authority: that is the right and duty of the prince to consider the justness of the causes. However, the prince should represent his people. Magyari compares Hungarians to the Jews with the help of the texts of the Bible and the Old Testament. He thinks Hungarians are God's chosen people, like the Jews were, who are now being punished by the Turks. The purpose of punishment is to redirect the chosen people to the right way of faith, so to give up idolatry. [8: 138–139] At the same time Magyari finds it important to follow the examples of the past pagan and Christian kings, too [8: 124], to the extent it is not in contradiction with the commands of God. People must not follow that rule of the kings which contradicts to the commands of God. [8: 140]

If a prince has a just cause to initiate a war, namely to defend the faith or country, then the prince is supposed to consider the consequences of war, namely the harms possibly caused by the war. If the harm is much more compared to the just purpose of the war, then the war must not begin. This rule is the rule of general proportionality of *ius ad bellum*. [8: 159] Magyari, unlike Erasmus, does not discern the different forms of the general rule, the rules of the reasonable chance of success, of last resort, and of particular proportionality.

If the war has a just cause and it is proportional, too, then it is important for the prince to initiate the war with the intention defined by the just cause. Magyari forbids those wars which are grounded on envy, pride, hatred, conceit, or are waged for glory, wealth, or building an empire. He takes crusades, the offensive war for conversion, against the Turks as such wars. [8: 159] This sort of the rule of right intention includes the form which is mentioned by Thomas Aquinas, namely, Christian soldiers should fight against the enemy with charity, for the salvation of the enemies. This rule was a *ius in bello* rule in the Middle Ages, and the purpose was to secure a possibility for the Christians to be soldiers. In Magyari's theory this rule gets a new interpretation, and becomes a *ius ad bellum* rule, according to which the content of the prince's intention to initiate a war should suit to the content of the just cause. To put it in another way: a just war should be waged without ulterior motives.

The other form of medieval rule of right intention is that initiating a just war, the prince needs a peace conception which includes the enemy who will be defeated; this, as a further purpose, is prescribed by Magyari as well. The proper peace conception for him is characterised by the absence of Catholic ("papist") idolatry, and it is the peace which returns to the direct respect of God, the peace of "Jewish Christianity". [8: 138–13]

Magyari, like Erasmus, does not have much to say on the rules of waging war, *ius in bello*, because both thinkers understand war as bringing about demolishing consequences. However, Magyari mentions a specific subject, the problem of preparing for a just war: before the prince initiates a war, he needs to build an army by which he can have

a just fight with chance against the enemy. The just building and training of this army is called *ius ante bellum* in our age.

According to Magyari, four sorts of rules should be taken into account in *ius ante bellum*: the rules of everyday life of soldiers (which result in a specific soldiers' ethics); the rules of restoring and maintaining the valour of warriors; the rules of supporting the elements of artificial courage (which are the major part of soldiers' ethics); and finally the rules of civil-military relations of that age (which are needed regarding the differences between the "old" civil ethics and the new military ethics).

Based on these sorts of rules, the armed forces should be built in a way that its soldiers should have "proper discipline", which prevents them from wandering about at their will. [8: 133] Hence, soldiers are supposed to live in barracks in order not to disturb the peace of civilians by their wandering, robberies, and ravaging. In the barracks the soldiers should be satisfied by relatively little food and drink, and they should practice themselves in their profession, discipline (together with artificial courage, [9: 23–24] the swiftness, and the abilities of leadership). The maintenance of the barracks should not be charged financially or otherwise on the civil society, because it would lead to dissention between the army and civil society. Soldiers, however, should be paid every time, so that they could sustain themselves and do their tasks. The military pay or the failure of the pay shows clearly whether soldiers are honoured or not. For maintaining or restoring the honour of soldiers the armed forces need to be standing, rather than hiring every applicants in necessity, who are often quite inexpert. This is because these latter soldiers react negatively to the properly trained and honoured soldiers, too. For a similar reason it is important to care about the wounded or killed soldiers, who risked their lives for the country. [8: 160–173]

To sum up Magyari's theory of justification of war one can state that for him Erasmus shaped the course, but his theory has independent parts as well. Magyari's theory is a form of just war theory, whose key points are the legitimate authority restricted by the representative function of the prince; the just causes for initiating a war for defending Christian faith, the issue of own country and neighbouring country; the modern form of the rule of right intention; the rules of proportionality and right intention of his age; and last but not least, the rules of *ius ante bellum*.

Conclusion

Hungary found itself in the middle of the Europe-related events from the 15th to the 17th centuries. These centuries were the years of the Turkish conquest and the danger for Hungary and Europe. For this reason, in both Europe and Hungary several thinkers conceptualised the justification of war against the Turks. The Hungarian authors took over the European patterns of thought, like humanism, Reformation, or the ideas of Jesuits, however, in many cases they altered or completed the received ideas. One example of this process is István Magyari's book *Az országokban való sok romlásoknak okairól* (1602, *On the causes of the many decays of the countries*). The ideas of this book are mainly from the European reformer Erasmus, but Magyari adapted Erasmus' ideas to his own age and to the specific situation of Hungary. By this Magyari built a specific theory of just war, which

has its own place in the development of warfare ideologies in the Early Modern period of Hungary and Europe.

References

- [1] AQUINAS, T.: The Summa Theologiae II/II. q. 40. In REICHBERG, G. – SYSE, M. H. – BEGBY, E. eds.: *The Ethics of War: Classic and Contemporary Readings*. Malden, Blackwell Publishing, 2013.
- [2] ERASMUS, D.: *Against War*. Boston, The Merrymount Press, 1907.
- [3] ERASMUS, D.: A Complaint of Peace. In. LEVI, A. H. T, ed.: *Collected Works of Erasmus Vol. 27–28*. Toronto–Buffalo–London, University of Toronto Press, 1986.
- [4] ERASMUS, D.: On the War against the Turks. In. RUMMEL, E. ed.: *The Erasmus Reader*. Toronto, University of Toronto Press, 1990.
- [5] ERASMUS, D.: The Education of a Christian Prince. In. LEVI, A. H. T. ed.: *Collected Works of Erasmus Vol. 27–28*. Toronto–Buffalo–London, University of Toronto Press, 1986.
- [6] FERNÁNDEZ, J. A.: Erasmus on the Just War. *Journal of the History of Ideas*, 34 2 (1973), 209–226. DOI: <https://doi.org/10.2307/2708726>
- [7] RON, N.: Erasmus' ethological hierarchy of peoples and races. *History of European Ideas*, 44 8 (2018), 1063–1075. DOI: <https://doi.org/10.1080/01916599.2018.1485002>
- [8] MAGYARI I.: *Az országokban való sok romlásoknak okairól*. Budapest, Magyar Helikon, 1978.
- [9] BODA M.: Az alapvető katonai erények mibenléte és helye a hosszú 19. század magyar hadtudományában 2. rész – A bátorság. *Hadtudomány*, 28 2 (2018), 18–29.

Public Service Management in Ecuador

Stefany CEVALLOS¹

This article addresses the perspectives of Public Service Management in Ecuador, a Latin American country which saw various social changes and political paradigms. The new Constitution of Ecuador was launched in 2008 in a scenario where nationalism replaced the liberal paradigm in Ecuador. Its main features were the defence of postliberal values and sovereignty as a superior principle. On the other hand, the role of the public sector in the economy of Ecuador grew after 1972 when petroleum revenues increased remarkably. Nowadays, the public sector reduction was entered into force after the collapse in the price of crude oil in 2014 and an earthquake of 7.8 Mw that devastated the coast of Manabí in 2016. In this context, during the presidency of the former president Rafael Correa, new principles were instituted, such as decentralisation, the new concept of public servant and new methodologies such as National Management for Results. The methodology used is secondary data sources including various types of books, journal articles, government and non-governmental reports, government implementation plans.

Keywords: public service, new public management, constitution, decentralisation, accountability.

Introduction

Ecuador is the third smallest country in South America. United States dollar is used here as the official currency.² The country is excellently located within the Andean market, has a high oil and mineral potential, and is rich in agricultural resources and energy; it is a country where transportation is subsidised.

The Andean country of 17.08 million inhabitants adopted a new constitution in 2008.³ After having an unstable democracy for a decade,⁴ the country is, to quote President Rafael Correa, “not in a period of change, but in a change of period”. The strategic framework

¹ Ph.D. student, National University of Public Service; e-mail: stefy220_@hotmail.com; ORCID: <https://orcid.org/0000-0003-1460-7324>

² Devaluation of the Sucre (national currency of Ecuador), a moratorium of the foreign debt and the intensification of poverty in the period of 2000–2007.

³ The Constitution is legal, organic and procedural. Legal because it has rights of particular importance that shall be protected, which shall be the aim of the State; organic because they determine the organs that form part of the State and that are expected to guarantee the rights; procedural because they establish mechanisms of participation for public debates. [1: 775–776]

⁴ Approximately 38 coups d'état since Ecuador became a Republic.

for good governance is “Living Well” (*Buen Vivir or Sumak Kawsay*), and the New Public Management (NPM) mirrors this new approach of Sumak Kawsay, [2] as set forth in the 2008 constitution of Ecuador and the National Plan for Living Well (Plan Nacional para el Buen Vivir, PNBV).

In Ecuador, historical processes led to the achievement of democracy in both the public and private spheres. In 2008, the Constitution of the Republic incorporated a set of principles for New Public Management. The objective of the present research is to give an overview of the development of the Ecuadorian Public Service Management system in the light of international and regional development trends.

In the current juncture, in Ecuador the construction of a paradigm of “equitable socioeconomic development” has allowed the birth of public policies. Public policies place within a normative frame of a constitutional state governed by rights the configuration of a Constitution of rights for a National Development Plan for the pursue of “Well Being”. The National Development Plan aimed at “Well Being” was focused on the reduction of poverty by means of an equal distribution of wealth and the sustainability of natural resources.

Related to the New Public Management, this research will analyse decentralisation, the new concept of public servant and the new methodology, the National Management for Results, as an implementation in the national legislation. Finally, I consider important to emphasise that the constitution of the republic (2008) undertakes the construction of national policies oriented to public investment, with the aim to promote the reform of the State.

The State of Ecuador

The State in its modern conception corresponds to a cultural and ideal process with the idea of a not individualized power. [3] Indeed, the State plays a very important role in the provision of services, as guarantor of the rights entrenched in the Constitution: this is its foremost duty.

Table 1. *The State of Ecuador.* [4]

Ecuador	
Political regime:	Social liberal state
Public administration:	New Public Management (NPM)
Characteristics: accountability is a primary requirement in developing countries.	

In Ecuador there was a change in the political and ideological views, that was embodied in the constitution of Ecuador. From the predominantly neoliberalist wave in the nineties that focused on the regional level, the country shifted toward a model in which the State strongly intervenes and participates in the economy, and its institutions are endowed with legitimacy to exercise their powers. This political historical process with a socialist hue is known as neo-developmentalism. Neo-developmentalism is part of capitalism, but it maintains the life of the neoliberal. [5]

Article 1 of the Constitution of the Republic of Ecuador reads: “Ecuador is a constitutional State of rights and justice, a social, democratic, sovereign, independent, unitary, intercultural, multinational and secular State.” [21]

Article 275: “The development structure is the organized, sustainable and dynamic group of economic, political, socio-cultural and environmental systems which underpin the achievement of the good way of living (Sumak Kawsay).” [21]

The State of Ecuador is responsible for guaranteeing the basic needs of its citizens, according to Article 314: “The State shall be responsible for the provision of the public services of drinking and irrigation water, sanitation, electricity, telecommunications, roads, seaport and airport facilities, and others as established by law.” [21]

In this context, since 2008 the legal structure and the way of operation and provision of public services changed. Rafael Correa boosted the constituent process, and a Constituent Assembly was held in the city of Montecristi in the province of Manabí, which concluded with the issuance of the Constitution of Ecuador in 2008.

Indeed, the Constitution of Ecuador changed the State model by establishing a Constitutional State of Rights and Justice, which places human beings over capital, and where human rights are protected by the constitution, without the need to mediate any Law for recognition. [6] In Ecuador, the Constitutional State of Rights and Justice, is the guarantee of a humanist model, in which there is a true subjection and fulfilment of the Law and of the fundamental rights. [7]

New Public Management

New Public Management in Latin America arose in the region as a system that meets the feasibility requirements for carrying out reforms that contribute to more efficient and flexible public administrations.

The principal institution is Latin American Center of Administration for Development (CLAD) seen as an international public body. Its core objective is the modernisation of public administrations as a strategic factor in economic and social development processes.

The mission of the CLAD is to encourage analysis, exchange of experiences and knowledge related to state reform and public administrations modernisation. This mission is carried out through different activities such as: international meetings specialised on these subjects, publications, document and information services, research and technical cooperation activities of its members and actors from other regions. [8]

Table 2. *Member states in the Latin American Centre of Administration for Development (CLAD).*

<i>Member countries:</i>	Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, Salvador, Spain, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Portugal, Republic of Dominica, Uruguay, Venezuela
<i>Observer member:</i>	Angola

[Adapted from Latin American Center of Administration for Development (CLAD).⁵ Retrieved from <https://clad.org/documentacion/cedai/>]

⁵ Retrieved from <https://clad.org/documentacion/cedai/> (Downloaded: 09.06.2020)

NPM is the result of two important documents: A New Public Management for Latin America [9] and the Ibero-American Charter for the Public Service. [10] A New Public Management for Latin America arose from the need to introduce reforms in Latin American public administrations, and the Ibero-American Charter formalises the agreement made by a broad set of countries in the region regarding the organisational guidelines to adopt tools and processes that shall contribute to the improvement of its efficiency.

In the framework of CLAD, NPM in Ecuador is constituted by public services that provide tangible or intangible goods to citizens, with quality and warmth care, in order to guarantee constitutional rights and aimed at the construction of the Living Well regime.

NPM offers two types of provision of a public service: the direct provision of a public service that is carried out by governmental institutions, whether they are those of the central government or by autonomous entities. [12] On the other hand, the benefit is indirectly configured when the public administration decides to grant a delegation. A public service is provided by an individual, for example through a concession or authorisation regime, such delegation is also carried out directly by the law. However, it is necessary to point out that this administrative act of authorisation becomes a kind of permission that the state grants for individuals to carry out their activities under a regulatory umbrella that allows the state to intervene and suspend that activity in order to avoid disputes in case that activity is rendered improperly.

Besides, there is a specific section about strategic sectors: telecommunications, non-renewable natural resources, transportation and refining of hydrocarbons, biodiversity and genetic heritage, radio spectrum, water, and others determined by law. Article 315 of the Constitution of the Republic of Ecuador reads: “The State shall set up public companies for the management of strategic sectors, the provision of public services, the sustainable use of natural resources or public assets and the exercise of other economic activities.” [21]

In this context, having considered a strategic sector implies a reservation in favour of the state, who has full capacity to intervene in those sectors to regulate, control and manage them in a way that is the most convenient. The management of these sectors has a constitutionally defined model, it must be carried out through the constitution of public or mixed-economy companies. In Ecuador, the delegation of the management of strategic services to the private sector, The Organic Code of Production, Commerce and Investments provides that only exceptionally, by a presidential decree, and when it is necessary and appropriate to satisfy the public interest; when there are no technical or economic capacities for that; or when a service cannot be provided by public or mixed companies.

Decentralisation

Ecuador is a unitary state, with a two-tier structure of decentralisation. The country is divided into 24 provinces (Provincias) which are formed by one or several cantons. According to the Constitution of Ecuador (2008), these provinces may also gather to create an autonomous region, but only those of geographical significance. The lower level consists of 221 municipalities called Canton or Municipios. [13] These entities are further subdivided into around 1500 parishes (parroquias) which are small politico-territorial divisions that may be classified into rural or urban parishes. They are under the authority

of a municipality which has the power to create or modify them. This subsidiary tier of decentralisation aims to be an intermediary between the people and the municipalities. [14]

The Constitution of Ecuador (2008) is dedicated to decentralisation, as the government launched an Organic Code for Regional, Autonomous and Decentralized Organization (COOTAD) [14] in the frameworks of the Living Well program for the reinforcement of the democratic state in Ecuador; it aims to deepen the decentralisation and deconcentration processes.

The administration, decentralisation and development model of the Decentralized Autonomous Governments is determined within the framework of planning and other state regulations of the national level. According to the Constitution of the Republic of Ecuador, Article 1: “This Code establishes the political-administrative organization of the Ecuadorian State in the territory: the regime of the different levels of decentralized autonomous governments and special regimes, in order to guarantee their political, administrative and financial autonomy. In addition, it develops a model of compulsory and progressive decentralization through the national system of competencies, the institution responsible for its administration, the sources of financing and the definition of policies and mechanisms to compensate for imbalances in territorial development.” [21]

It is important to emphasise that in Latin America the best example of decentralisation is Mexico. However, Ecuador’s decentralisation is not in the executive level but in all government levels. Centralism in Ecuadorian history caused that public management is in the three largest cities of Ecuador: Quito, Guayaquil and Cuenca. In 1563, the Royal Audience of Quito was created, with three main centres of authority: Quito, Guayaquil and Cuenca. In 1830, the Republic and its first Constitution enshrined that the departments are the same three. [15]

Indeed, before 2007 the decentralisation of the executive branch was based on the vertical regionalisation of the country, which divides it into natural regions: Pacific Region, Andes Region, Amazon Region and Insular. However, this regionalisation fails to overcome centralised management in Quito, Guayaquil and Cuenca being the most important provinces of Ecuador. Furthermore, since 2008 Ecuador is governed within the framework of a new political-citizen agenda, which is embodied in the Constitution of 2008. Indeed, in total there are 9 zones, 140 districts and 1,134 administrative planning circuits for the organisation of the executive in the territory. Administrative levels of planning are also the levels of deconcentration.

In this context, the recovery of the public is prioritised as the basis of the democratic transformation of the state, which aims to generate a change in distribution and redistribution of wealth based on a new development model outlined in the first National Development Plan (2007–2010).

The deconcentration from the executive branch in Ecuador allowed this renewed way of thinking about development, guided by the principles of dignity and solidarity, rescuing first of all the collective sense of Well Living for the making and consolidation of a democratic state in which all citizens can trust and refine its mechanisms and competences based on the recognition of territorial diversity and culture.

Public Servants

In the 2007 Constituent Process the idea of meritocracy was installed in Ecuador under the umbrella of the Ibero-American Charter of the Public Service in order to bet on a better state project and professionalisation of its public function (public service or civil service).

In addition, the idea is established that citizens are the ones who supervise and control the provision of the service as continuous users, and citizens participate in its exercise through mechanisms such as accountability. It is also established that in the New Public Management the services must be characterised by efficiency, quality and “warmth”. [16]

As for the regulation related to the civil service career of the public administration, this is the Management of Human Talent in the public sector. In Ecuador its action is regulated in the Organic Law on Public Service, (L.O.S.E.P. 2010) Article 229: “Public servants shall consist of all those persons who in any way or under any category, provide services or hold an office, function, or dignity in the public sector.” [17]

The rights of public servants cannot be waived. The law shall determine the executive body in charge of human resources and remuneration for the entire public sector and shall regulate admittance, advancement, promotion, incentives, disciplinary system, job security, salary scale and termination of duties of its employees.

In Ecuador, the rights and guarantees are inalienable, indivisible, interdependent and of equal hierarchy, fully justifiable, directly and immediately applicable by and before any public, administrative or judicial server, without the need for compliance with conditions or requirements not provided for in the Law; however, there may be laws that limit the exercise of rights which should be considered ineffective. The rights of the people are not only those established in the Constitution and in international treaties, but they can include those derived from the “dignity of the people”. The highest body of constitutional control and interpretation is the Constitutional Court, that is also responsible for administering constitutional justice. [18: 14] Indeed, the Constitution itself requires that public, administrative, or judicial servants, in the field of human rights, make the interpretation that is most convenient for the effectiveness.

National Management for Results

National Management for Results in Ecuador was a challenging process. There were two scenarios: the first was when former President Rafael Correa attended a meeting at the national firm Petroecuador in the framework of a workshop where progress and management were exposed through a tool called Company by Results (EPR) and the second moment was the continuous improvement of public management versus inefficiency and bureaucracy.

In October 2010, the Presidency of the Republic signed a consulting contract with the Ecuadorian company, e-Strategia Consulting Andes, for the “Implementation of a Government Methodology for Results and Computer System”. [19]

Since 2010, when this National Management for Results entered in force in Ecuador, the method prescribed control by parameters of results, and allowed to evaluate the performance of the institution semi-annually or annually, whether or not it reached the

objectives set, or the level of progress expected of them; and in case of failure, it can be known clearly what indicator failed, and thus one can investigate the causes that led to a misguided decision, and modify the structure to improve the quality of service provision.

Chronologically, the coining of terms related to management by results, goes back to the Austrian author of “management”, Peter Drucker. [20] However, its heyday, when its application took a greater momentum in the public sphere, was the New Public Management in Britain in the eighties, which strongly influenced the Latin American countries.

In this context, CLAD and the Inter-American Development Bank (IDB), regarding the projects Management for Results and Monitoring and Evaluation, were considered that Management for Results is more effective because they produce better results, are more innovative, flexible and have a higher assurance.

However, it appears that one of the main risks that arise from a results-based management policy is that the public administration does not know how to previously define objectives, or still worse, these objectives are not clear and not duly socialised to their citizens. In fact, putting aside participation and transparency would be basic in the New Public Management.

Conclusions

In Ecuador, the construction of a paradigm of “equitable socioeconomic development” has allowed the birth of public policies placed within a normative frame of a constitutional State governed by rights, with the configuration of a Constitution of rights, which appears as a National Development Plan for the search of “Well Being”.

This paper concludes with the prospects of Public Service Management in Ecuador. The state of Ecuador was presented in order to understand the ideological model that has defined the role of the state in the framework of the 2008 Constitution of the Republic of Ecuador. In effect, the Ecuadorian authorities undertook an effort to modernise the state and increase its planning, management, and development promotion capacities, achieving notable results in some areas. A clear example of this is that, according to the World Bank’s Worldwide Governance Indicators (WGI), between 2008 and 2015 Ecuador was the Latin American country, and one of the 10 countries worldwide, that advanced the most in government effectiveness.

In fact, the present study will be helpful for introducing Public Management in Ecuador; in the national centre of excellence for the research of public administration that meets the highest standards of the international scientific community.

References

- [1] ÁVILA, R.: From Legal Right State to Constitutional Right State and Justice. In. *Latin American Constitutional Rights Yearbook*. 10th Edition, CQ Press, 2009.
- [2] CORTEZ, D.: *Social construction of “Sumak Kawsay” in Ecuador. Genealogy of strategic design and managing policies of life*. Quito, Universidad Andina Simón Bolívar, 2011.

- [3] ROTH, D. – NOEL, A. *Public Policies: formulation, implementation and evaluation*. Bogota, Aurora, 2007.
- [4] BRESSER-PEREIRA, L. C.: Managerial Administration in Brazil: Reflections of a Reformer. In: SCHNEIDER, B. R. – HEREDIA, B. eds.: *Reinventing Leviathan*. Miami, North-South Center Press, 2001.
- [5] CYPHER, J.: Institutional-Structural Impediments to National Innovation Systems in Latin America. *Journal of Institutional Economics*, 6 3 (2014), 34–53. <http://institutional.narod.ru/jis/jis6.3.pdf> (Downloaded 09.06.2020)
- [6] FERRAJOLI, L.: *Derechos y garantías. La ley del más débil*. Madrid, Trotta, 2002.
- [7] FERRAJOLI, L.: El derecho como sistema de garantías. In *Derechos y garantías. La ley del más débil*. Madrid, Trotta, 1999. 15–36.
- [8] *Latin American Center of Administration for Development (CLAD)*. <http://old.clad.org/> (Downloaded 09.06.2020)
- [9] *A New Public Management for Latin America*, 1998. <http://old.clad.org/portal/publicaciones-del-clad/revista-clad-reforma-democracia/articulos/011-junio-1998/public-administration-and-development-in-latin-america-a-neoinstitutional-approach> (Downloaded: 09.06.2020)
- [10] *The Ibero-American Charter for the Public Service*, 2003. <http://siare.clad.org/cartaiberfunpubingles.pdf> (Downloaded: 09.06.2020)
- [11] GASTÓN, J.: *Técnica jurídica, servicio, función pública y sus servidores*. México, Jurídica Universitaria, 2007.
- [12] FERNÁNDEZ RUIZ, J.: Disertación sobre el servicio público. *Foro: Revista de Derecho*, 13 1 (2010), 5–21.
- [13] *National Institute of Statistics and the Censuses (INEC)*. www.ecuadorencifras.gob.ec/geoport-1/ (Downloaded: 09.06.2020)
- [14] *Organic Code for Regional, Autonomous and Decentralized Organization (COOTAD)*. www.defensa.gob.ec/wp-content/uploads/downloads/2016/01/dic15_CODIGO-ORGANICO-DE-ORGANIZACION-TERRITORIAL-COOTAD.pdf (Downloaded: 09.06.2020)
- [15] AYALA MORA, E.: Centralismo y descentralización en la historia del Ecuador del pasado a la situación actual. *Procesos: revista ecuatoriana de historia*, 1 19 (2003), 203–221. DOI: <https://doi.org/10.29078/rp.v1i19.269>
- [16] MARTÍNEZ MOSCOSO, A.: La Prestación de los Servicios Públicos de Calidad. *El Siglo*, 21 (2016), 27.
- [17] *Organic Law on Public Service (L.O.S.E.P.)*, 2010. www.trabajo.gob.ec/ley-organica-del-servicio-publico-losep/ (Downloaded: 09.06.2020)
- [18] ECHEVERRÍA, J.: El Estado en la nueva Constitución. In GRIJALVA, A. et al. eds.: *La Nueva Constitución del Ecuador. Estado, derechos e instituciones*. Quito, Corporación Editora Nacional, 2009. 17.
- [19] Inter-American Prize for Effective Public Management: National Management for Results. OAS, 2014. www.oas.org/es/sap/dgpe/innovacion/Banco/docs_paises/Ecuador_Planificacion_2014.pdf (Downloaded: 09.06.2020)
- [20] DRUCKER, P.: *Managing for Results*. New York, Harper and Row, 1964.
- [21] *Constitution of the Republic of Ecuador*, 2008. www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf (Downloaded: 09.06.2020)

Voluntary Rescue Service in Hungary: The HUSZÁR Team

Tamás HÁBERMAYER,¹ Péter HORVÁTH²

HUSZÁR, the Hungarian National Organisation for Rescue Services, was founded in 2012 and now has a staff of over 80. HUSZÁR is a special rescue unit that can be deployed in domestic and international disaster management. Based on the United Nations International Search and Rescue Advisory Group (UN INSARAG) classification, HUSZÁR is a medium level urban search and rescue team and its units are equipped with special skills and technical equipment. A special feature of the team is volunteerism combined with professional interventional skills. Its subunits can manage individual interventions, they have participated in several international disaster relief tasks following earthquakes and tsunamis, and they have also played an active role in the preparation of other nations' rescue teams.

Keywords: *HUSZÁR, INSARAG, Hungary, voluntary rescue team.*

Introduction

When a disaster occurs, the arrangement and performance of rescue operations as well as the management of the consequences place a significant burden on the defences of the affected country. Such situations require considerable mobilisation, high-level coordination of tasks and optimal distribution of the available resources. The efficient performance of all these tasks is dependent on the timely detection of imminent threats, prudent planning and properly trained forces that are skilled in aversion. Certain disasters (e.g. flood, excessive ground water at familiar or expected locations) can be managed with traditional precautions and planning; however, there are some extraordinary events that are almost impossible to prepare for (e.g. a new, unprecedented type of disaster or an earthquake whose magnitude is unpredictable). Such events can be managed by a novel type of hazard planning that is based on capabilities and expert networks and whose aim is to develop adaptability and rapid reactions. The inclusion of voluntary rescue teams is an essential improvement of threefold significance. Firstly, it is the local citizens who perform the very first intervention at the site of the disaster. They are present in the close proximity of the event, thus if they are not affected by the disaster, they can perform some immediate rescue operations. Following an earthquake, they can for instance search for survivors in the collapsed buildings and provide

¹ Ph.D. student, National University of Public Service, National Directorate General for Disaster Management; e-mail: tamas.habermayer@katved.gov.hu; ORCID: <https://orcid.org/0000-0002-6677-9163>

² Ph.D. student, National University of Public Service, National Directorate General for Disaster Management; e-mail: peter.horvath2@katved.gov.hu; ORCID: <https://orcid.org/0000-0001-7595-7980>

first aid. Residents can be prepared for local hazards; therefore, they can effectively assist professional rescue teams. Another important consideration is local knowledge. People who are familiar with the affected area can significantly increase the efficiency of interventions if they cooperate with those involved in disaster relief. Even if we consider these two factors alone, the role of volunteers is obvious. The third consideration is specific: there are professional types of interventions (e.g. dog search, diving, cave and alpine rescue), which, if offered as voluntary services, can markedly support the efforts of official forces. However, the equipment and preparedness of voluntary teams cannot be taken for granted as there can be marked differences between individual organisations. In view of their equipment and skills, some voluntary teams are only prepared for the aversion of local threats, while more professional, skilled organisations can serve national or even international purposes. As regards international search and rescue, the guidelines of INSARAG were endorsed by the United Nations General Assembly Resolution 57/150. [1] The voluntary Urban Search and Rescue (USAR) team of Hungary, called HUSZÁR, has recently been re-classified in accordance with the INSARAG guidelines, so this paper is going to examine the highest professional level. In view of the skills and capabilities of its subunits, the team can be considered a professional organisation in the field of earthquake-related search and rescue tasks.

However, the question is how a team of volunteers can meet the professional requirements set by UN INSARAG concerning urban search and rescue even if they are coordinated and supported by the government.

Therefore, the aim of this paper is to introduce HUSZÁR, the Hungarian urban search and rescue team, its special features and versatility; the team which could fulfil the requirements of the international qualification system.

As part of our research, we contacted the heads of the rescue subunits, analysed the composition of the team, the qualifications of the members as well as the versatility of the technical equipment. Previous interventions of the member organisations were also investigated and we reviewed how a complex unit can be established by combining several voluntary organisations.

The HUSZÁR Rescue Team

The voluntary rescue team of Hungary, HUSZÁR, was classified as a medium USAR team in 2012, when it successfully met the professional requirements of the UN at an international field exercise and classification in Hajdúszoboszló, Hungary. The official rescue team of the country, HUNOR, received its classification at the same time, thus Hungary is one of the few countries that has two rescue teams with a UN INSARAG qualification.

Since 2012 the HUSZÁR team has participated in several successful interventions, which mostly dealt with floods and excessive ground water, as these phenomena are the most frequent hazardous events caused by natural processes in Hungary and the neighbouring countries. The affiliated organisations of the team have also participated separately in disaster relief operations following earthquakes, tsunamis, and other natural disasters in Europe, Asia and Africa, which highlights the professionalism of the team.

Hungarian Act No. CXXVIII of 2011 concerning disaster management [2] provides the following definition of voluntary rescue teams: “A voluntary civil society organisation with specially trained members and professional equipment established for the prevention and relief of natural disasters or hazardous events, performance of disaster management tasks and minimisation of human loss and suffering.”

The subunits of the HUSZÁR has met the requirements of the National Classification,³ so all of them belong to registered voluntary rescue organisations.

Since its classification, the team has taken part in several field exercises and trainings, all of which have contributed to its development. The professional skills of the team have become broader and its technical equipment has been developed to meet modern challenges. We can state that its present preparedness fits the revised UN INSARAG guidelines and it could be put into action on each and any day of the year.

Meeting International Guidelines

INSARAG has more than 90 countries and international organisations in its ranks. Every accepted member belongs to this branch of the United Nations. The most important aim is to develop most effective methods and techniques to be employed in earthquake response and to coordinate the activity of those who take part in the rescue. The guidelines required for urban search and rescue preparedness and interventions were compiled by the countries and international organisations that belong to the network of INSARAG. The guidelines were based on all the experience gained from interventions performed since its establishment, so they comprise the highest level disaster management methods. The observation and application of these guidelines enables the cooperation of international organisations and rescue teams from various countries by following the same principles and regulations, and the coordination of the rescue tasks can also be realised at a high level. The adoptable and professional nature of the INSARAG guidelines, together with the positive, stimulating effect they had on the disaster management system of the individual countries, as well as the quality assurance (classification and monitoring) all make INSARAG one of the most developed international systems, but it may well be the most developed one.

The INSARAG classification defines three levels of capacity for USAR teams (light–medium–heavy). HUNOR is classified as a heavy, while HUSZÁR as a medium team. Medium and heavy USAR teams have the ability to conduct technical or dog search and rescue operations in collapsed or failed structures to look for humans and they have the technical equipment to lift and move heavy objects. The staff can pull down, cut, reinforce or support concrete and structural steel typically used for construction, work with alpine techniques, detect, identify and isolate hazardous substances. The medical staff can perform resuscitation, amputation and can provide life support. The rescue teams must be adequately staffed and logistically sufficient to allow for 24-hour operations at a single intervention site for 5–10 days (light–5, medium–7 and heavy–10). [3]

³ Voluntary rescue teams have to acquire a classification in order to ensure the authenticity of their organisation, the professional nature of their interventions, and also to create an effective base for cooperation with the national disaster management forces. For more details (in Hungarian) see: <https://katasztrofavedelem.hu/26431/nemzeti-minositesi-rendszer> (Downloaded: 12.02.2020)

HUSZÁR Subunits

“Disaster management is a national issue. A unified command of defence is governmental responsibility. All citizens have the right to learn about the potential hazards in their environment and familiarise themselves with the rules of prevention. It is also their right and duty to take part in disaster management.” [2: para 1 (1)]

HUSZÁR is a medium urban search and rescue team composed of voluntary subunits of special classification. Its staff belong to voluntary rescue organisations that have been classified and registered by the National Classification of Hungary. The units have a cooperation agreement with the Directorate General for Disaster Management, Ministry of Interior, Hungary (in Hungarian: Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság – BM OKF). The combined force of the units, HUSZÁR, is a medium USAR team classified by INSARAG. Professional command and notification of deployment are performed by the regional representatives of BM OKF, who are almost always voluntary members of the units.

HUSZÁR is composed of six classified units, that can be deployed individually to assist with domestic disaster management. The units are the following:

- Pilisvörösvár Volunteer Firefighters (in Hungarian: Pilisvörösvári Önkéntes Tűzoltó Egyesület – Pilis ÖTE);⁴
- Pest County Search and Rescue Team (in Hungarian: Pest Megyei Kutató-Mentő Szolgálat – PMKMSZ);⁵
- Zala Special Rescue Team (in Hungarian: Zala Különleges Mentők Egyesület – ZKM);⁶
- Hungarian Red Cross (in Hungarian: Magyar Vöröskereszt – VK);⁷
- Search–Rescue and Fire-Fighting Association of Pécs (in Hungarian: Pécsi Kutató-Mentő és Tűzoltó Egyesület – Pécs KMTE);⁸
- Volunteer Firefighters and Life Saving Association of Kaposvár (in Hungarian: Kaposvári Önkéntes Tűzoltó és Életmentő Egyesület – KÖTÉL).⁹

The members of the units are volunteers with special skills and experience of several years or even a decade. The staff include physicians, veterinary surgeons, paramedics, nurse practitioners, psychologists, dog handlers, firefighters, joiners, cavers, industrial alpinists, static engineers, explosives experts, heavy rigging and hazardous substance specialists. One part of the staff obtained their INSARAG classification back in November 2005 during a classification exercise held at the previous military base in Lenti-Zajda, Hungary. These rescue teams had been deployed several times earlier, which had justified their role in disaster relief. [4: 5]

The professional members of HUSZÁR have had numerous opportunities to utilise their skills when saving human lives and material goods. The volunteer firefighters of Pilis ÖTE, Pécs KMTE and KÖTÉL work closely together with the official national

⁴ Official website: <http://vorosvartuzi.hu/>

⁵ Official website: <https://kutato-mento.hu/>

⁶ Official website: <http://zala.katasztrofavedelem.hu/zala-kulonleges-mentok-egyesulete>

⁷ Official website: <http://vorosskereszt.hu/>

⁸ Official website: www.rescue-pecs.hu/

⁹ Official website: <http://kotelmento.hu/>

disaster management service, thus they contribute to citizens' safety on a daily basis. The members of PMKMSZ have several years of experience in the field of alpinism and dog search. They primarily work in the capital of Hungary and Pest County, but their search dogs have a global reputation as well. The Hungarian Red Cross have four representatives in the medical component of the team, who have full-time jobs in hospitals or at the ambulance services. Eighty percent of the members of ZKM works for official law enforcement bodies, so they also use their specialised knowledge and skills on a daily basis.

By examining the composition and previous interventions of the units and the volunteers we drew the conclusion that the high-level versatility of HUSZÁR is due to the fusion of the know-how of the individual, classified units.

The unique individual skills and the daily practice of the personnel provide a solid base for the operation of a medium USAR team. The UN INSARAG guidelines recommend the following arrangement and composition for a medium USAR team:

Table 1. *The recommended arrangement and composition for medium USAR teams.* [2: 35]

USAR Component	Tasks	Suggested Staff Allocation	Suggested Number (Total 40)
Management	Command	Team Leader	1
	Coordination	Deputy Team leader	1
	Planning/Follow Up	Planning Officer	1
	Liaison/Media/Reporting	Liaison Officer	1
	Assessment/Analysis	Structural Engineer	1
	Safety and Security	Safety Officer	1
	RDC/OSOCC/UCC	Coordination Officer	2
Search	Technical Search	Technical Search Specialist	2
	Dog Search	Dog Handler	2
	Hazardous Materials Assessment	Hazardous Materials Specialist	2
Rescue	Breaking and Breaching; cutting; shoring; technical rope	Rescue Team Manager and Rescue Technicians	14 (2 teams comprising 1 Team Leader and 6 Rescuers)
	Lifting and Moving	Heavy Rigging Specialist	2
Medical	Medical Team Management: Coordination and administration of medical team. Integration with local health infrastructure Care of team (including canines) and victims encountered	Medical Doctor	1
		Physician, Paramedic, Nurse	3
Logistics	BoO	Logistics Team Manager	1
	Water supply	Transport Specialist	1
	Food supply	Logistician	1
	Transport capacity and fuel supply	Base Manager	2
	Communications	Communications Specialist	1

Composition of the HUSZÁR personnel in the 2017 re-classification:

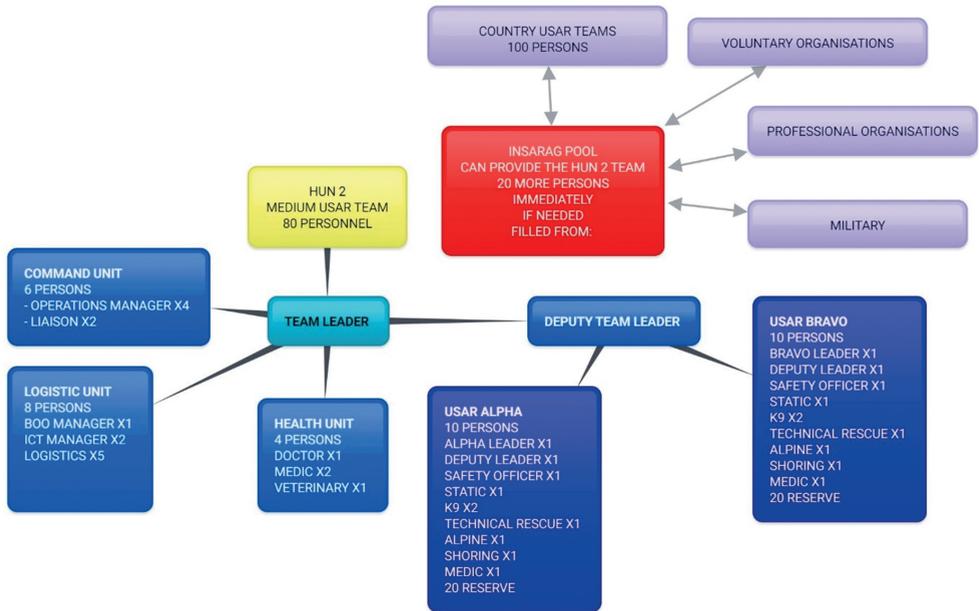


Figure 1. *HUSZÁR staff.*
[Edited by the authors.]

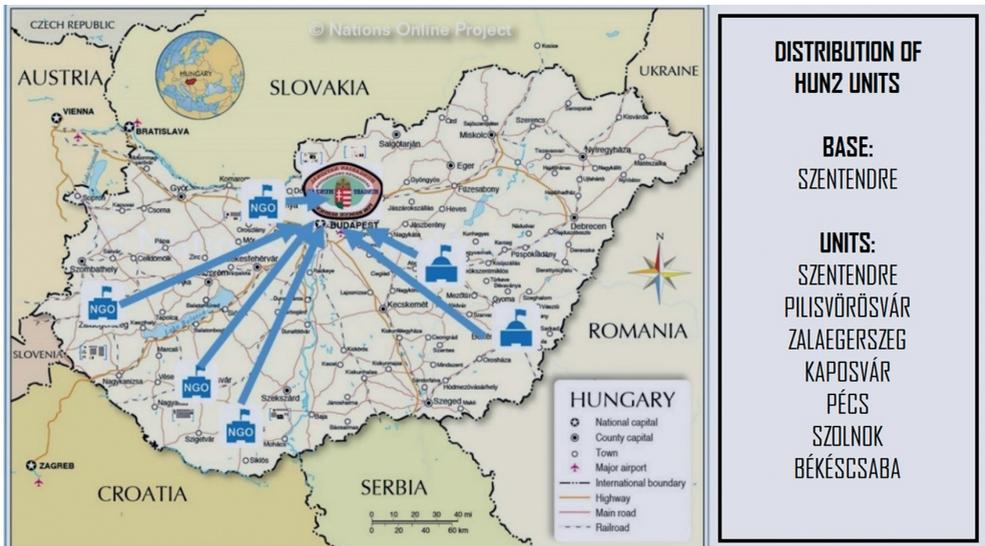


Figure 2. *Location of HUSZÁR units.*
[Edited by the authors.]

The capabilities of HUSZÁR are summarised in this INSARAG Team Fact Sheet:

USAR TEAM FACT SHEET		 INSARAG Preparedness – Response	
<i>Team details to be uploaded in the VO before departure and given to RDC/UCC on arrival.</i>			
TEAM INFORMATION			
A.0 Team-ID	HUN-2		
A.1 Team name	HUSZÁR	A.2 Home country	HUNGARY
A.3 Number of persons	40	A.4 Number of dogs	4
A.5 Team type responding	Light <input type="checkbox"/>	Medium <input checked="" type="checkbox"/>	Heavy <input type="checkbox"/> Other _____
A.6 INSARAG Classification	None <input type="checkbox"/>	Medium <input checked="" type="checkbox"/>	Heavy <input type="checkbox"/>
Responding elements:			
A.7 Technical Search	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.8 Canine search	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.9 Rescue	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.10 Medical	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.11 Hazmat detection	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.12 Structural engineers	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	Number <input type="text" value="2"/>
A.13 RDC/OSOCC support	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.14 UC support	yes <input checked="" type="checkbox"/>	no <input type="checkbox"/>	
A.15 Other capabilities	Drone reconnaissance (if it is allowed in the country)		
A.16 Self-sufficiency (number of days)	Water <input type="text" value="7"/> days	A.17 Food	<input type="text" value="7"/> days
A.18 Expected arrival date [DD-MMM]	<input type="text"/>		
A.19 Expected arrival time [hh:mm]	<input type="text" value="0:00"/>		
A.20 Point of arrival	A.21 Aircraft type _____		
SUPPORT REQUIREMENTS			
<u>Transport for</u>			
B.1 Persons (number)	40	B.2 Dogs (number)	4
B.3 Equipment (ton)	6,00 tons	B.4 Equipment (cubic metres)	30,00 m ³
<u>Supplies</u>			
B.5 Gasoline (litres per day)	150 litres	B.7 Cutting Gas (cylinders)	Type <input type="text" value="Oxygen"/> <input type="text" value="Propane"/> <input type="text" value="Acetylene"/>
B.6 Diesel (litres per day)	150 litres	Number <input type="text"/>	
B.8 Medical Oxygen (cylinders)	No. _____	Size <input type="text"/>	
	Size _____	B.9 BoO Space Requirement (m ²)	1200 m ²
B.10 Any other logistical needs	technical water in the BoO 200 litres/day;		
CONTACTS			
Contact 1		Contact 2	
c.1 Name	SAMPLE PERSON 1	c.5 Name	SAMPLE PERSON 2
c.2 Mobile phone	+1111111111	c.6 Mobile phone	+2222222222
c.3 Sat phone		c.7 Sat phone	
c.4 E-Mail	samplemail1@sample.hu	c.8 E-Mail	samplemail2@sample.hu
c.9 Base of Operations Address (if known)			
c.10 Radio Frequency (BoO)	<input type="text" value="1"/> <input type="text" value="4"/> <input type="text" value="9"/> . <input type="text" value="6"/> <input type="text" value="9"/> <input type="text" value="3"/> MHz		
<i>(GPS coordinates normally in Datum WGS84)</i>			
c.11 BoO GPS coordinates (if known)		c.11 GPS Coordinates <i>decimal format</i>	
		c.11 GPS Coordinates <i>other formats</i>	
Form completed by: _____ Name			

Figure 3. HUSZÁR Team Fact Sheet. [5]
[Completed by the authors.]

The figure shows that the rescue team has all the necessary structural (management, search, rescue, medical and logistic) components set forth by the INSARAG guidelines.

In Hungary the units are located a few hundred kilometres from each other. Their primary objective is the aversion of local hazards; however, they regularly exercise together and share all the experience they gain from individual deployments.

The equipment necessary for international deployment is stored at the base of PMKMSZ in Budapest and on the premises of the subunits. Some equipment has two sets. This arrangement saves a lot of time in case of an occasional international deployment (air transport) since the transport will be sent from the Liszt Ferenc International Airport in Budapest. Should deployment be required in another region of the country, the domestic coverage of the whole country means that individual regional units can get to the scene of the event faster and they can start the initial survey earlier. By using the tools and devices operated by the units, search and rescue tasks can be commenced immediately and the other units can join in when they arrive. Cooperation between the units is continuous, which allows for joint financing or joint submission of tenders for new equipment. The units also exercise or take part in field practices together, thereby creating a strong and effective team that can fulfil the INSARAG guidelines and have a valid registration among the international USAR teams.

In summary, we can say that the individual and combined professional knowledge and skills of the units, which they use continuously, on a daily basis as part of their work, is an essential strength of the team in domestic and international disaster management tasks.

Recommendations

Properly executed volunteerism is a social value. It is important for the volunteers themselves as the society benefits from the positive effects of the activity, and it provides the volunteers with valuable feedback. This feedback helps the members of the voluntary organisations to remain engaged and motivated during the performance of their rescue operations. It has also been noted that a higher level of cooperation between volunteers is associated with the involvement of more professionals, which exerts a further positive effect on innovative capacity. Innovation results in novel, faster and more effective solutions during the interventions, which brings further success and recognition, thereby increasing motivation. Therefore, we recommend the further, more thorough investigation of voluntary organisations that have excellent performance and results in a specific field of activity (e.g. cave rescue, dog search, alpine techniques, etc). As part of the investigation, special attention has to be paid to the application of innovative technology as well as the acquisition of special interventional methods, since these can improve the efficiency and cost-effectiveness of official, governmental bodies.

No matter which national or international urban search and rescue team we talk about, belonging to any of them is significant honour, professional recognition and considerable responsibility as well. Working in such a special setting involves several challenges and the time factor of 100 hours exerts a strong influence on performance. Therefore, the training of rescue teams has to be continuous, focusing on special skills, equipment, as well as the culture of individual countries and regions. Apart from that, bridging linguistic and procedural differences is also essential for international coordination since an extensive earthquake, for instance, will certainly lead to severe damage with several interventional sites, and local INSARAG rescue teams will definitely need to be involved. As technology advances, the application of electric devices (which also necessitates further skills and trainings) can be of great assistance, since they can markedly improve the efficiency of

interventions. Under the aegis of the United Nations, all rescue teams follow the INSARAG guidelines as the common platform of coordination, and the working language of action is English. This background information probably explains why being a member of such a team is considered to be of great honour by the volunteers. Besides high-level professional skills, team members obviously have to fulfil an ever-increasing number of requirements (e.g. language skills, application of electric devices, coordination in an international setting). Leaders have to face even higher expectations as they need:

- outstanding professional, IT and linguistic skills, as well as stress tolerance;
- significant creativity and improvisation skills;
- managerial, communication and coordination skills;
- familiarity with international protocol;
- dedication and motivation to represent their own country.

It has to be stated that not everybody is suitable for these operations, as most of the tasks are performed under extreme (and hazardous) conditions, which needs conscious preparation. When interventional planning takes place, sound competition does occur among the members, and all leaders aim to send their best experts to the site of international rescue operations. There is no legal hierarchy between the international rescue teams, only cooperation, since effectivity requires coordinated operations. When INSARAG principles are applied properly, the team is led by the most competent person, who is accepted by everybody else. All operations need outstanding professional, IT and linguistic skills; stress tolerance; creativity; managerial, communication and coordination skills; familiarity with international protocol, as well as dedication and motivation at the same time. The most essential guideline is that assistance has to be truly helpful rather than constituting further difficulties for the countries in need. US INSARAG sample forms have an electronic version as well, which can be uploaded in the Kobo Toolbox system and used instead of or parallel to the paper-based version. This will create a common, effective system of all participating groups, and all qualified teams will be able to perform professional tasks together on the basis of the common platform.

References

- [1] MUHORAY Á.: *Katasztrófamegelőzés I.* Budapest, NKE Szolgáltató Nonprofit Kft., 2016. https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10287/ebook_XL_KVI_Katasztrofamegelozes_I.pdf?sequence=1&isAllowed=y (Downloaded: 20.02.2019)
- [2] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. www.fao.org/faolex/results/details/en/c/LEX-FAOC129205 (Downloaded: 12.02.2019)
- [3] *INSARAG Guidelines. Volume II: Preparedness and Response. Chapeau Manual A: Capacity Building.* New York, United Nations Office for the Coordination of Humanitarian Affairs, 2015. <http://portal.undac.org/pssuportal/portalrest/filessharing/download/public/7FBS4Bt4kuozXvN> (Downloaded: 12.02.2019)

- [4] JACKOVICS P.: *Társadalmi és civil szervezetek szerepe a polgári-, és katasztrófavédelem tükrében.* www.vedelem.hu/files/UserFiles/File/konf2007/pv/Jackovics_doc.pdf (Downloaded: 12.02.2019)
- [5] *INSARAG – Team Fact Sheet.* www.insarag.org/images/Documents_and_forms/USAR_Team_Fact_Sheet.pdf (Downloaded: 03.06.2020)

Solutions for the Accessibility of Water Sources for Fire Extinguishment

Gergely HERCZEG¹, Ágoston RESTÁS²

Water is an essential fire extinguishing agent. Besides the existence of water for this purpose, the availability of water sources is essential as well. Quick and efficient access to water sources contributes to effective firefighting, thereby avoiding any increase in damage, and it protects human life. With regard to the water sources, the authors examine and analyse the anthropometric data, and the physical properties of the equipment needed for the water. These are also used to determine the conditions of optimal access to the various water sources for firefighting.

Keywords: water sources for firefighting, fire hydrant, water sources, accessibility, fire intervention requirements.

Introduction

Water is an essential extinguishing agent during firefighting. In addition to the availability of water for fire extinguishment, it is also essential to have access to water sources, during firefighting, revision and maintenance. Accessibility is determined, on the one hand, by the characteristics of the human body and, on the other hand, by the physical properties of the devices required for the water. At this time, we do not know under what conditions the fire protection equipment and the water sources for fire extinguishment are available (taking into account e.g. anthropometric features). In some cases, the current regulations formulate only a general requirement for accessibility. However, they do not always provide guidelines on the implementation, which is of specific nature. The author aims to determine the conditions required for the availability of the water sources.

According to the author, fire hydrants, water storage tanks, wall fire hydrants can be considered as water sources. There are currently only a few Hungarian and international publications on the topic. However, we can find several papers in international and national literature on the topic of ergonomics and anthropometry. In many cases, these publications also deal with the authors' broader field of expertise, but they are not explicitly concerned with the relationship between water sources and humans. They deal with the conditions for

¹ Doctoral student, National University of Public Service, Faculty of Military Sciences and Officer Training, Doctoral School of Military Engineering; e-mail: herczeggergely@gmail.com; ORCID: <https://orcid.org/0000-0001-9633-5152>

² Ph.D., associate professor, National University of Public Service; e-mail: restas.agoston@uni-nke.hu; ORCID: <https://orcid.org/0000-0003-4886-0117>

quick use and easy access to the water sources for firefighting. Otherwise, these publications deal only with the authors' narrow field of expertise. Typically, standards or guidelines deal with this topic. [1, 2] There are only a few articles that refer to the technical tools used for salvage by water.

Scientific research is essential in fire prevention to increase efficiency, decrease injuries, and to maximise the rescued value. [3: 159] Nowadays, engineering comes into view increasingly in fire protection. [4]

Because of the reasons mentioned above, this paper can be supplementary, as it attempts to present data that contributes to the sufficient availability of the water sources for firefighting. Based on data, methods, and principles that can be found in the Hungarian and international literature, the author has developed suggestions that help to determine the necessary parameters for the availability of water sources. During the research, the author analysed the relevant national and international literature, including standards and other documents. The authors study and compare national and international literature as well as various standards and guidelines, and through this comparative analysis they will formulate suggestions for the accessibility to water sources.

On the one hand, the literature generally mentions data related to the size of the human body, [5] and on the other hand, there are concrete suggestions that can be used in other fields that require similar technique. [6] So far, research has used anthropometric data to produce ergonomic results. However, they have focused primarily on the interaction between man, machine, and the environment, and have tried to optimise them. These studies rarely include occasional activities such as the use of water sources for firefighting.

A 2016 study suggested that a fire hydrant should be available within 100 m from the main entrance of the buildings, thereby increasing the 30 m requirement in Portugal. [7] Myburgh and Jacobs also deal with the use of fire hydrants, but not with the conditions of their availability. They conclude that it is advisable that the hydrants be as close to the fire as possible. [8] Zhou and Reniers investigated the relationship between the number of fire hydrants and the success of firefighting. They found that increasing the number of fire hydrants improves the success of firefighting. [9] Based on a questionnaire made in Taiwan, Wang and Shih stated that the most commonly used water sources for firefighting are hydrants. [10] A 2014 study dealt with the hydrodynamical optimisation of hydrants, but their research did not extend to the availability of the fire hydrants. [11] Hassanain, Hafeez, and Sanni-Anibire assessed in their study a fire hydrant with a free space of 914 mm and located within 122 m from the protected building as suitable. [12] Sierra, Rubio-Romero and Gámez point out that wall fire hydrants should be easily accessible, but they do not specify criteria for it. [13] According to J. A. Smith, firefighting areas should be first cleared from snow for easier accessibility, but he does not specify the extension required for access. [14]

One of the main areas of ergonomics is physical ergonomics. It deals with the physical activity, the structure of the human body, its dimensions, and also its biomechanical and physical characteristics. [15] Anthropometry is the science of the characteristics of the human body, which examines the dimensions, shape, power, and working capacity of the body. Anthropometry is a branch of ergonomics. [16: 6] In case of an extraordinary event or fire, the human behaviour differs from the ordinary, [17] so, in such a situation, the water sources for firefighting must be as noticeable and accessible as possible. The goal of

the author is to facilitate the decision-making that is difficult in such a situation, and thus to provide effective firefighting.

In 97.9% of the territory of Hungary, it is guaranteed that the firefighters arrive at the fire scene in 25 minutes after the alarm. [18] If the arrival of the firefighters is suffering a delay, it is expedient if the workers of the facility make the water sources accessible prior, and it is not a task of the firefighters.

Easy access to the water source used for fire extinguishment allows a quick use. Accessibility shall be allowed to everybody who may be able to use the water source for firefighting or wants to inspect or maintain it. When water sources are accessible, the firefighting can be accomplished quickly and efficiently. When studying the current Hungarian regulations, it is not clear whether the legislator prescribes water sources for firefighting only to facilitate the intervention of the fire departments or to facilitate firefighting by non-firefighters.

The balance of the fire protection could be unstable if there are cars parking on the keep clear area around the water source. [19: 195]

Mainly wall fire hydrants with rigid hose are used in case of a fire of combustible materials that are not under voltage. Its use does not require any specific training. These can be, for example, outdoor fires, bush fires, or municipal waste container fires. It can be a good idea to designate for this task people in workplaces who are trained and able to do firefighting. [20]

Considering that the legislation prescribes water sources in order to facilitate the firefighting for non-firefighters, it is advisable that the rules of fire protection include their availability. The author examines the accessibility of water sources from the perspective of a healthy adult.

Criteria of Accessibility

We must know the anthropometric data of the potential users in order to determine the availability of some types of water sources for firefighting. We can find representative data on this in a standard. [21] Although the object of this standard is the dimensioning of the access openings used on the machines, it is nevertheless suitable for determining the availability of water sources for firefighting. The standard includes anthropometric data according to percentiles. "The x% percentile of a distribution is the number less than or equal to x% of the elements." [22: 22] I always recommend the percentile that gives access to as wide a range of users as possible. Accessibility to the water source requires an unobstructed space, which is at least 2,094 mm high and at least 726 mm wide. It may also be necessary to exert more force for the use of the water sources for firefighting. The water sources demanding more force for the operation should be between 920 mm and 1,105 mm above the ground level. Height limits that allow less power are between 600 and 1,520 mm. [23] According to the NFPA 1142 8.4.1. (National Fire Protection Association, USA) regulation, at least 0.9144 m space should be held around the output manifold connections of the hydrants. [24] According to the NFPA 14 7.3.1. regulation, the centre of the closed valves for wall fire hydrants (e. g. valve, tap) shall be at least 0.9 m and not more than 1.5 m from the ground. The recommended height of the water supply stump of the dryline shall

be between 457 mm and 1,219 mm above the ground, according to paragraph 6.4.6. [25] According to the NFPA 1 18.5.7.2. regulation, at least 1,524 mm space should be held around the hydrants having an inside diameter greater than 64 mm. [2] According to DIN 14461-1, the height of the closed valve of the wall fire hydrant shall be 1,200–1,600 mm above the ground. [1]

One of the requirements of the fire hydrant is that they shall allow the water to safely get out, taking into account the minimum bending radius of the hose. The manufacturer does not always specify the minimum bending radius of the hose at nominal pressure. [26] According to the Q1 figure of the harmonised standard, the hoses have to be tested so that when bended, they shall lie flat between the guide rails with a radius 22 times more than their inner diameter. [27] The same is required by the relevant Hungarian standard 7.8.3. [28] A 75 mm diameter “B” hose is used to supply the fire engines with water. [29]

The minimum bending radius of the outer bend of the hose “B”:

$$r = \frac{22 \cdot 75 \text{ mm}}{2} = 825 \text{ mm}$$

A hydrant key is also required for the operation of the hydrants. The length of the ground hydrant key is about 600 mm. When we place it on the hydrant, it describes an arc of 300 mm from the longitudinal axis during the opening. [30] Besides, the distance required to hold the fire key is 150 mm, taken also into account the length of the hand. [23] So, the required space for opening the hydrant is 450 mm around the longitudinal axis of the hydrant.

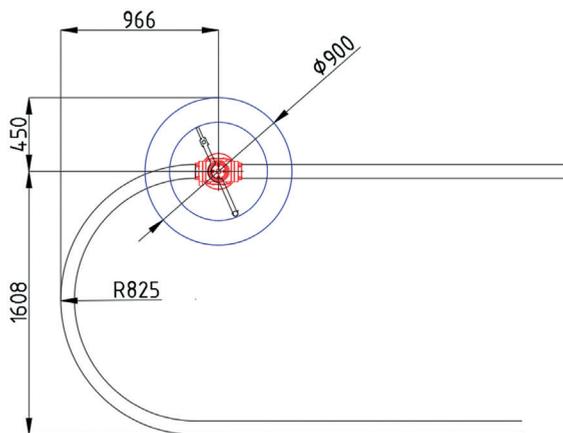


Figure 1. Ground fire hydrant with two “B” hoses, hydrant key. [Created by the author.]

Figure 1 illustrates the operational position and dimension of the devices required to operate the ground fire hydrant. Based on these dimensions, a simplified scheme of free space can be determined around the fire hydrant (Figure 2).

The free area around the fire hydrant should have a solid surface. It will ensure that in all weather conditions the traffic around the hydrant and the operation of the hydrant will be undisturbed. The slope conditions of the pavement must be suitable for people to stay and travel on it. Therefore, the limit for the maximum slope for pedestrian traffic is applicable

here, which is 1 : 8. [31: 268] The fire hydrant should also be approached on a solid road surface. However, its width should be at least equal to the shoulder width (726 mm), [23] the slope limit of 1 : 8 is also applicable here. A solid pavement is also reasonable because, in the case of underground hydrants, if the environment of the hydrant is not rigid, the sediment deposited by watercourses formed during rainy weather may obscure the hydrant. The solid pavement around the hydrant can help to locate the hydrant under the sediment. Also, if the solid pavement is long enough in the opposite direction to the slope, it will reduce the amount of sediment. The criterion of accessibility of outdoor hydrants in winter is de-icing and snow removal. If the installation has a heated pavement, we suggest extending it to the surroundings of the water sources and the roads leading to them. If there is no heated pavement, the road leading to the water source must be de-iced continuously. [28]

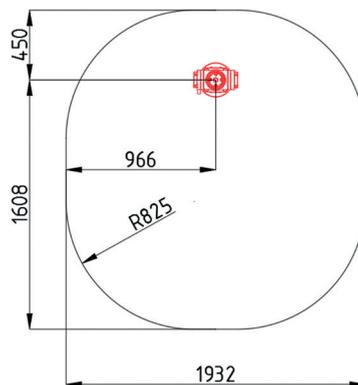


Figure 2. *An illustration of the availability of an outdoor ground fire hydrant.*
[Created by the author.]

Suction hoses are required to extract the amount of water that we can remove from the water sources by suction. It can withstand the effects of internal pressures, which is below the atmospheric pressure. Water extraction by suction may occur when water is taken from cisterns. The connection point of the water output manifold is optimised from the perspective of human force and ergonomic design when it is positioned at the height of 920–1,105 mm. The height of the output manifold of the fire engine shall also be taken into account during the design. It is advisable to maintain a space large enough to operate the fire engine in front of the connection of the output manifold of the water source. It is necessary to take into account the dimensions of all fire engines, to ensure the accessibility to water sources.

One of the most extended water carrier vehicles in Hungary is the fire engine Heros Aquarex S10. It has a length of 8,300 mm, a width of 2,550 mm, a height of 3,520 mm, and the maximum authorised mass of it is 25,000 kg. [32] In the EU, the maximum width of a vehicle on the road is 2,550 mm, the maximum allowed height is 4,000 mm, and the maximum allowed length is 11,000 mm. [33] When planning the open spaces and the accessibility, it is advisable to take into account the maximum permissible size of the vehicles, as this prevents subsequent modifications and extensions, which may become

a financial burden. For the possibility of the connection of the output manifold connector and the output manifold at the rear of the vehicle, it is advisable to keep free space, at least a length of one suction hose between the connector of the water source and the rear of the vehicle. In general, a 110 mm diameter suction hose is used in Hungary, which is 2,000 mm long. [34] This is why the required distance is 2,000 mm. The length of the free space in front of the output manifold connection of the water source shall be the permitted length of the vehicle, the length of the suction hose, and the total length of the space required for traffic around the vehicle (shoulder width). This value is 13,726 mm, based on the above. The size of the free space to be provided is the permissible width of the vehicle. The protruding part of the vehicle is the size defined by the space required for free movement. Considering this, the author recommends for this value to be at least 5,000 mm. The height of the free space in front of the connection of the output manifold of the water source shall be at least equal to the sum of the maximum possible height of the vehicle plus the height of the human body with supplements. [23] This value is 6,094 mm.

If the fire engine is installed perpendicularly to the axis of connection of the output manifold of the water source, the space required for accessibility can be determined based on the minimum bending radius of the suction hose.

The minimum required bending radius of a 110 mm diameter suction hose is 1,100 mm in Hungary. [35] In this condition, the outside of the hose bent at the minimum required bending radius shall be curved with a radius of at least 1,230 mm. In this case, the wall thickness of the hose is ignored.

Figure 3 illustrates the horizontal dimensions of the installation site, which is perpendicular to the connection of the output manifold of the water source.

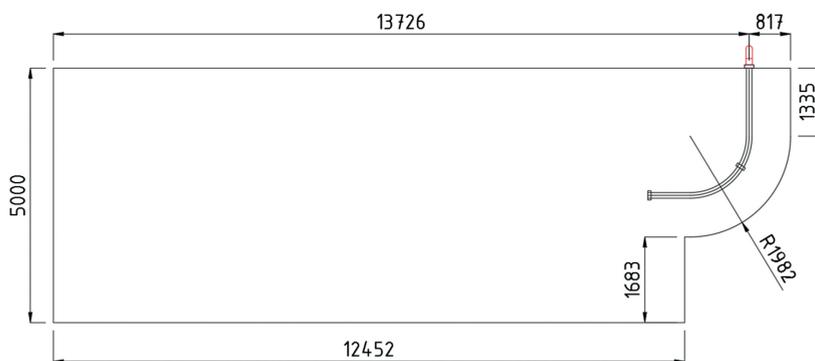


Figure 3. *The size of the area around the connection of the output manifold of the water source.* [Created by the author.]

Summary

The author presented data that are relevant for the equipment needed for the use of water sources for firefighting. Using these data, I determined the conditions of the availability

of the water sources, primarily the horizontally free spaces around the water sources for firefight. Also, I determined the optimal height of those parts of the water source where greater force is needed, and the height of the lowest and highest points of the parts requiring less force for optimal accessibility. The solutions presented by the author can also improve the effectiveness of firefighting interventions and may be suitable for firefighting in the case of vehicle fires in land, water, and air. This paper provides an opportunity to implement general regulation by quantifying it.

For accessibility of the water sources, the authors have identified the following data, which provides access for a wide range of users, and includes rare uses:

- on the way to the water source a path 2,094 mm high and 726 mm wide should be provided;
- the lowest point of the control of the water source should be 600 mm from the ground (floor);
- the highest point of control of the water source should be 1,520 mm from the ground (floor);
- the height of the control of the water source, which requires more force, is optimal between 920 and 1,105 mm above the ground (floor);
- the geometric data of the space kept free around the hydrant are shown in Figure 2;
- Figure 3 shows the horizontal dimensions of the installation site, which is perpendicular to the connection of the output manifold of the water source.

The values mentioned above are primarily based on literature; they consider the dimensions of the human body and human effort. It is an everyday activity for firefighters to use water sources. However, it is a rare task for workers in a facility. Therefore, it may be useful to examine by experiments the solutions developed by the author before using the data in practice.

References

- [1] *DIN 14461-1:2016-10 Feuerlösch-Schlauchanschlüsseinrichtungen. Teil 1: Wandhydrant mit formstabilem Schlauch.* www.beuth.de/de/norm/din-14461-1/258819312 (Downloaded 30.04.2019)
- [2] *NFPA 1 Fire code. 2018 edition.* www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1 (Downloaded 30.04.2019)
- [3] PÁNTYA P.: Kutatási alapok a katasztrófák elleni védekezés technikai fejlesztéséhez. *Hadmérnök*, 12 1 (2017), 158–169.
- [4] RESTÁS Á. – PÁNTYA P. – HORVÁTH L. – RÁCZ S. – HESZ J.: A tűzvédelem komplexitása a korszerű megelőzéstől a hatékony beavatkozásig. In RESTÁS Á. – URBÁN A. szerk.: *Katasztrófavédelem*. Budapest, BM OKF, 2015. 161–165.
- [5] *MSZ EN ISO 7250-1:2018 Az emberi test alapvető méretei műszaki tervezéshez. 1. rész: Testméret-meghatározások és mérési pontok (ISO 7250-1:2017.)*
- [6] *MSZ EN 547-2:1996+A1:2009 Gépek biztonsága. Az emberi test méretei. 2. rész: A hozzáférési nyílások méretezésének alapelvei.*

- [7] FERREIRA, T. M. – VICENTE, R. – DA SILVA, J. A. R. M. – VARUM, H. – COSTA, A. – MAIO, R.: Urban fire risk: Evaluation and emergency planning. *Journal of Cultural Heritage*, 20 (2016), 739–745. DOI: <https://doi.org/10.1016/j.culher.2016.01.011>
- [8] MYBURGH, H. M. – JACOBS, H. E.: Water for firefighting in five South African towns. *Water SA*, 40 1 (2014), 11–18. DOI: <https://doi.org/10.4314/wsa.v40i1.2>
- [9] ZHOU, J. – RENIERS, G.: Simulation analysis of the use of emergency resources during the emergency response to a major fire. *Journal of Loss Prevention in the Process Industries*, 44 (2016), 1–11. DOI: <https://doi.org/10.1016/j.jlp.2016.08.007>
- [10] WANG, C-P. – SHIH, B-J.: Research on the Integration of Fire Water Supply. *Procedia Engineering*, 211 (2018), 778–787. DOI: <https://doi.org/10.1016/j.proeng.2017.12.075>
- [11] HYUN, I.-H. – CHEON, S. – KIM, D. – SECK, D. – CHOI, S.: Improvement of Fire Hydrant Design to Enhance Water Main Flushing. *Procedia Engineering*, 70 (2014), 857–863. DOI: <https://doi.org/10.1016/j.proeng.2014.02.094>
- [12] HASSANAIN, M. A. – HAFEEZ, M. A. – SANANI-ANIBIRE, M. O.: A ranking system for fire safety performance of student housing facilities. *Safety Science*, 92 (2017), 116–127. DOI: <https://doi.org/10.1016/j.ssci.2016.10.002>
- [13] SIERRA, F. J. M. – RUBIO-ROMERO, J. C. – GÁMEZ, M. C. R.: Status of facilities for fire safety in hotels. *Safety Science*, 50 7 (2012), 1490–1494. DOI: <https://doi.org/10.1016/j.ssci.2012.01.006>
- [14] SMITH, J. A.: Preparing for winter: Proactive measures to prevent injury and property damage. *Professional Safety*, 42 8 (1997), 28–32.
- [15] SZABÓ Gy.: *A katonai szolgálatból származó fizikai terhelés értékelésének módszerei.* (Doktori értekezés) Budapest, NKE, 2013.
- [16] PHEASANT, S.: *Bodyspace Anthropometry, Ergonomics and the Design of Work.* London, Taylor & Francis, 2003.
- [17] RESTÁS Á.: Tűzoltók szemtől szemben az érintettekkel: Viselkedésformák tűz- és káreseteknél. *Bolyai Szemle*, 13 3 (2014), 25–35.
- [18] BÉRCZI L. – PAPP CS. L.: A mentő tűzvédelem diszlokációja a valóságos fehér foltok függvényében. *Védelem – Katasztrófavédelmi Szemle*, 20 2 (2013), 9–11.
- [19] ÉRCES G. – KOMJÁTHY L.: Mérnöki módszerek szerepe a felszíni alatti vasútvonalak tűzvédelmi helyzetének alakulásában. *Hadmérnök*, 13 4 (2018), 191–198.
- [20] HAGEBÖLLING, D.: *Taschenbuch betrieblicher Brandschutz.* Essen, Vulkan Verlag, 1999.
- [21] *MSZ EN 547-3:1996+A1:2009 Gépek biztonsága. Az emberi test méretei.* 3. rész: Testméretek.
- [22] FIDY J. – MAKARA G.: *Biostatistika.* Budapest, InforMed 2002 Kft, 2005.
- [23] HERCZEG G.: Tűzvédelmi eszközök optimális elhelyezésének antropometriai meghatározása. *Hadmérnök*, 13 3 (2018), 18–27.
- [24] *NFPA 1142 Water supplies for suburban and rural fire fighting. 2017 edition.* www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1142 (Downloaded 30.04.2019)
- [25] *NFPA 14 Installation of standpipe and hose systems.* 2019 edition. www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=14 (Downloaded 02.05.2019)
- [26] HERCZEG G.: TvMI használati szabályokról I. – Tűzvédelmi eszközök hozzáférhetősége. *Védelem – Katasztrófavédelmi Szemle*, 23 5 (2016), 12–16.

- [27] MSZ EN 15889:2011 Tűzoltó tömlők. Vizsgálati módszerek.
- [28] MSZ 1185:2016 Tűzoltó tömlők. Vízáró lapos nyomótömlők és szerelt tömlők tűzoltó szivattyúkhöz és -járművekhez.
- [29] 3/2015. (VI. 8.) BM OKF utasítás a tűzoltóságok Szerelési Szabályzatáról.
- [30] MSZ 9771-3:2009 Tűzcsapok és tartozékaik. 3. rész: Tűzcsapkulcsok.
- [31] HANSEN, D. J.: *Occupational Health Fundamentals*. s. l. CRC Press, 1991.
- [32] NAGY G.: Heros Aquarex S10 vízszállító gépjármű. *Védelem – Katasztrófavédelmi Szemle*, 26 1 (2019), 59–61.
- [33] Council Directive 96/53/EC of 25 July 1996 laying down for certain road vehicles circulating within the Community the maximum authorized dimensions in national and international traffic and the maximum authorized weights in international traffic. *Official Journal*, L 235, 17 9 (1996), 59–75.
- [34] MSZ 1078:1971 Tűzoltó szívótömlő.
- [35] MSZ EN ISO 14557:2003 Tűzoltótömlő. Gumi és műanyag szívótömlők és tömlőszerelvények.

Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment

Ferenc KOCZKA¹

Regarding the Internet, individuals expect anonymity and confidentiality, but the authorities expect as much traceability as possible. Individuals are provided with encryption procedures used in internet communication, supported by more and more efficient devices and applications. For law enforcement, the publicity of these procedures could be a serious problem. However, in addition to a well-functioning technical background, conscious use of tools is required to maintain anonymity. In this article I present the necessary techniques to achieve this goal, their operational principles, scopes and points that may enable the technology to be compromised. In the second part of this article, the partial results of my research will be presented, which measures the presence and activity of the darknet; it can provide a basis for carrying out similar investigations and can help develop the protection process.

Keywords: darknet, VPN, TOR, onion routing, electronic warfare.

Introduction

The supervision and military use of cyberspace is necessary not only in defence, but also in the achievement of information superiority, and is in the primary interest of all countries. This fact has been recognised by the military leadership of many countries and they elaborated, at least partially, some kind of strategy for warfare in cyberspace. In each of these strategies, there is a clear integrative effort to handle the potential and the threats of cyberspace in line with traditional military infrastructures and activities. The supervision and control of cyberspace is an essential task, but given the previously unimaginable amount of data and quite varied communication methods, this requires a fundamentally new approach.

Previously, tools and procedures developed for military purposes in civilian life were typically not available, at most only with a long delay. However, with regard to cyberspace, this is not the case: there are public procedures for encrypting, obfuscating and concealing data and preserving confidentiality, against which the major military powers do not have an effective means of defence.

¹ IT director at Eszterházy Károly University; e-mail: koczka.ferenc@uni-eszterhazy.hu; ORCID: <https://orcid.org/0000-0002-7541-6495>

The darknet may play a special role in certain areas of information operations. Although the darknet is based on military development, its potential can be used against anyone, including its creator. The purpose of this article is to review darknet, to raise awareness of the military application capabilities, functionality and scope of darknet, and to present the results of a measurement that examined the presence and use of darknet. In doing so, I use a combined research paradigm. First, by means of a deductive research strategy, I review the main characteristics of darknet, and then comes, in the context of inductive logic, the case study and the cross-sectional study. I examined a large section of domestic higher education using the logfile analysis method in Eszterházy Károly University on this issue.

Layers of the Web

With the rapid development of the Internet, the number of computers connected to the network is also growing rapidly; some sources say that in September 2019, 58% of the total population of the Earth, 4.33 billion people, had Internet access. [1] This technical opportunity brought along a number of applications that have become decisive for the daily existence of mankind and have made many previous methods or resources outdated or replaced them with new ones. The most popular service is still the web, which has become an interactive and dynamic service that combines a wide range of technologies from the initial simple and static descriptive html base. The number of websites has exploded, with approximately 1.7 billion sites operating. When writing these lines, [2] finding the necessary information and navigating them was a problem from the outset. In the early stages of the Internet, it was advisable to use various collection sites, which were later almost completely replaced by search engines²—the extent of their dominance is illustrated by the fact that today, when developing websites, developers need to take their expectations into account. Search engines work based on background programs (so-called bots) that continuously monitor the entire web space and collect its data into their database that is the base of searching processes. The set of websites to be visited by search bots is mainly from internet name servers,³ which are supplemented by links found in processed web pages. Therefore, search engines are far from being able to map the entire web universe, leaving many websites invisible to them—some sources consider the number of visible websites to be 4% of the total web.

From the perspective of access, web content is classified into three different classes. Open access websites and contents that search engines find are called surface web.

Web contents that use surface web technology but are invisible to search engines are a second layer called the deep web. Invisibility can be for many reasons, including pages

² The first really popular search engine was Altavista (<http://altavista.com>), founded in 1995. Its rivals (Google, Bing, Yahoo, etc.) used much better technologies, so it was pointless to maintain it. The name has been owned by Yahoo since 2003.

³ Name servers (DNS servers) store internet names that represent the addresses of websites. Naming is not technically indispensable, but their absence would make it difficult to access pages because, among other limitations, they could only be referenced with an IP address. Therefore, websites containing public information always have DNS names, which is an ideal starting point for search engines.

protected⁴ by the password or captcha, contents available only after registration, personal accounts, private cloud storage, virtual offices, content returned based on search for each page, results of database queries and responses returned to non-http or https. Web contents that are not shown by any external links or DNS entries remain invisible for search engines. The deep web and surface web operate with the same technology and therefore do not provide anonymity to the service provider or the party that uses it. It is not ideal to display non-public content because of this, although there are exceptions.⁵

The third layer is also invisible to search engines, because its network technology is different from that used in the previous two layers, so you need specialised software to reach it. This part of the Internet, called darknet, was created for a double purpose. On the one hand, it provides anonymity to the person who browses, so that the identity of the content service server operator is hidden. On the other hand, it is to hide servers, in which darknet's infrastructure ensures that the exact location of content servers cannot be determined during their operation. The infrastructure implemented by darknet requires a software specialised for this purpose, and traditional browsers cannot be used to access web pages that are operated there.

Darknet's assessment is controversial, as the need for anonymity subsists in practice in four main areas. On the one hand, it acts as a means of avoiding network control and censorship in repressive regimes and provides anonymity to users who need to be cautious. It is also to secure sensitive data transmission, server hiding, and data leaking. Darknet's client-side anonymity feature has been used by the New York Times from 2017, the BBC from 2019, and other newspapers followed. [3, 4] In Hungary, it is used in investigative journalism to receive content in which the identity of the person who leaks the data is to be hidden. [5] China's internet restrictions are well known, but this feature also plays a great role in other countries, such as Saudi Arabia, because of restrictions and monitoring of networks. [6] In these countries, restrictions on access to web content can be circumvented using darknet,⁶ so the DuckDuckGo search engine is available as an alternative to Google, as well as the alternative Facebook,⁷ which already received one million visitors a month in 2016.

Darknet also provides servers with anonymity, which is also an excellent opportunity for criminals. Based on its concealment capabilities, their services can be hidden and operate with great certainty, leaving its exact location undetectable. In this part of cyberspace, all types of illegal activities can be carried out which do not require a personal presence: from trade in credit card data, drugs, ransomware and organs to the distribution of drugs, weapons, information and raw materials, all are available. Darknet protects Wikileaks documents,⁸ 3D-printed weapons files, and many other areas of crime that go beyond the scope of this article. The veracity of the services that criminals provide is always doubtful, sellers are unknown in the protection of technology, and there is no possibility of a claim

⁴ Captcha is a control question that computer programs are currently unable to answer. Typical examples are hard-to-recognise texts, possibly counting tasks.

⁵ There are a number of websites that publish illegal—or at least questionable—content through the internet service provider that runs them on the surface web, with the ISP running them operating in one of the developed countries. For example, Satan's Temple at <https://www.churchofsatan.com>. The Inspire Magazine is now usually distributed on publicly accessed but hacked websites.

⁶ Source: <http://3g2upl4pq6kufc4m.onion/>

⁷ Source: www.facebookcorewwi.onion/

⁸ WikiLeaks is available at <http://suw74isz7wqzpmgu.onion>

or a guarantee. There are several attempts to infect the visitor's computer, steal data, and install malware. Since the payment for illegal services is usually made in a cryptocurrency, they often try to access crypto wallets using sophisticated methods on darknet. They analyse the contents of the clipboard and try to exchange the identification code for bitcoin wallets found therein, or to publish and hijack the payment process with a modified browser which they have manipulated. [7]

The interests of national defence justifies research on the issue in order to monitor or possibly prevent the functioning of darknet and its alternatives, and to develop control and eradication options for illegal activities carried out there.

Implementation Options

There are several ways to implement anonymity and confidentiality. The Tor Browser is certainly the best-known browser for web use, which builds on the Tor protocol to hide the IP address of the browsing machine. This browser is actually a modified Firefox that connects with the target web server via the Tor network and initiates the download of the page. Tor Browser functionality can be reached with plug-ins for other browsers. From an operational point of view, I2P and FreeNet are alternatives, both of which require a combined infrastructure for service users to provide anonymity insurance.

Another solution is to channel data traffic into an encrypted channel, typically based on a VPN server. The two leading providers of VPN⁹ solutions today are ExpressVPN and NordVPN.¹⁰ When using such a service, the client traffic is transferred through one of the VPN provider's servers and transmits its requests (even twice) to service providers in the encrypted form. The request is sent to the destination server by the VPN provider's server so that they can only identify its IP address. The target server returns its response to the VPN server, which sends it back to the client. Client anonymity is guaranteed by the logging strategy provided by the VPN provider, and it is questionable whether, in critical cases, it can help authorities to establish the identity of the person requesting anonymity.

Both solutions have advantages and disadvantages, but since they can be used together, it is recommended to combine them to improve the security of anonymity.

Other methods of anonymous access also exist: the so-called on-the-go operating systems can be installed on a CD or USB drive on any machine, with only the most necessary information available to others.

Chat software that provides encrypted communications are another situation, some of which are based on central servers, while others rely on peer-to-peer relationships. Their best-known representatives are Telegram, Tox and Signal, which was considered the safest by Edward Snowden.

The range of softwares aimed at encrypted communications and user anonymisation is expanded from time to time, so that people who wish to use it can easily find another alternative when a system is compromised. However, an error in the principles or even in the implementation of a particular software easily results in a loss of confidentiality.

⁹ Source: www.expressvpn.com

¹⁰ Source: <https://nordvpn.com>

The TOR

Tor stands for *The Onion Router*, developed by United States Naval Research Laboratory (NRL) to protect government communications in the mid-1990s. The first publicly available version was released in 2002. The source code was later made free by the NRL, opening the door to a wide spread and further development. The development continued in 2006 by The Tor Project, a non-profit organisation that develops and maintains Tor today, although in 2016 the entire development team quit and their positions were replaced by others.

The Tor network is based on a system of independent Tor nodes. The basic task of such a node is to ensure the encrypted transmission of data packets flowing through it to an adjacent node, which is currently done with a 128-bit symmetrical key.

Some nodes are configured differently, so they play a prominent role: they can be used to exit the public Internet, i.e. these points provide a connection to the surface and deep internet, so they are used as exit nodes.

The Tor network is therefore based on encrypted traffic between each node, so that the order of the nodes in that relationship will only be the same during a session. This feature is performed by a single component, the Tor browser, while for alternative implementations, the browser and the component for maintaining the network can be implemented in two separate softwares. The nodes that participate in the sessions are selected by the client itself (the so-called initiator). This step queries a list¹¹ of guard nodes that serve as the entry points from one of the Tor directory servers,¹² then, based on this knowledge, selects the nine machines and exit points that you will use in that session.

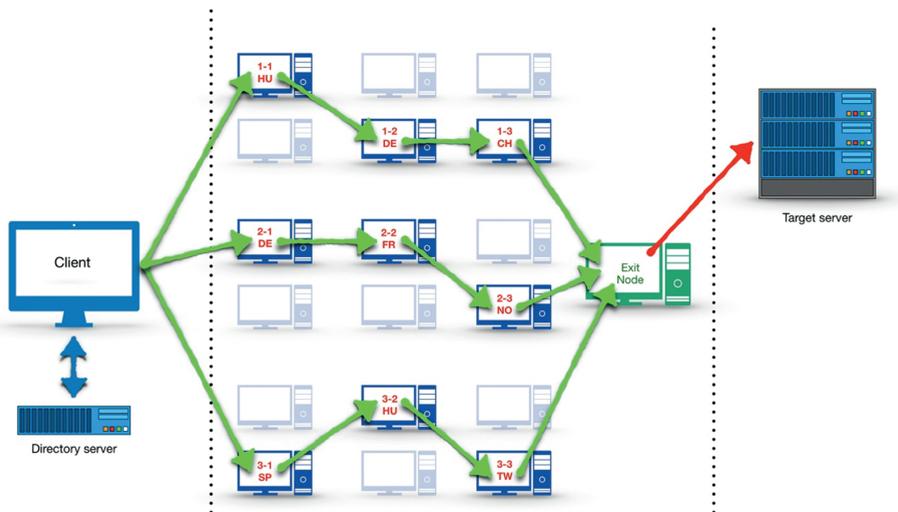


Figure 1. *How the Tor protocol works.* [Created by the author.]

¹¹ Their current list is available at: www.dan.me.uk/torlist/

¹² There are a number of rules when choosing nodes. On the one hand, they must be a sufficient distance apart, i.e. they must not be in the same subnet of /16. Guard nodes must be privileged nodes since they know the IP address of the client.

Tor's encryption method is different from the general method. As a first step, the initiator generates a master key to encrypt the data package that it must send over the network. After that it appends the master key to the encrypted package, then cuts the resulting package into three parts and starts them on the previously generated route (circuit). The method ensures that the master key required to decode the contents of the package is never fully present on any node. Each node encrypts the part of the subpackage that is on it over and over again, while also adding the key needed to decrypt the encryption. Thus, each of the keys used by each node is included in the transferred sub-data pack, so any node can decode the subpackage encrypted by the previous ones, but since it contains only a third of the original master key as a last resort, no node is able to restore the original data package even partially. According to the protocol, the subpackages will pass through 3–3–3 nodes by the time they get to the exit node. The exit node decodes all three subpackages backwards based on the previous ones and can match the original encrypted data packet and master key with the three subpackages. This will complete the final step of restoring the original data package, which the exit node delivers to the destination server over the open internet. The word onion on behalf of the Tor refers to this structure: the encryption layers of nodes are layered in the same way as the onion layers.

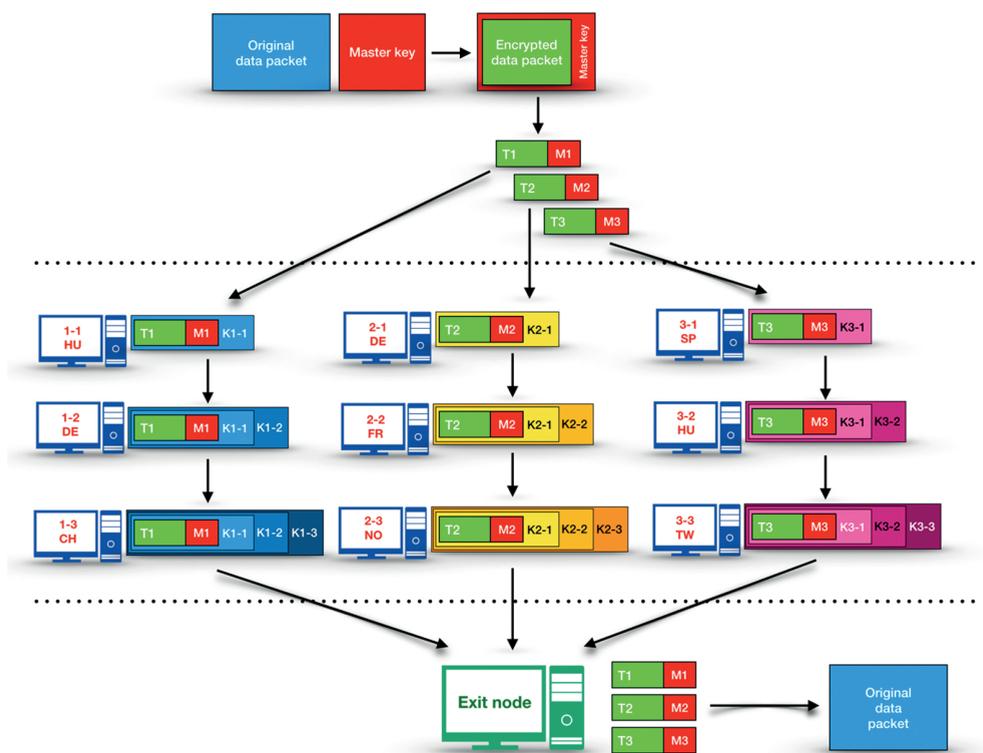


Figure 2. *Tor's encryption model.* [Created by the author.]

Based on the above, beyond exit points, the Tor no longer provides encryption on the Internet, so data traffic between the exit node and the destination server will be open or encrypted depending on the transfer protocol. Therefore, if you need confidentiality, Tor browser should not be used to visit websites which are available on the open Internet and to which the connection is not made via https.

The selection of nodes in each packet was initially random, but according to the Tor protocol specification, the exit node is first determined to make sure it has a connection to the destination. [8]

Based on the above, the logs of a computer serving a web page include only IP addresses for exit points when browsing with Tor Browser instead of the address of the computer that initiated the connection. Therefore, tracing network traffic is available up to this point. Moreover, the addresses of the exit points change from time to time, making it even more difficult to identify. This can be found in the following example: a few lines of a web server log are shown below and each connection was made by different clients. The first items in the log lines are the IP addresses of the computers which download the pages; all three addresses in this example are one of the exit points on the Tor network. [9]

```
198.98.50.112 - - [30/Sep/2019:20:12:26 +0200] "GET / HTTP/1.1" 20...
198.98.50.112 - - [30/Sep/2019:20:12:31 +0200] "GET /favicon.ico H...
109.70.100.29 - - [30/Sep/2019:20:12:38 +0200] "GET /?module=cStat...
109.70.100.29 - - [30/Sep/2019:20:12:39 +0200] "GET /templates/fva...
51.15.106.67 - - [30/Sep/2019:20:12:52 +0200] "GET /?module=cISP&...
51.15.106.67 - - [30/Sep/2019:20:12:53 +0200] "GET /templates/fva...
```

Exit points are located in different parts of the Internet. Therefore, the Tor browser automatically bypasses protections which block network connections by a source IP to ensure that a website is not available from specific countries.¹³

Hidden Services of Tor

Tor allows for hidden services (so-called onion services). These are in most cases websites, file sharing, or chat services whose servers cannot be physically located. [10] Hidden services are based on a more complex mechanism that requires the introduction of new communication elements in addition to the creation of previously presented circuits; along with the three introduction points, a rendezvous point is required. [11]

In the case of this use of the Tor network, the addressing of hidden servers is also different from the public Internet DNS system. [12] In traditional DNS, names are included in a hierarchically distributed database, all elements of which are legally managed by the name owner. In a network that provides anonymity, this type of name resolution cannot be provided due to the operation of the logging mechanisms, so the Tor network provides a special method for addressing servers that do not require DNS servers. The name service

¹³ For example, the Pandora music site (www.pandora.com) is not available from Hungary.

provided in this way is similar to that used in traditional DNS but introduces a special ending: “.onion”.

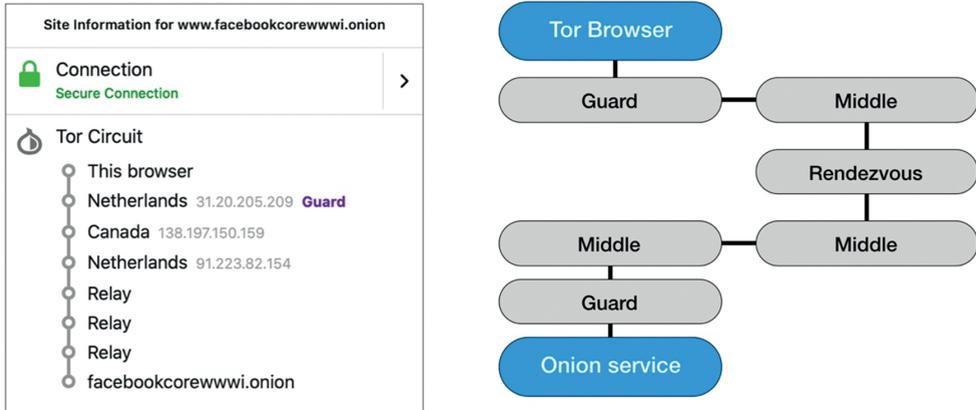


Figure 3. A path of an Onion service. [Created by the author.]

The name of the hidden server is formed by an algorithmic path. The name of the server is the Base64 encoded first half of the sha-1 hash of the public key used for communication. This is why the names of servers on the Tor network are not meaningful, easy-to-remember strings. [13, 14] It is possible to create memorable names, but this requires a reverse procedure: the name must be found by trying the above procedure. Finding a key pair for that name requires a lot of computing resources, so most names which were created in this way only refer to the feature in a few characters. According to some calculations, approximately 2.6 million years is required to produce a desired name of 14 characters long, “facebookcorewwi.onion” used for Facebook is merely the result of a lucky coincidence. [15]

Therefore, IP addressing is only relevant in the lower network layer of the service, and this addressing is no longer relevant to the layers above it, so methods which can work in traditional IP networks are not useable for forensic investigations.

Attack Points

The existence of the Tor network is therefore an advantage on the one hand and a disadvantage for governments on the other hand. PSYOP¹⁴ operations can easily and safely deliver information to targeted areas. Certain types of crimes can be committed without leaving cyberspace. Darknet services play an important role in the communication, financial manoeuvres and fraud management of criminals and terrorist organisations. It is in the interest of repressive regimes to make it impossible to operate, so several measures have been

¹⁴ PSYOP stands for psychological operations, which is based on the information provided to the party to be affected. “In short, PSYOP is the function of the DOD devoted to changing attitudes and behaviour in foreign target audiences; it is frequently described as propaganda outside the military.” [16]

taken to achieve this. Bypassing anonymity provided by the Tor network may be a priority for both clients and servers of many national defence and law enforcement organisations. Although, from a technical point of view, Tor is safe, it is possible to successfully attack its users and reveal their identity at several points, as evidenced by several previous examples.

Since most Tor users are not aware of the exact functionality of the technology, there is a good chance that in the long term they will not follow all precautions. The use of the technology keeps them in the misconception that their activities will remain hidden in all circumstances. Human mistakes can be made, and if the authorities are willing to invest a great deal of energy, it allows identification in the long term. Some operators of darknet's largest illegal commercial sites have become identified not because of technological but human error.

One of the best-known drug distribution sites was Silk Road, launched in 2011. In 2013, its operator was identified as a result of a banal error: in a forum post, he used his known darknet name at the same time with his real email address.¹⁵ [17] It has made more than \$1 billion in sales over its two-and-a-half-year operation, its operator Ross Ulbricht was sentenced to life in prison in the US.

Faith in the anonymity of cryptocurrencies also proved false: tracking its use made it possible to capture one of darknet's most trafficked child site operators in 2019. [18] This case, if the authorities' claim is accepted, fundamentally calls into question the full confidence in blockchain payments.

Exit nodes are the Achilles heels of the Tor network. If an attacker can take control of such a node due to a possible poor configuration or vulnerability, it can intercept unencrypted data passing through it. It is a good option for authorities wishing to supervise the use of Tor to create or maintain an exit point already set up for attack purposes. This opportunity was demonstrated by Dan Egerstad in 2006, who obtained identifiers and passwords belonging to various embassies, among others the Dalai Lama's office and India's Defence, Research and Development Office. [19, 20] To prevent attacks in this direction, exit points that are unsafe are provided, together with other exit nodes, with BadExit flags and can be filtered on an online map. [21]

To narrow the boundaries of the deepnet and the darknet, search engines use a number of methods that may in some cases prove highly effective. Google, Microsoft and Apple are also trying to do everything they can to collect a lot of data about their customers beyond their browsing habits and geographical location. A huge set of tools are deployed to achieve this goal. In most cases, this is based on the provision of a valuable service to the customer and the requirement of more or less personal data necessary for operation.

Google provides a number of services free of charge, which, by the way, can identify users. They developed their own browser including a sign-in feature. This provides a range of convenient services—storing passwords, organising visited websites—and provides the perfect environment for profiling the user. In addition to the search service, Google's expansion strategy now extends to video streaming (YouTube) for their music service (Google Play Music) and the cloud service for file storage (Google Drive). There are a number of other services that indirectly provide information to implement the profiling

¹⁵ Source: <https://bitcointalk.org/index.php?action=profile;u=3905;sa=showPosts;start=0>

of users. Google stores all the personal activities in their systems which can be traced back later.¹⁶

In addition to the above, a number of other methods are used to gather as much information as possible. Through the free DNS service,¹⁷ any computer activity that requires name resolution will be known to Google servers. This will inform Google's system about which websites its customers visit as well as which other servers are accessed when using other services. The same service reveals entry points for Google for pages on the deepnet that were previously unknown to them. The free image service lets them analyse millions of images. In these images, the people can be easily identified by facial recognition which, by developing AI, opens up new horizons for them.

The geographical situation of visitors is also known to them. In addition to Google, Apple and Microsoft maintain a database of the hardware addresses of WiFi routers whose geographic location has previously been determined using a device with a GPS receiver. Based on this, they can determine the position of any WiFi device that was once connected by a GPS-enabled mobile phone, but even this is not necessary: Cars which have collected data for Google Street View also have detected and built a database about WiFi routers with their SSIDs¹⁸ and hardware addresses. [22] Moreover, there is no suitable method for avoiding such data collection in real circumstances.

Some traditional hacking tools, such as keyloggers, can easily bypass the protection methods that provide anonymity. DNS also poses vulnerability for anonymous browsers. If a DNS service defines "onion TLD" in its namespace and registers an onion service address originated from the Tor network, traffic from browsers can be hijacked to a prepared web page outside the Tor network, and that method may lead to the loss of anonymity.

The Tor network could also create a major vulnerability in the protection of IT systems. In addition to the ability to bypass many firewall services, the onion service installed in networks (even a virtual server behind NAT)¹⁹ can maintain a continuous connection to the Tor network. This opens the possibility of access to the protected network without operators enabling it in the firewall configuration. In general practice, a more permissive set of rules is applied to guard protected networks behind firewalls, so launching a hidden service could be the starting point for further attacks. The firewalls don't detect anything from the inward connections because of the contact from behind them.

Knowing the security flaws of individual systems in electronic warfare can be of paramount importance in cyberspace warfare, so they move extremely large resources to achieve a positive position. Software and devices exploiting vulnerabilities are cyber weapons based on which complex cyberattacks can be built. [23] Software enabling vulnerabilities to be exploitable have become commercial products, several companies are involved in their research, acquisition and sale.²⁰ NSA's XKeyScore system analyses traffic running through more than 700 servers around the world in around 150 key positions during

¹⁶ Source: <https://myactivity.google.com/myactivity>

¹⁷ IP addresses of Google's free name servers are 8.8.8.8 and 8.8.4.4.

¹⁸ Service Set Identifier. During the wireless network service, the short name used to identify the device and the service.

¹⁹ NAT: Network Address Translation. A commonly used method for hiding networks from others. Behind the NAT device computers do not have a public IP address and cannot be accessed from outside the network.

²⁰ Zerodium offers extremely high fees for a remotely exploitable new vulnerability on the <https://zerodium.com/program.html> site.

normal Internet usage. Based on the content that runs through it, it creates fingerprints of individual users; in order to activate it one simply needs to visit the Tor or Linux Journal websites. [24] These systems have the means of data collection and triggering capabilities that make it impossible for a person to maintain anonymity for the entire life cycle.

Motion data recorded by GPS-enabled mobile devices can identify their owner without linking them to other databases. Places visited regularly, areas of work, the coordinates of the apartment and their location at a specific time make the person's movement habits precisely identifiable, [25] and compared to the movement of other devices and also his contacts, can pose a serious national security problem.

Based on the examples above, it is clear that internet activity can clearly identify users of the services. It can be said that darknet activity links even a single faulty technical movement when using darknet to one of its other profiles in consideration with the data collected previously. The result of this will be the loss of anonymity.

Application Options

NATO decided at the 2016 Warsaw Summit to declare cyberspace an operational area. [26] The data collection techniques presented so far exemplify the fact that there are a number of possibilities for monitoring and controlling cyberspace, focusing primarily on the hands of the world's leading multinational companies. As cyberspace as an operational area has already been raised, preparations for strategies for it have already begun in several countries, including China and the United States. The question arises as to what cyberspace operations darknet's public services may influence, how they can be used to achieve and maintain cyber superiority, and how they can be used in defensive and offensive operations.

Cyberspace operations are presented in nine main areas that can work in layers of physical, logical, and cyber personality, that make up the structure of cyberspace. [27]

The physical layer is made up of geographical and network elements. Since darknet's operation is based on public internet infrastructure—and its services are provided in the higher tiers—this layer has no significant impact.

Darknet elements are firmly represented in the logical and cyber personality layers. The logical layer includes darknet network infrastructure, protocols that implement anonymity and hiding, and their softwares. On the top, in the cyber personality layer, there are programs which provide the services, e.g. the Tor browser. Darknet services should therefore be taken into account when carrying out cyberspace operations.

In *computer network exploitation*, the aim is to collect as much data as possible and transfer it to processing centres where the data is processed. Darknet's logical infrastructure may play a role in this operation, because it can be used to maintain data connections for which standard firewalls are not an obstacle. Although such a connection does not require significant computing performance, simple IoT devices do not contain enough resources to operate in darknet. On a slightly stronger hardware, with long-term power supply, this connection can be maintained for a longer period of time.

Detection of traffic at a darknet endpoint within a network is not trivial in a network environment that maintains a number of connections with the outside world. Therefore, a minicomputer created to build and maintain a darknet connection is remotely accessible,

opening a backdoor for the attacker. A minicomputer's fast, high-level operating system can run complex softwares. If such a machine is located in a computer network, its darknet traffic is difficult to locate in the case of a carefully configured system and may play an active role in violating any element of the CIA²¹ triad.

After the successful installation or placement of such a machine, operational security can be attacked at several points, especially in the field of transmission and network security. The most common of these include—but are not limited to—partial detection of network infrastructure, interception and partial analysis of traffic, collection and transmission of sensitive information in the event of open data transmission, conduct of disruptive activity, services redirecting, deceiving, sending malware to additional network components; but it is also much easier to exploit other security problems from a machine in the internal domain of the network.

Darknet can play an important role in carrying out psychological operations. In doing so, the aim is to provide information to the opposing party that may affect their behaviour, motivations and emotions. PSYOP includes messages of propaganda: white propaganda is the delivery of clearly worded, credible information to the target audience, the purpose of black propaganda is essentially manipulation, the source and content of the information communicated is not real. And grey propaganda seeks to influence the thinking of the target audience by operating with partial truths and time shifts.

Darknet operational capabilities in PSYOP are also to be considered in defence, but may play a role primarily in offensive operations. Because such a server can be created and operated at an extremely low cost, it is therefore highly suitable for creating sources of information that support these operations in such a way that it can only be prevented by serious difficulties concerning the dissemination of information. Hidden services ensure the anonymity of the source of the information, so that the target persons do not have the opportunity to have accurate information about the authenticity of the source and the real entity behind the information. Therefore, this technology is used successfully in grey and black propaganda.

In white propaganda and in the media, darknet's ability to anonymise the target can be used to protect the target, allowing the sender to transmit real information without being detected by authorities.

However, darknet is not generally known and is much more difficult to use. The address of the wanted website is difficult to memorise. Therefore, darknet cannot be effective without education having been organised before it is used, for which other channels should be used.

Analysing Tor Traffic

Tor network statistics are available on Tor Metrics, [28] where the network's operating parameters have been published. Looking back to recent years, there have been several periods in which traffic has increased significantly. There has been a strong increase from September 2013, with the usually 800,000-strong user camp swollen to 5 million over

²¹ Confidentiality, integrity and availability.

a short period of time. This was not of social, but of a technical nature. The Mevade/Sefnit botnet, which spread during that period, was communicating on darknet, so the increased user number represented the number of infected machines. In a later version of the botnet, SSH was used, so the load on the Tor network also dropped to normal. Publishing technical enhancements has brought about a similar change: the appearance of the Snowflake plugin for browsers has inspired many users to try it out, which could be seen in Tor Metrics charts for a short period of time.

Monitoring the user number and Tor network load during cyber protection can provide useful information about when a malware appears and when it communicates over the Tor network; monitoring of this could be important for an organisation's IT operators.

Tor usage rate can be measured by network traffic.²² I could not find any current research publishing the results of such a measurement, so I developed a methodology for this and measured the volume of traffic sent to and from the Tor network for six weeks at Eszterházy Károly University. I evaluated the data by analysing logfiles; during the evaluation, I processed them with shell scripts based on Unix filters. The objectives of the investigation were as follows:

- Description of the amount, nature and volume of traffic coming into the University's network from the Tor network.
- Quantification of the use of the Tor network by university students and staff.
- Detection of the appearance of an onion service or exit point and determination of the detection methodology.
- Comparison of attack traffic from the Tor network and public internet.
- Assessment of the situation revealed in the course of measurements, elaboration of a strategy and drawing of possible conclusions.

I collected the data on which the measurement was based in logfiles. To extend the logging mechanism, it was necessary to change the settings of the university's central routers. Setting up the measurement configuration was based on the fact that the Tor network hides only the user on the one hand and the website you visit on the other, and not the fact of using the Tor network.

Data sources from the Tor network can be clearly identified as this list is made available continuously by network operators in an easy-to-process form.²³ Because exit points can change, its set needs to be updated with a script which runs at least every day. During the measurement, we recorded the IP addresses of source exit nodes, the target computer of each data package, and the target port. The destination port provides information about the service of the university network, e.g. viewing a website or attempting to access a server management interface.

In analysing the nature of traffic, we found that HTTP and SSH traffic dominated as 99% of the darknet traffic is directed at them. This is unexpected given that there are several services known from previous vulnerabilities in the university network. Attacks based on exploiting DNS vulnerabilities belong to the most effective methods, and the RDP protocol

²² Detection of solutions concerning the previously presented VPN connections is beyond the scope of my investigation.

²³ The list of Tor exit nodes is available on <https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1> website.

has been a priority in the forecasts for 2019. [29] Despite this, the number of attacks directed to these services from the darknet was minimal.

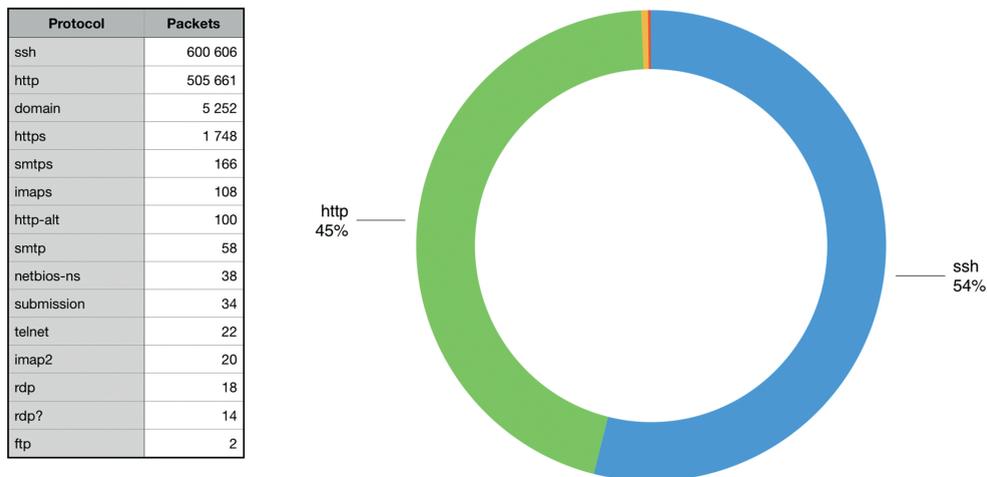


Figure 4. *The protocol distribution of darknet traffic.* [Created by the author.]

According to further measurements, data packets to e-mail softwares were in a similarly low number. The number of spams did not decrease noticeably in recent years, but there is no need to send mail on the darknet. Due to the operation of the SMTP²⁴ protocol, they can be efficiently distributed on the public Internet and the darknet is not ideal for transmission of large amounts of mail data in a short period of time.

RDP and SSH protocols allow remote logon typically to server computers. SSH is very prevalent in remote management of Unix-based systems, so this connectivity is in most cases thoroughly protected and there is extensive documentation of its methods on the Internet. Thus, from changing the service default port to disabling administrative logins and combining failed login attempts with firewall rules, there are many protection options available. However, it is not expected that a legal request for connections from the darknet will be necessary. These connections are predominantly from softwares that attempt to get valid login information. Darknet infrastructure provides a hide-and-hide service for its runners.

In order to ensure risk-proportionate protection, the number and type of attack attempts from the public Internet direction should be examined and compared with those from the direction of darknet. Because most traffic from the public Internet is legal, the method used to measure darknet traffic cannot be used. The solution is the use of honeypot. This is a computer that shows a real service operation to an attacker by allowing known errors to be exploited or a successful login.²⁵ Honeypots are important parts of identifying and monitoring the initial activity of new malwares. SSH and HTTP traffic were measured

²⁴ SMTP is a collection of rules for e-mail posting.

²⁵ Sshesame is a ssh server that provides the attacker with seemingly successful login.

with a honeypot. The results of the investigation in the given period are shown in the table below:

Table 1. *Comparison of darknet and public Internet traffic for SSH and HTTP protocols*
[Created by the author.]

Protocol	Darknet	Public net
ssh	600,606	2,091,682
http	505,661	200,885

It is important that the traffic data of the public net applied to a single computer (to the honeypot), while attack attempts from the darknet were directed to the entire university network, which includes approximately 1,500 computers. Thus, it can be concluded that during this period the maximum attack traffic from darknet was only a fraction of the number of attacks from the public internet.

Examination of Tor relations initiated from the university also yielded informative results. This was also measured by analysing the traffic of a central router, in which we examined only connections where clients did not embed their Tor traffic into a VPN tunnel. In the latter case, because of the encrypted content, it is not possible to determine the real target of the network traffic. Two methods are available: checking the traffic of its default outbound port, or using the addresses of the guard nodes.

In measuring traffic, it was found that approximately 196 connections were initiated during the investigated period, which came mostly from the author, so we could not report significant darknet activity by the client during the period under consideration.

The appearance of a server providing onion service is rather difficult to identify. According to the protocol, this traffic can be linked to guard node traffic, but by using the VPN solutions already presented, the operator can provide an additional hiding procedure. From the monitoring of guard node traffic and its comparison to other data, gained e.g. from observation of 24-hour traffic, it is likely that such a server will operate. Along similar principles, the internal source of an ongoing VPN connection should also be checked.

Conclusions

Encryption of internet traffic, anonymisation services and public availability of procedures providing encrypted connections without central servers transform the work of national security and law enforcement agencies. Former intelligence data collection tools and electronic equipment used for monitoring and listening are expected to solve previously unknown tasks. Public authorities are expected to be aware of the technologies that criminal circles can use under cover and that ensure hidden communication for them.

Blocking or enabling traffic from the darknet is regulated by the IT security policies or the firewall protection policy of many institutions. Act L of 2013 sets frameworks for state and municipal bodies, to which the 41/2015 Regulation of the Ministry of the Interior is added, providing principles for five types of security departments in line with confidentiality, integrity and availability. Rules for critical infrastructures are defined in

Act CLXVI of 2012. Currently, neither these nor other regulations impose restrictions on darknet traffic, so it is currently up to an organisation to decide whether to filter it.

Attacks from the darknet are different in nature from those coming from the public internet. According to my results, it concerns several services and therefore it does not seem appropriate to filter it separately on the servers – the rules enforced on the public internet are sufficient. On this basis, there is no reason to use serious resources in the examined institution to prevent attacks from the darknet.

It could be a good idea to enable web traffic to reach the original destination of the darknet. If it is assumed that persons belonging to groups relevant from the perspective of national security may appear in the organisation, it is worth activating traffic in this direction before an exceptional event indeed occurs. A change in the level of activity may predict preparations for an act. In the case of public and municipal organisations, especially critical infrastructures, it is expected that Tor servers will not be able to operate in their IT systems. In addition to distributing illegal content, their presence can also help attack protected network elements, so detection of their appearance, continuous monitoring and automation of these organisations is an important task.

References

- [1] KEMP, S.: Digital 2019: Internet trends in Q3 2019. *Datareportal*, 2019. <https://datareportal.com/reports/digital-2019-internet-trends-in-q3> (Downloaded: 2.10.2019)
- [2] DEYAN, G.: How Many Websites Are There In 2020. *techjury*, 2019. <https://techjury.net/blog/how-many-websites-are-there/#gref> (Downloaded: 25.10.2019)
- [3] SANDVIK, R.: The New York Times is Now Available as a Tor Onion Service. *NYT Open*, 2017. <https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482> (Downloaded: 11.11.2019)
- [4] BBC News launches ‘dark web’ Tor mirror. *BBC* (online), October 23, 2019. www.bbc.com/news/technology-50150981 (Downloaded: 10.12.2019)
- [5] VANDEKERCKHOVE, W.: Freedom of expression as the “broken promise” of whistleblower protection. *La Revue des Droits de L’Homme*, 10 (2016), 1–17. DOI: <https://doi.org/10.4000/revdh.2680>
- [6] KOCH, R.: Here are all the countries where the government is trying to ban VPNs. *ProtonVPN*, 2018. <https://protonvpn.com/blog/are-vpns-illegal/> (Downloaded: 3.10.2019)
- [7] CHEREPANOV, A.: Fleecing the onion: Darknet shoppers swindled out of bitcoins via trojanized Tor Browser. *We Live Security*, 2019. www.welivesecurity.com/2019/10/18/fleecing-onion-trojanized-tor-browser/ (Downloaded: 25.10.2019)
- [8] DINGLEDINE, R. – MATHEWSON, N.: Tor Path Specification. *Github*, 2019. <https://github.com/torproject/torspec/blob/master/path-spec.txt> (Downloaded: 03.01.2020)
- [9] *List of TOR exit nodes*. <https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1> (Downloaded: 1.10.2019)
- [10] *Onionshare*. <https://onionshare.org> (Downloaded: 20.12.2019)
- [11] WINTER, P. – EDMUNDSON, A. – ROBERTS, L. M. – DUTKOWSKA-ZUK, A. – CHETTY, M. – FEAMSTER, N.: *How Do Tor Users Interact with Onion Services?* 2018. <https://nymity.ch/onion-services/pdf/sec18-onion-services.pdf> (Downloaded: 11.12.2019)

- [12] MOCKAPETRIS, P. V. – DUNLAP, K. J.: Development of the Domain Name System. (Originally published in the Proceedings of SIGCOMM '88.) *Computer Communication Review*, 18 4 (1988), 123–133. www.cs.cornell.edu/people/egs/615/mockapetris.pdf (Downloaded: 12.12.2019)
- [13] *HiddenServiceNames*. <https://trac.torproject.org/projects/tor/wiki/doc/HiddenServiceNames> (Downloaded: 20.12.2019)
- [14] APPELBAUM, J. – MUFFETT, A.: The “.onion” Special-Use Domain Name. *IETF*, 2015. <https://tools.ietf.org/html/rfc7686> (Downloaded: 10.12.2019)
- [15] *Tim Taunbert's Blog*. <https://timtaubert.de/blog/2014/11/using-the-webcrypto-api-to-generate-onion-names-for-tor-hidden-services/> (Downloaded: 10.12.2019)
- [16] COOK, C. – COVEN, D.: What's in a Name? Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change. Online Exclusive Article. *Military Review*, 3 (2018). www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/ (Downloaded: 04.06.2020)
- [17] NORRY, A.: The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin. *Blockonomi*, 2018. <https://blockonomi.com/history-of-silk-road/> (Downloaded: 5.10.2019)
- [18] VOREACOS, D.: U.S., South Korea Bust Giant Child Porn Site by Following a Bitcoin Trail. *Bloomberg*, 2019. www.bloomberg.com/news/articles/2019-10-16/giant-child-porn-site-is-busted-as-u-s-follows-bitcoin-trail (Downloaded: 25.10.2019)
- [19] ZETTER, K.: Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA. *Wired*, 2007. www.wired.com/2007/11/swedish-research/ (Downloaded: 1.10.2019)
- [20] Shadows in the cloud: Investigating Cyber Espionage 2.0. Joint Report: Information Warfare Monitor – Shadowserver Foundation. *The Citizen Lab*, 2017. <https://citizenlab.ca/wp-content/uploads/2017/05/shadows-in-the-cloud.pdf> (Downloaded: 04.06.2020)
- [21] *TorMap*. <https://tormap.void.gr> (Downloaded: 1.10.2019)
- [22] MAYER, D.: Google explains why Street Views car record Wi-Fi data. *ZDNet*, 2010. www.zdnet.com/article/google-explains-why-street-view-cars-record-wi-fi-data/ (Downloaded: 11.12.2019)
- [23] CSERHÁTI A.: A Stuxnet vírus és az iráni atomprogram. *Fizikai Szemle*, 61 5 (2011), 150–155. <http://fizikaiszemle.hu/archivum/fsz1105/cserhati1105.html> (Downloaded: 10.12.2019)
- [24] TUCKER, P.: If You Do This, the NSA Will Spy on You. *Defense One*, 2014. www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (Downloaded: 6.12.2019)
- [25] JOHNSTON, A.: Bradley Cooper's taxi ride: a lesson in privacy risk. *SalingerPrivacy*, 2015. www.salingerprivacy.com.au/2015/04/19/bradley-coopers-taxi-ride-a-lesson-in-privacy-risk/ (Downloaded: 02.01.2020)
- [26] SIPOSNÉ KECSKEMÉTHY K.: NATO-csúcstalálkozó az elrettentés és a védelem jegyében (Varsó, 2016. július 8–9.). *Hadtudomány*, 27 1–2 (2017), 114–126.
- [27] HAIG Zs.: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.
- [28] *TOR Metrics Portal*. <https://metrics.torproject.org> (Downloaded: 01.10.2019)
- [29] *PandaLabs Annual Report*, 2018. https://partnernews.pandasecurity.com/uk/src/uploads/2018/12/PandaLabs-2018_Annual_Report-uk.pdf (Downloaded: 01.01.2020)

Governmental Regulation of Cybersecurity in the EU and Hungary after 2000¹

TAMÁS SZÁDECZKY²

The term information security evolved to cybersecurity nowadays, which emphasises the interdependence of information assets and the importance of cyber-physical systems. Parallel to this, the need for appropriate management of the EU and government strategies and new public administration tasks also appeared.

In the European Union, the first measure concerning this issue was the establishment of the European Union Agency for Network and Information Security (ENISA) in 2004, mostly with consultative tasks. The first official cybersecurity strategy in the EU, called the Open, Safe and Secure Cyberspace, was accepted in 2013. Afterwards, ENISA's role has been strengthened as well as its range of tasks were broadened. Beside the critical infrastructure protection efforts, the Network Information Security (NIS) directive and related legislation were a giant leap towards a common level of cybersecurity in the community. The formation of an EU Cybersecurity Act and filling NIS with more practical guidance is an ongoing process nowadays.

Despite being a post-socialist country, Hungary is in the first line of legislation on cybersecurity in the community. Since 2005 there were several government decrees, from 2009 the first act-level rules on the information security of some governmental services. Based on the National Security Strategy, the National Cybersecurity Strategy was formed in 2013. The same year the first information security act applicable to all government, local government, governmental data processing and critical infrastructure service providers has come into force. The alignment of the National Cybersecurity Strategy to NIS directive happens these days.

Thus, the regulation of cybersecurity in the EU and in Hungary are heading in the right direction, but the practical implementation today is far away from the strategic objectives. The community is lagging far behind the United States of America and China, just to mention the most important players in the field.

Keywords: *cyber strategy, information security legislation, incident response, ENISA.*

¹ Supported by the ÚNKP-17-4-III-NKE-26 New National Excellence Program of the Ministry of Human Capacities.

² Ph.D., associate professor, National University of Public Service, Faculty of Public Governance and International Studies, Department of Public Management and Information Technology; e-mail: szadeczky.tamas@uni-nke.hu; ORCID: <https://orcid.org/0000-0001-7191-4924>

Introduction

The word cybersecurity seems to be a bit overused nowadays, but as other researchers have already demonstrated, it is different from the “classical” term information security. In both terms, information-based assets stored or transmitted using information and communication technologies (ICT) are included. But information security also includes paper-based information. According to the definition of the International Telecommunication Union’s (ITU) definition in 2008, cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organisation and user’s assets. Organisation and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability, integrity—which may include authenticity and nonrepudiation—and confidentiality. This is pretty much similar to the term information security. However, the term cybersecurity includes non-information-based assets (e.g., a high-voltage substation) that are vulnerable to threats via ICT. This is similar to the interdependency between critical infrastructure elements. Thus, “in cyber security the assets that need to be protected can range from the person him/herself to common household appliances, to the interests of society at large, including critical national infrastructure”. [1: 100] The new model of cybersecurity needs a different approach to security organisation: the classical security models have to be revised. [2]

The importance of cybersecurity is well-known and often communicated by decision makers. However, the implementation and preparedness have deficiencies. This might happen because of lack of knowledge, resources or experience.

Table 1. *Legal regulations about cybersecurity in the EU and Hungary.*
[Edited by the author.]

Year	The European Union	Hungary
2004	Regulation on establishing ENISA	
2012		National Security Strategy
2013	EU Cybersecurity Strategy The new regulation on ENISA	National Cybersecurity Strategy, Information Security Act
2016	NIS directive	
2017		
2018		
2019	Cybersecurity Act	
2020		The new National Security Strategy

Technological development, as I have already pointed out, made local system security improvements indispensable. [3] In case of e-government systems, a higher level of the problem also exists: attack against multiple systems or against a full infrastructure. This

can be part of a conventional war, as cyberwar, or may be an unconventional event, called cyberterrorist attack; they all concern cybersecurity. Thus, a major part of cybersecurity can be only managed on governmental or supranational level, with cybersecurity strategies, legal regulation, and dedicated authorities. [4] Table 1 shows parallelly the changes in the EU and Hungary, which will be detailed in this article.

Cybersecurity Strategy in the EU

Before forming any exact strategy, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10th March 2004 establishing the European Network and Information Security Agency* [5] came into force. The regulation established ENISA, with the following objectives (Article 2):

- “the Agency shall enhance the capability of the Community, the member states and, as a consequence, the business community to prevent, address and respond to network and information security problems;
- the Agency shall provide assistance and deliver advice to the Commission and the member states on issues related to network and information security falling within its competencies as set out in this Regulation;
- building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors;
- the Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.”

It is important to remark the verbs used: enhance, provide, develop, and update. They show us an intention to form a soft agency without policy-making power. The exact plans with ENISA were also unclear. [6]

The tasks aligned with the objectives above were the followings:

- collect appropriate information to analyse current and emerging risks;
- provide advice to stakeholders;
- enhance cooperation between different actors;
- facilitate cooperation between the Commission and the member states;
- contribute to raise awareness;
- assist the Commission and the member states in their dialogue with industry;
- track the development of standards;
- advise the Commission on research;
- promote risk assessment activities;
- contribute to Community efforts to cooperate with third countries;
- express its own conclusions independently.

As we see from the list above, the tasks are supportive functions. There are no regulatory, standardisation or audit functions dedicated to ENISA. In contrast, in the field of data protection, the European Data Protection Supervisor has authority to audit EU organisations.

The bodies of ENISA are the Management Board, the Executive Director, and the Permanent Stakeholders' Group.

The first official cybersecurity strategy in the European Union was formed with the *JOIN (2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union*. It's the *Open, Safe and Secure Cyberspace* formed on 7th February 2013. It states that "the borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent." [7] The first statement is: "The EU's core values apply as much in the digital as in the physical world, the same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain." [8] According to *Tallinn Manual 2.0*, most of the physical world international law rules can be applied on the cyberspace conflicts, but there are some unregulated issues. For those new points, additional rules are required. But cybercrimes are typically a field where all real-life legislation can be used, only the context, the device and the methodology changed.

The strategy defined five strategic priorities, which address the challenges:

- "achieving cyber resilience;
- drastically reducing cybercrime;
- developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- develop the industrial and technological resources for cybersecurity;
- establish a coherent international cyberspace policy for the European Union and promote core EU values." [7]

In the first strategic priority—achieving cyber resilience—the need to modernise and strengthen ENISA was articulated. [9]

After nine years of ENISA's operation and providing nearly 300 publications—with focus topics incident and risk management, critical infrastructure protection, trust services and computing cloud—a new regulation came into force. *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004* has changed the objectives: [Section I. Article 2. para 1–5]

- "the Agency shall develop and maintain a high level of expertise;
- the Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security;
- the Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market;
- the Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents;

- the Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.” [10]

The tasks were also changed according to the objectives (Article 3):

- “support the development of Union policy and law, by advising, providing preparatory work, and analysing;
- support capability building by supporting the member states, promoting voluntary cooperation, assisting by the operation of a Computer Emergency Response Team (CERT);
- support the raising of the level of capabilities of national/governmental and Union CERTs promoting dialogue and exchange of information, with a view to ensure that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;
- support voluntary cooperation;
- cooperate with Union institutions, bodies, offices and agencies;
- contribute to the Union’s efforts to cooperate with third countries and international organisations.” [10]

The most important change in the tasks was the establishment of CERT–EU, as a new service, and also a part of Computer Security Incident Response Teams (CSIRT) network according to Network Information Security (NIS) directive (*Directive [EU] 2016/1148*) Article 12. Para. 2. Incident management became more important in the operation of ENISA with these changes than in 2004. The incident management theory and practice are very wide; they range from operational procedures to governmental response. Illustrative key topics are ISO/IEC 27035, ITIL-based incident response, forensics, and operation of CSIRTs. [11]

The only change in the organisation was the staff’s addition under the Executive Director, and the Management Board shall establish an Executive Board.

In 2016, the European Commission adopted the *Commission Communication on Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final*. The document dealt with the making of most of NIS cooperation mechanisms and enhancing the capabilities and responsibilities of ENISA. The section also mentions European Cybercrime Centre (EC3) at Europol as a possible cooperation partner. The Commission is required to evaluate ENISA by 20 June 2018, but plans to do it earlier.

So a future change was foreseeable with the *2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the “EU Cybersecurity Agency”, and the repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”)*. The voting was forecasted to June 2018. Furthermore, on 13th September 2017, the President of the European Commission, Jean-Claude Juncker announced an implementation toolkit for the Network and Information Security Directive; and a report to ensure an effective response in case of cyber-attacks in the member states.

As the topic is in the focus of general interest and even had many political debates, the acceptance lasted for a while. The new act is *Regulation (EU) 2019/881 of the European*

Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). [12]

The objectives of ENISA changed slightly:

- the Agency shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks;
- the Agency shall assist the Union institutions, agencies, and bodies, as well as the member states, in developing and implementing policies related to cybersecurity;
- the Agency shall support capacity building and preparedness across the Union, by assisting the Union, member states and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience;
- the Agency shall promote cooperation and coordination at Union level among the member states, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to cybersecurity;
- the Agency shall increase cybersecurity capabilities at Union level in order to complement the action of member states in preventing and responding to cyber threats, notably in the event of cross-border incidents;
- the Agency shall promote the use of certification, including contribution to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market;
- the Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.

The tasks improved heavily: the task list consists of 60 elements, grouped into the following seven articles:

- Tasks relating to the development and implementation of Union policy and law;
- Tasks relating to capacity building;
- Tasks relating to operational cooperation at Union level;
- Tasks relating to the market, cybersecurity certification, and standardisation;
- Tasks relating to knowledge, information and awareness raising;
- Tasks relating to research and innovation;
- Tasks relating to international cooperation.

Another focus is the forming of new European cybersecurity certification schemes (see Article 46): “The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.” [12] Those schemes,

with the additional national schemes defined in Article 57, may provide a higher level of IT security interchangeability within the EU.

Cybersecurity Organisation in Hungary

The first comprehensive security and defence policy system of Hungary after the political change in 1989 did not recognise cyber threats. Neither the *National Assembly resolution no. 94/1998 (XII. 29.) on the security- and defence policy principles of the Republic of Hungary*, nor the *Government Decision 2073/2004. (IV. 15.) on the National Security Strategy of the Republic of Hungary*, nor the *Government Decision 1009/2009. (I. 30.) on the National Military Strategy of the Republic of Hungary* included cyber defence as an objective. According to these policies and strategies, the defence against cyber-attacks was treated individually, even in the legal regulation.

The first regulations in Hungary dealing with information security of governmental organisations were the following:

- *Government Decree 195/2005 (IX. 22) on security, interoperability and uniform use of electronic administration systems;*
- *Government Decree 84/2007 (IV. 25) on security requirements of the Central Electronic Service System and related systems;*
- *Government Decree 193/2005 (IX. 22) on detailed rules for the electronic filing;*
- *Government Decree 194/2005 (IX. 22) on requirements for electronic signatures and the associated certificates used in the administrative proceedings, as well as requirements for certification service providers issuing the certificates;*
- *Government Decree 182/2007 (VII. 10) on the regulation of the central electronic service provider system.*

The *Act on Electronic Public Service* (accepted in 2009) was the first act-level regulation dealing with information security in governmental organizations. [13]

In sum, we may say that a relatively low awareness of the legislator and the business was observable in the usage of international IT security standards, despite its significance and the high risk in some areas. [14] No obligations were found in acts of the Hungarian Parliament for enforcement of standards in IT security. There have been built-in self-control procedures in some acts, but in practice, those procedures actually did not work efficiently. [15]

In 2009 a small change was commenced with the adoption of *Act LX of 2009 on electronic public services*. It has highlighted the requirement of security as a basic principle.

According to *Act LX of 2009 on electronic public services*, organisations providing ICT based public services ensure the publicity of data of public interest (according to the Act on data protection and freedom of information) and protection of personal and any other data during the provision of services. [16]

IT security-related requirements were detailed in the following regulations:

- *Government Decree 223/2009 (X. 14) on the security of electronic public services;*

- *Government Decree 224/2009 (X. 14) on the central electronic system service's recipient identification and authentication services;*
- *Government Decree 225/2009 (X. 14) on electronic public services and their use;*
- *Government Decree 78/2010 (III. 25) on requirements of electronic signatures in administration and certain rules for electronic communication.*

A major change in the regulation started with the *Government Decision 1035/2012 (II.21.) on Hungary's National Security Strategy*, which stated that the information security of electronic public services, critical infrastructure and cyber defence capabilities have to be improved. The next step in this way was the *Government Decision 1139/2013 (III. 21.) on Hungary's National Cybersecurity Strategy*, which is still in force. The main objectives of it are to establish incident reporting and response capability, develop international cooperation, and develop trainings, exercises, baseline security and cooperation. These are actually very similar to the aims of the NIS, but articulated somewhat earlier.

The recent cyber operations increased the global political awareness in this area, thus on 25th April 2013 the Hungarian Parliament accepted *Act L of 2013 on the electronic security of state and local government organisations*. Its scope is slightly broader than just state and local government organisations, but also includes national data processors and critical infrastructure, therefore even private companies might be included (e.g. public utilities). [17] The act is based on international best practices and standards (e.g. ISO/IEC 27001:2013), although does not reference them directly. The law operates with the essential items known in the information security field as the CIA triad (confidentiality, integrity, and availability). The act requires the integrity and the availability of information systems in a closed, complete, consistent way, proportionate to the risks for the electronic system and components. It is important to explicitly include the proportionality of the security control implementation to risks. This enforces the conduction of a risk assessment and decisions based on that. This changes the malpractice of implementing security measures in an ad hoc manner, and is to minimise security budgets. [18]

The act established the National Electronic Information Security Authority under the control of the Ministry of National Development. The new task of vulnerability testing and log analysis was dedicated to the National Security Authority and the long before established Government Computer Emergency Response Team (GovCERT) was moved to the Special Service for National Security, which is a secret service in Hungary.

Afterwards the field of cybersecurity, including the organisations above, was handed over to the Ministry of Interior with *Government Decree 187/2015. (VII. 13.)*. Thus, the National Cyber Defence Institute was formed in the Special Service for National Security with the following features:

- administration by National Electronic Information Security Authority;
- incident management and response by GovCERT-Hungary;
- forensic log analysis and vulnerability testing by National Security Authority.

Another change coming into force in the meanwhile was the NIS directive. The National Cybersecurity Strategy has to be aligned with the requirements of NIS, *Chapter II (National frameworks on the security of network and information systems) Article 7 (National strategy on the security of network and information systems)*. This is an ongoing process right

now. Also, the *Information Security Act* is affected by NIS, Article 8 (*National competent authorities and single point of contact*) and Article 9 (*Computer security incident response teams [CSIRTs]*). The National Cyber Defence Institute is planned to be a competent national authority according to Article 8 of *NIS Directive (EU) 2016/1148*. There are four designated CSIRTs according to Article 8 of this directive:

- LRLIBEK for critical infrastructures, operated by the National Directorate General for Disaster Management, Ministry of the Interior;
- MILCERT, operated by the Military National Security Service;
- Hun-CERT, the Hungarian Computer Emergency Response Team for Council of Internet Service Providers, operated by the Hungarian Academy of Sciences, Institute for Computer Science and Control;
- and NIIF-CSIRT, which is the Computer Security Incidents Response Team of NIIF/HUNGARNET, the Internet provider of universities, higher education institutes, some secondary schools, academical research organisations and non-profit institutions in Hungary, operated by the National Information Infrastructure Development Institute.

Conclusion

ENISA was established in 2004 as a consultative body. Both the EU and the Hungarian Cybersecurity Strategy was accepted in 2013. The strategies implied changes in the treatment of the field of cybersecurity at the higher level. The objectives and tasks of ENISA have been changed, and the Hungarian authority was formed that year. The next step was the NIS directive and its implementation in the member states' law, which also provides reinforcement to EU legislation to improve ENISA.

One of the main objectives and tasks both for ENISA and in the Hungarian regulation is the training. Even in the private sector, there is a huge need for well-trained IT personnel. The required level of training is much higher in the cybersecurity than in classical back-office processes. In order to provide hands on knowledge, also real-life laboratories shall be used for such training. [19]

Another field of cybersecurity is that of military or cyber warfare. Many EU members, including Hungary, is a NATO member, which shapes our defence politics to a greater extent than the EU Common Security and Defence Policy. NATO recognised cyberspace as a "Domain of Operations" at the Warsaw Summit in 8–9 July 2016. In fact, there are no elements which are directly applicable at the member state level. There are many potential threats, like PSYOPS in the social media. [20: 117] Also, Internet of Things (IoT) as a civilian technology may pose risks to the defence sector. [21] But the fact that cyberspace became the fifth domain of operation, and the requirement that all military operations shall include such operations, will have a positive effect on defence.

Several changes happened in the previous years in the European legislation, and therefore preparedness to cybersecurity risk is much better nowadays, but we lag behind the United States of America and behind China. [22] Thus there is a long way to go.

References

- [1] SOLMS, R. – NIEKERK, J.: From information security to cyber security. *Computers & Security*, 38 (2013), 97–102. DOI: <https://doi.org/10.1016/j.cose.2013.04.004>
- [2] LEUPRECHT, C. – SKILLICORN, D. B. – TAIT, V. E.: Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, 33 2 (2016), 250–257. DOI: <https://doi.org/10.1016/j.giq.2016.01.012>
- [3] SZÁDECZKY, T.: Risk Management of New Technologies. *Academic and Applied Research in Military and Public Management Science (AARMS)*, 15 3 (2016), 279–290.
- [4] *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10th March 2004 establishing the European Network and Information Security Agency.*
- [5] LEWIS, J. A.: National Perceptions of Cyber Threats. *Strategic Analysis*, 38 4 (2014), 566–576. DOI: <https://doi.org/10.1080/09700161.2014.918445>
- [6] HEARN, J.: Moving forward? *Security & Privacy*, 1 2 (2013), 70–71. DOI: <https://doi.org/10.1109/MSECP.2003.1193215>
- [7] *JOIN (2013) 1 final, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union.*
- [8] *Tallinn Manual 2.0* <https://www.cambridge.org/hu/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB> (Downloaded. 14.09.2020)
- [9] RUOHONEN, J. – HYRYNSALMI, S. – LEPPÄNEN, V.: An outlook on the institutional evolution of the European Union cyber security apparatus. *Government Information Quarterly*, 33 4 (2016), 746–756. DOI: <https://doi.org/10.1016/j.giq.2016.10.003>
- [10] *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21st May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.*
- [11] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*
- [12] TONDEL, I. A. – LINE, M. B. – JAATUN, M. G.: Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45 9 (2014), 42–57. DOI: <https://doi.org/10.1016/j.cose.2014.05.003>
- [13] DEDINSZKY F.: *Informatikai biztonsági elvárások.* [Information security requirements.] Budapest, MeH-EKK, 2008.
- [14] SASVÁRI, P. – NEMESLAKI, A. – RAUCH, W.: Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises. *Academic and Applied Research in Public Management Science (AARMS)*, 14 1 (2015), 63–78.
- [15] SZÁDECZKY, T.: Information Security Law and Strategy in Hungary. *Academic and Applied Research in Military and Public Management Science (AARMS)*, 14 4 (2015), 281–289.

- [16] KISS, A. – SZŐKE, G. L.: New principles and instruments in the field of Data Protection Law. In RAPPAL, G. – FILÓ, Cs. eds.: *Well-being in Information Society 2014*. (Conference proceedings) Pécs, PTE, 2014. 208–215.
- [17] MUHA L. – KRASZNAY Cs.: Kibervédelem Magyarországon: áldás vagy átok? [Cyber defence in Hungary: Bless or curse?] *HWSW*, Paper 50206, 2013. www.hwsz.hu/hirek/50206/kibervelem-biztonsag-jog-torveny.html (Downloaded: 10.06.2020)
- [18] SZABÓ, Zs. M.: Cybersecurity issues of pension payments. In. SZAKÁL, A. ed.: *IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017*. New York, IEEE, 2017. 289–292.
- [19] DOMÍNGUEZ, M. – PRADA, M. A. – REGUERA, P. – FUERTES, J. J. – ALONSO, S. – MORÁN, M.: Cybersecurity training in control systems using real equipment. *IFAC PapersOnLine*, 50 1 (2017), 12179–12184. DOI: <https://doi.org/10.1016/j.ifacol.2017.08.2151>
- [20] BÁNYÁSZ P.: A közösségi média, mint az információs hadszíntér speciális tartománya [Social media as the special part of the information field of operations]. *Hadmérnök*, 12 2 (2017), 108–121.
- [21] TÓTH, A.: Future Information Security Threats to the Defense Sector. *Hadtudományi Szemle*, 10 4 (2017), 246–257.
- [22] SLIWINSKI, K. F.: Moving beyond the European Union’s Weakness as a Cyber-Security Agent. *Contemporary Security Policy*, 35 3 (2014), 468–486. DOI: <https://doi.org/10.1080/13523260.2014.959261>

Outlining a Set of Theory-based Requirements for the Future Digital Soldier

Szilveszter SZELECZKI¹

The military information scene is expanding as technology advances, and it has a fundamental impact on combat activities. It requires a high level of precision, expertise and dedication to set the right standards for military concepts and to establish a proper set of requirements of standards for military concepts, such as in NATO. Digital devices have become an integral part of the activities of the combatant soldier, as the use of modern tools makes combat activities more efficient. In a modern society, modernisation processes extend to the field of defence as well, resulting in intensive development in a growing number of countries. The requirements of the digital soldier are nowadays influenced not only by the warrior but also by those connected to him in the full information space, since a modern soldier is already an element of a network in network-centric military operations.

Keywords: digitalisation, requirement, information, soldier, NATO.

Introduction

In today's information-oriented society, the defence strategies of different nations undergo constant changes and innovations. Year after year, improvements and extensions can be seen in terms of technical equipment, procedures and methods. Perhaps one of the most prominent amongst governmental objectives is the development of modern strategic principles specifically designed for the present-day network structure related to the purposes of military innovation. During the cooperation of different arms, there is a need for continuous networking, and reliable operation of voice and data communications. Recent studies pay special attention to different activities on the battlefield. Some commentaries prefer, for example, the land forces, while others focus on other military branches. The land forces are considered to be the most common among the armed forces, and its targeted technological development nowadays clearly requires a network strategy mindset that, among other things, draws the attention of management to information issues.

Digital military concepts formulate a set of requirements specifically for the combatant. Looking back to the past, it can be seen that the military concepts of warfare went through

¹ Ph.D. student, National University of Public Service; e-mail: Szeleczki.Szilveszter@uni-nke.hu; ORCID: <https://orcid.org/0000-0003-2891-0527>

continuous analysis since the second half of the 20th century. Initially, they only focused on defence against grenades with regard to the capabilities of the uniform concerning shrapnel-protection, but later on, these concepts became more and more a technological issue in telecommunications, and with the spread of information technology, the continuous presence of voice and data connections became an integral part of the requirements. “Techniques for communication and computation cannot be studied in isolation: one technique for reducing communication energy usage is to perform more local processing, but this increases the amount of computation energy.” [1: 57] The combat situation of an infantry soldier is probably the most common situation: a soldier performs its own combat operation with its own personal equipment and strength. The networked, modern concept of this equipment system and arsenal belongs to the digital soldier. Investigating this concept and answering the emerging questions in the present day is becoming more and more important to the armed forces, and thus its comprehensive understanding and integration may be a key issue for future armed forces, where consistent, precise definition of requirements is essential. “Digital Soldier is seeking whitepapers to include specific technologies and/or novel integration ideas.” [2] Military developments bring up national and allied (e.g. NATO) requirements that also affect the digitisation of combat soldiers, so a set of requirements must be established, which serves the interests of all in the future.

Defining the System of Requirements

Purpose and function

The general aim of a digital military requirements system is to refine and upgrade the existing military equipment specifically for the combatant. In order to determine the subject in detail, it is necessary to take into account every field of activity that may be necessary in the course of modernisation. The definition of the objectives must be accompanied by the formulation of the exact purpose, which in this case contains the operational concepts of a military system. Of course, there are differences in priority between digital military objectives, which may be related to the planning and development process. In formulating the overall goal, the specific issues of the federal and national concepts complete the comprehensive elements of the system of requirements.

The definition of goals is closely linked to the interpretation and formulation of purposes. The basic purpose of digitising a fighting soldier is to enhance the soldier’s information capabilities, which he or she can effectively collect, use, and transmit in the course of his or her combat activities. It is the general duty of soldiers to fight bravely and steadily in combat; to find the most expedient way to defeat the enemy, to use all available tools wisely and effectively, and to act with determination. Thus, the purpose of the aforementioned military digitisation is basically modernisation, concerning also the flexible capability of using info-communication tools which can react quickly and efficiently to changing circumstances. Improvements and upgrades are only carried out where they are needed, and therefore a precise understanding and definition of the requirements can be considered as a basic condition for establishing the requirements of the digital soldier.

The Need for Requirements

In order to determine the exact requirements, first the fundamental effects of a given development or innovation must be examined. Digital soldier project can be termed as a general terminology and the first step in establishing an actual set of requirements is the examination of the necessity of each requirement, their possible positive and negative effects. As a consequence, the needs can be precisely delineated. It is important to have a conscious mindset that will result in deciding what is necessary and what can be judged sufficient. Obviously, there is a need for defence-related developments, because with the advancement of information technology, the activities of the soldiers must be improved to reach the highest possible standard, and the question rather arises as to what may be interpreted as necessary. This approach is associated with the practical experience and the related management opinions. Of course, the answers to questions about qualities of an innovative new info-communication system depend on many influencing factors, as there are several aspects to consider, especially the views of the participants in the network.

As for meeting the information needs, both from the perspective of the user warrior and from other actors within the network structure, a consistent set of requirements should be defined. Therefore, in digital military concepts, it is important to consider and define the boundary between what is needed and what is sufficient, because the priority values of the requirements can be determined specifically through a thorough analysis of the needs. The following types of essential requirements are required for the proper definition of requirements:

- technical requirements;
- system architectural requirements;
- system integration requirements;
- requirements for ICT (Information and Communications Technology) tools.

Finally, the aggregate data resulting from the above-mentioned necessities allows the need to meet the exact purposes and define a consistent set of requirements. The armed forces' pursuit of continual modernisation gives rise to the general need of digital military concepts, as the development of necessary and sufficient functionalities is periodically re-evaluated. Of course, reevaluation is also required for practical use, as a military subsystem or sensor, for example, may not produce the expected results for a networked warrior or its associated partners. Thus, usability appears as a crucial influencing factor for the finalisation of the need, since the effectiveness of the digital military system is decided in practice, not in theory.

Content of the Requirements

The content of the system requirements includes plans, concepts and the necessary conditions for the realisation of military concepts. The specification of the content of the requirements is a logically separate part of the digital soldier project, which is at the beginning of the entire project life cycle. In defining the content of the project requirements, it is worth to pay attention to the fact that there are methodologies specifically designed for project management that can provide quite a large amount of professional help with this military

project. Essentially, the methodologies provide some insight into the logical phases and parts of a project. Such a methodology guides the project from initial thinking to tangible results. An example of this is Project Cycle Management (PCM), which specifically promotes professional project planning.

Opinions differ on the need for methodologies, but experience from different sources makes it clear why it is worthwhile to use methodologies in a project. The best known of these reasons are:

- confused strategic frameworks;
- supply-driven projects (write a project that has money);
- poor situation analysis;
- activity-oriented planning;
- ignoring the needs of target groups;
- short term thinking;
- unexpected risks;
- inconsistency of results;
- costs are not in proportion to the benefits gained;
- lack of experience;
- immeasurable effects;
- inaccurate project documents.

Thus, the methodologies also help to define the requirements system precisely, as they place the emphasis on the importance of the detailed elaboration of the whole life cycle, the sequence, the expected results and the opportunities. Figure 1 shows the stages of the project lifecycle defined by the PCM methodology. The Digital Soldier Global Project also begins with a programming phase where leaders of nations analyse the current military situation, condition, organisational structure, function, tasks, and explore the options accordingly.

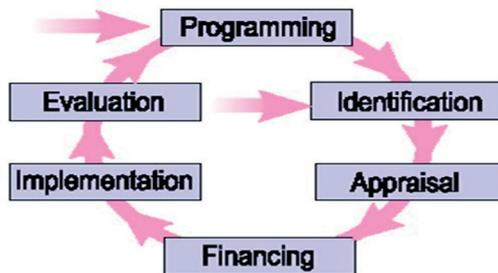


Figure 1. *The project lifecycle proposed by PCM.* [3]

Of course, when developing the requirements of digital military concepts, the standardised solutions used by NATO forces must be taken into account and the experience gained so far should be utilised. The content of the requirements may be determined on the basis of the following essential aspects:

- consideration of NATO's requirements;
- definition of specific requirements;
- allocation of responsibilities to requirements.

Feasibility

In the realisation of the digital soldier project, it is important to emphasise the conscious attitude of the combatant soldier that he/she is a system component. In this way, the information system can be used simultaneously by the combatant and other users in the network to receive or send data. "Other users" include other combat soldiers and members of upper management / superiors. It is therefore about implementing a complex system that fully integrates the combatant's activities, where the designation of requirements requires a high degree of complexity.

When talking about the points to be considered during the definition of the set of requirements, I suggested observing NATO's relevant requirements. As to the feasibility of the requirements, various NATO documents may be linked here, including:

- NATO Standardization Agreements (for instance STANAG 5048);
- NATO Allied Engineering Publications (for instance AEP-76 VOL 1);
- NATO Allied Data Publications (for instance ADatP-34);
- NATO Allied Tactical Publications (for instance ATP 3.2.2);
- NATO Allied Joint Publications (for instance AJP-6).

From the aspect of the feasibility of the plans, it is essential to consider the possibilities to fit them into the order of standards, announcements, procedures, methodologies and to make modifications and corrections in the definition of the requirements based on their contents. For example, the digital military concept should take into account NATO's information communication requirements for different hardware and software designs, with particular reference to interoperability, which obviously has a high priority among member countries. With regard to interoperability, interface as a concept extends to info-communication tools, and more specifically to the communication between all information-based devices. [4] From the point of view of info-communication, compliance can be interpreted on the basis of three essential aspects:

- data link level compliance;
- voice connection level compliance;
- global, system-level compliance.

Thus, the feasibility of digital military systems requirements is related to the imaginative tools that include various system link controllers, data and voice model structures, protocols. These tools must cooperate with each other during operations, that is, they must be interoperable. Some of the aforementioned NATO standards serve this purpose specifically, increasing allied efficiency and continuous cooperation between current information and network-oriented military forces. Thus, several official NATO publications deal with issues about requirements to achieve interoperability. "*NATO's interoperability policy defines the term as the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objective.*" [5]

Figure 2 shows NATO's call for why it is necessary and worthwhile for member states to use published standards in their development.

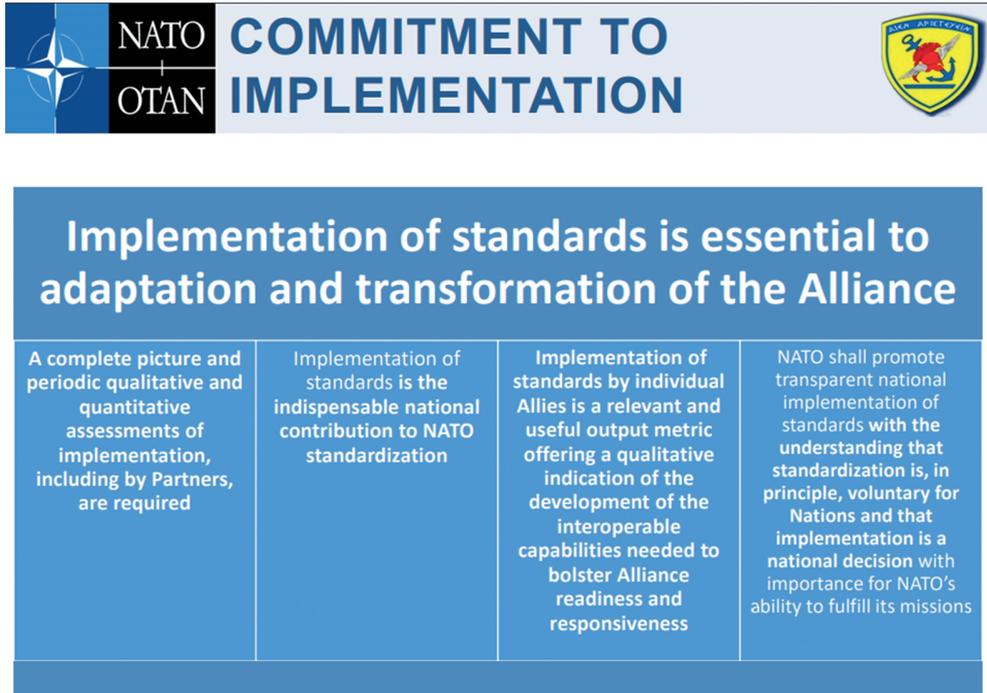


Figure 2. NATO's call about standards implementation. [6: 10]

Therefore, taking standards into account alone provides guidance for digital military concepts. Whether it is about relationship models, structures, hierarchies, or any specifications in management and control systems, they are all essential parts of the requirements. For example, NATO STANAG 4677 discusses these parts, while NATO AEP 76 already addresses systematic deployment, prioritising network concepts. Thus, these standards all contribute to the realisation of the requirements of basic digital military concepts, where the information exchange focuses on the activities of the fighting soldier, all at joint operation level.

Information has a growing power in the modern world, thus affecting the feasibility of innovative military projects. Therefore, adapting to the information space must also be the central element of the feasibility of digital military concepts, since the ability to use information can fundamentally influence a combat activity. “The principal needs of the Army for tactical command, control, and communications (C3) applications fall into two categories. First, to enhance the lethality of the Future Soldier, advanced information technologies are needed to insure reliable, wideband, networked communications over an area commensurate with evolving battlefield environments. Second, for the Future Soldier 2030 to maintain information dominance, situational awareness data set must reflect higher-level tactical internet and global command and control system network intelligence.” [7: 13]

Feasibility in military terms may also depend on answering information security issues, since a high level of information activities is the core element of military operations. “Most

commercially available systems do not address relevant military needs, typically lack the validated algorithms that make real time computed information useful, and are not open architected to be integrated with the soldier technological ecology.” [8: 1147] The enemy wants to get the most up-to-date information; thus, its protection and management requires the most effective procedures and methods. “The sharing of the information wins the fight, not the biggest or best bullet. We are looking at a soldier as a communications intelligence platform, not just a person with a weapon system.” [9] The same goes for counter-activities and support activities. Information processing issues therefore, like interoperability, also require high priority, mature solutions concerning the feasibility of requirements. When implementing the requirements for a fighter’s military info-communication activities, it should be taken into account that the soldier:

- collects information;
- stores information;
- processes information;
- transmits information.

Information capabilities therefore play a crucial role in defining the set of requirements. These require a detailed, prioritised development. The hardware and software differences between countries also appear to be decisive factors in the feasibility of requirements for digital military concepts. There will be a lot of questions and answers from participants involved in the implementation of the requirements so that the digital soldier project can begin to be built on the right specification using the information communication capabilities at its disposal.

Applicability

The applicability of the requirements is largely shaped by the experience gained from the above mentioned practices, which differ in the armies of different countries and represent different values. It is important to note that the timeliness of the requirements plays an important role in the usability issues, as the decision-makers need to make well-founded decisions about the future, generally on an annual basis. For example, an American article says: “Army HQ has a vision for the future soldier of the 2020s that exploits rapid advances in technology to revolutionise the dismounted soldier’s equipment in its entirety.” [10] Which means that they are planned to be used for a relatively short period of time, a few years after which the definition of long-term time will be reassessed. The usability is guided by design ideas and suggestions for the most efficient solution. Design solutions should take into account military operational requirements, which place a high priority on practical aspects of attack and defence. The requirements may be applied for military purposes in the following areas: “Command and control, lethality, mobility, survivability, sustainability.” [11: 127]

The various services involved in the activities of a combatant may be active or passive, which of course also have to be organised in relation to operational issues. These functionalities may change over time and space, depending on the combat situation, including the information they provide.

Focusing on networking through the example of the American FIST program, in response to changing circumstances, the following is stated: “The network system will reroute automatically to allow continuity of operation when a communications link is broken, for example when a soldier moves over a hill or ridge.” [12] Information must be managed in a centralised system that requires a set of hardware and software that can use that information for further operations. By thoroughly defining the requirement types mentioned above, the following functionalities required by the digital military concept can be implemented:

- positioning, target marking system;
- digital voice and data communication;
- management support system;
- energy supply system;
- sensory monitoring system;
- weapons system;
- clustered information system;
- modern uniform solutions.

Imaginations

Capability concepts

At first glance military digitalisation ideas seem to be what digital communication is about, but in most cases they consist of a much broader, larger set. In today’s digital world, more and more advanced and higher-level services can be imagined and demanded. When defining military info-communications concepts, one must consider the set of properties that include the info-communication service that is exactly needed. During normal operation, it is important to understand when, where and how it is expedient to use a particular service.

In relation to NATO, the member countries have different titles and ideas for the future digital soldier. For example, Land Warrior in America, Future Integrated Soldier in Great Britain, Gladius in Germany, Combatiente Futuro in Spain and FELIN in France. In essence, each member country strives to adopt its own and the allied ideas for its project, which will raise combat soldier capabilities to a higher level. These ideas and projects consist of several basic requirements which can be defined as a kind of modernisation capability. These are as follows:

- info-communication capability;
- armed ability;
- survivability.

Military developments are progressing over time to develop a more modern mobility capability in these capability areas. Info-communication abilities can be linked to the emergence of novel concepts aimed at networking the combatant’s information capabilities, thereby expanding individual abilities. A certain device capable of collecting, storing, processing and transmitting information can be classified here. Examples include radios, sensors, display units, storage and distribution devices. With regard to radios,

tactical radios with a sufficient bandwidth and capability of transmitting both voice and data to appropriate range come into the forefront.

Radios capable of IP-based data transmission are a major step in the development of digital communication, the integration of which can be interpreted as a fundamental factor. To optimise the use of the data channel, the most appropriate channel access protocols should be used. In this way, radios capable of these are preferred, as they may meet the requirements that can be expected in the future. General ideas about sensors include information about different states and active signals. This includes, for example, active detection information, which can occur in light and sound. Of course, in the light range, laser and infrared solutions are the ones that can be used for target designation, while the sound range can provide the information. This information would be monitored by a clustered sensor array that would provide the information to the warrior and the senior leadership within a short period of time. Blue Force Tracking is typically an information service that requires up-to-date information to function. "The section leader is equipped with BMS (Battle Management System), a veritable nexus for communication networks, contributing to a fully digitized battlefield network. Hosted in a lightweight portable computer adapted to military environments, it allows the leader to control platoon or squad manoeuvres, give orders to and collect intelligence data from every soldier on the battlefield. Built around a processing module and a remote touch screen, the computer allows leaders to exchange information (data, images, video, virtual maps) and communicate using radio networks." [13]

Weapon-related issues and the requirements that apply to them are essentially dependent on technical parameters. The information capabilities of the various 7.62 mm and 5.56 mm assault rifles could primarily be combined with a subsystem that can, for example, designate a target and process information from another subsystem for further use. In this context, for example, the development of target illumination methods and the exact specification of its requirements may be necessary. "In the future, soldiers will be equipped with a weapon system that would allow them to identify a target, and then simply to aim and shoot. They will receive relevant data, and will be equipped with night vision equipment." [14]

In terms of survival, defence objectives come to the forefront, with the help of which the soldier manages and solves situations occurring in the battlefield. An article on a German concept reads: "The body armour component is designed for protection from detection, biological and chemical agents and extreme climatic conditions. It includes flame retardant equipment, a ventilation shirt and insulating layers to stabilize body temperature, and ballistic protection." [15] Raising survivability to a higher level is highly dependent on the magnitude of the defence options.

With this in mind, the following solutions can be considered:

- modern uniforms;
- technical devices providing protection:
 - against designations;
 - against atomic, biological and chemical weapons;
 - against landmines;
- heavy-duty kits.

System Implementation Ideas

Different ideas can be classified according to their abilities. Referring to the breakdown as needed, detailed operational requirements can be broken down into technical, system architectural, system integration, and info-communication schemas.

The technical requirements for the digital soldier determine the basic information task systems in which both the user and the service provider appear. The exact definition of the expected capability of a technical device is essentially provided by the technical requirements. Sensor-related and other communication parameters, such as size, fit, design and other technical values and definitions, are also required for the system linked to the info-communication network. “Digital soldiers also need to interconnect their sensors, tactical computing and communication devices. In order to achieve full wideband connectivity, a data switch needs to be a real wideband communication protocol.” [16] It is an important criterion that parameters must be effectively reflected in military practice.

From an architectural point of view, capabilities can be divided into different levels. For example, a distinction can be made between some basic and some complementary skills. These levels can be defined in steps, or expanded to more specific sub-levels. The realisation of all these will result in a complex system of ideas. You can also define a priority difference for stepwise deployment. An imaginary structure similar to this is shown in Figure 3, to illustrate a step-by-step layout in the field of info-communication capabilities with some examples that can be expanded to meet customer needs. The architectural approach to the project is necessary because it will result in a systematic consideration and development of system components based on each other. For example, the concept of a helmet camera can only be tested if its image can be transmitted to a display device. Thus, in this case, first the proper functioning of the camera and its information transfer capability must be ascertained, and this must be followed by the proper functioning of the information display unit.

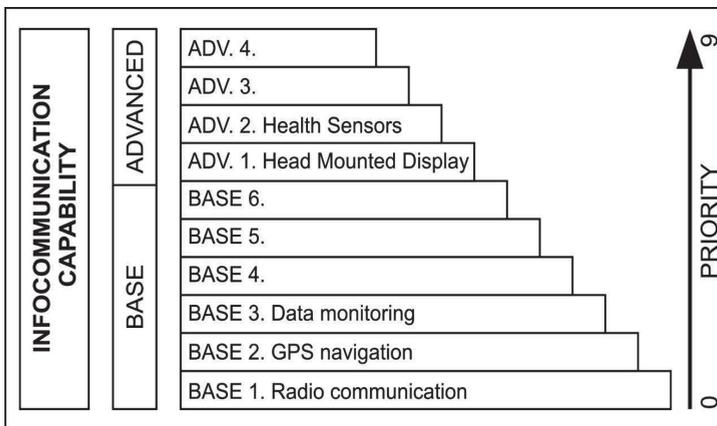


Figure 3. *Illustrated structure of the info-communication capability.* [Created by the author.]

System integration concepts focus on the integration of devices to be used in the digital military system. In this requirement, an imaginary list should be created which should

include the relationship between the devices, communication, control levels, representations and other features, in which the interoperability mentioned above will also play a role. At the simple logical level, the system integration can be imagined in four steps as shown at Figure 4 below. The processes must be detailed and specified that can take very-very long time.

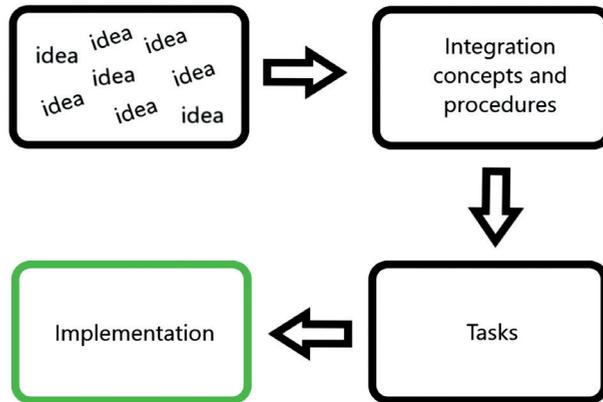


Figure 4. *Simple way from ideas to implementation.* [Created by the author.]

So, the list should include the following main integration concepts and procedures:

- selecting partners and ensuring continuous communication;
- precise definition of development tasks based on the technical requirement;
- providing a development background for information concepts between components;
- ensuring cooperation between developments;
- proper handling and serial-numbering of prototypes;
- developing tests to be applied to prototypes;
- preparation of documentation containing full applicability;
- continuous monitoring of processes, allocation of responsibilities.

Info-communication tasks, expectations and their implementation ideas have to be defined for the devices. In application terms, the following types of devices are generally required:

- communication device;
- interfacing / distribution device;
- power supply device;
- navigation device;
- display device;
- detection device;
- data collection tool.

Applicable tools also need to consider their software background and capabilities for adapting devices to the appropriate requirements, resulting in the most efficient implementation from a technological perspective. Figure 5 shows the previously mentioned project, called “Land Warrior” in American terminology, showing a future warrior with his toolbox.

LAND WARRIOR

Staff Sgt. Brian Tidwell of B Company, 4th Battalion, 9th Infantry Regiment wears the Manchu version of Land Warrior. The 4-9 recently completed a year in combat in Iraq. They were the first unit to take the sophisticated command and control system into battle. Leaders equipped with Land Warrior say the system helps cut through the fog of war with a constant flow of information they've never had before.

GRAPHIC BY CHRIS BROZ/STAFF
PHOTOS BY ROB CURTIS/STAFF

GPS ANTENNA

Dimensions: 3" diameter
Weight: 0.24 pounds
This flat disc attaches to the soldier's load-bearing equipment and connects Land Warrior to satellites overhead to allow the soldiers to pinpoint his position and the locations of other Land Warrior-equipped soldiers.

SOLDIER CONTROLLER UNIT

Dimensions: 6.11" (L) x 3.47" (W) x 1.47" (H)
Weight: 1.13 pounds
The soldier control unit acts as a "tactical mouse," allowing the wearer to access Land Warrior features such as maps, graphics, satellite imagery and messages with the touch of a finger.

CPU

Dimensions: 9.0" x 7.25" x 2.77"
Weight: 1.5 pounds
The central processing unit contains a microcomputer processor for managing information flow, sending and receiving text messages and storing digital maps, graphics and images.

PELTOR HEADSET

Weight: 1 pound
This is a standard audio headset with a microphone used by combat units. It plugs into Land Warrior for use with the voice radio.

HELMET-MOUNTED DISPLAY

Dimensions: 7.13" x 1.88"
Weight: 0.42 pounds
This component resembles a miniature computer screen that allows the soldiers to view the terrain before him, track the location of his unit members, mark objectives, read text messages and view other mission-related information.

NAVIGATION SUBSYSTEM

Dimensions: 7.84" x 7.25" x 2.95"
Weight: 1.15 pounds
This contains the GPS and digital compass for use in land navigation for tracking the wearer's positioning and heading on a map as well as the positions of fellow Land Warriors.

HELMET INTERFACE ASSEMBLY

Dimensions: 3.63" x 0.75"
Weight: 0.45 pounds
This component links the Helmet Mounted Display to the other components of the Land Warrior System.

VIEW OF BACK PANEL INTERIOR

BATTERY

Dimensions: 8.66" x 3.54" x 2.57"
Weight: 2.14 pounds
Each Land Warrior equipped soldier carries two rechargeable Lithium Ion batteries, each capable of supplying 10 hours of power.

LAND WARRIOR RADIO

Dimensions: 8.66" x 3.54" x 2.57"
Weight: 1.45 pounds
This is a voice and data radio system for communicating from squad and platoon level and up to higher headquarters level. Soldiers can send text messages and the mission planning materials in addition to using it for voice communications.

© 2008 Army Times Publishing Co.

Figure 5. The American future warrior conception. [17]

Each of these devices must be examined and a set of practise-based and detailed requirements must be set out. A digital military network system can only be realised if all the hardware and software components that one wants to apply have complete, accurate ideas, analysis, and evaluation. All of these can help to create the most effective system of claims about the digital soldier.

Summary

The Digital Soldier is a global military concept that provides support to combat soldiers using the most up-to-date, state-of-the-art technology. This program is specifically focused on the combat situation when a combat soldier performs his task using his personal equipment. When designing and specifying requirements, it is essential to consider the user environment, but network-oriented concepts must also be met. For the military, the timeliness of information always plays an important role, as it is either armed or all-military, and knowing the exact real-time combat situation is invaluable. The concept of a digital soldier is made up of several sets of capabilities that can result in a modern warrior equipped with competitive technology. Injection and development of info-communication capabilities is an extraordinary development, but weapons and other supplies and tools are also undergoing major changes in military system organisation.

There are many aspects that need to be worked out in detail in the requirements, and different methodologies or information from experience can help with their quality. A kind of specialisation process is already under way within NATO member states (e.g. monitoring, reconnaissance and target-designation tools independent of time of day or weather). As a component of the system, the capability of monitoring, displaying, and transmitting data on the physical and health status of soldiers during combat has emerged as a requirement, but the specific development process has not yet begun. Traceability of friendly forces is now becoming a basic requirement in vision. Requirements should include step-by-step expectations and ideas about capabilities. As technology advances, military ideas can be periodically re-evaluated. We must be able to meet the new challenges of the age, otherwise the availability of a country's armed forces and its ability to maintain security could easily be reduced. If the digital military program is based on the definition of a high level of detailed requirements, its implementation will result in the appearance of the most effective capabilities possible.

References

- [1] *Meeting the Energy Needs of Future Warriors*. Washington, D.C., The National Academies Press, 2004. DOI: <https://doi.org/10.17226/11065>
- [2] HARPEL, D.: Army to hot industry day for digital soldier initiative. *Defense Systems Journal*, 2018. www.dsjournal.com/2018/11/08/army-to-host-industry-day-for-digital-soldier-initiative/ (Downloaded: 05.06.2020)
- [3] Six Cycle Project – PCM (Figure from a conference paper entitled “Identifying under reporting issue of construction industry in Malaysia”). *ResearchGate*, 2009. www.researchgate.net/figure/Six-Cycle-Project-PCM-World-Bank-Logframe-Methodology-Handbook-2009-There-are-three_fig1_305143957 (Downloaded: 05.06.2020)
- [4] FARKAS, T. – HRONYECZ, E.: The Info-Communication System Requirements of the Deployable Rapid Diagnostic Laboratory Support “Sampling Group” II. *AARMS*, 14 1 (2015), 53–61.
- [5] NATO Interoperability. *NATO Multimedia Library*, 2019. www.natolibguides.info/interoperability (Downloaded: 05.06.2020)

- [6] NATO Policy for Standardization. *International Standardization Workshop*, 2018. www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/2018%20International%20Standardization%20Workshop/20181030-Item6a-NATOStandardizationPolicyandQuizIntlStdznWorkshop-_Myriounis.pdf?ver=2018-11-07-095044-083 (Downloaded: 05.06.2020)
- [7] Future Soldier 2030 Initiative. *Wired*, 2009. www.wired.com/images_blogs/dangerroom/2009/05/dplus2009_11641-1.pdf (Downloaded: 05.06.2020)
- [8] FRIEDL, K. E.: Military applications of soldier physiological monitoring. *Journal of Science and Medicine in Sport*, 21 11 (2018), 1147–1153. DOI: <https://doi.org/10.1016/j.jsams.2018.06.004>
- [9] STACKPOLE, B.: Keeping the Connected Soldier Connected with Simulation. *DE 247 Digital Engineering*, 2016. www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation/ (Downloaded: 05.06.2020)
- [10] Supporting the Army's Future Soldier Vision. *UK GOV Laboratory*, 2018. www.gov.uk/government/case-studies/supporting-the-armys-future-soldier-vision (Downloaded: 05.06.2020)
- [11] MURRIN, D.: *Defence First – A New Model for Britain's Defence Forces*. 2016. www.davidmurrin.co.uk/sites/default/files/2019-08/a_new_model_for_britains_defence_forces_october_2016.pdf (Downloaded: 05.06.2020)
- [12] FIST – Future Infantry Soldier Technology System. *Army Technology*, 2019. www.army-technology.com/projects/fist (Downloaded: 05.06.2020)
- [13] Felin Sagem (Fantassins Equipements Liaison Intégrés) – French future infantry soldier system. *Army Recognition*, 2019. www.armyrecognition.com/france_french_army_military_equipment_uk/felin_sagem_future_soldier_infantry_equipment_soldier_gear_technical_data_sheet_specifications_uk.html (Downloaded: 05.06.2020)
- [14] ARKIN, D.: The Digital Revolution of the IDF. *IsraelDefense*, 2016. www.israeldefense.co.il/en/content/digital-revolution-idf (Downloaded: 05.06.2020)
- [15] GETTLER, L.: German military increases order for Gladius “future soldier” system. *New Atlas*, 2013. <https://newatlas.com/future-soldier-rheinmetall-gladius/26271/> (Downloaded: 05.06.2020)
- [16] STEPANSKY, A.: OPED: new conformal batteries expedite moves to a digital soldier. *Defense Systems*, 2017. <https://defensesystems.com/articles/2017/10/cw/soldier-batteries-army.aspx> (Downloaded: 05.06.2020)
- [17] Land Warrior Rig. *Jack O' Lantern's MS Blog*, 2017. <http://jackolanternsmshblog.blogspot.com/2017/05/land-warrior-rig.html> (Downloaded: 05.06.2020)

Soft Targets: Definition and Identification¹

Tomáš ZEMAN²

Available definitions describe a soft target as a location with high vulnerability, but a low level of protection. However, such general definitions can hardly be used in the process of soft targets identification. The aim of the article is to create a temporary specific definition that could be utilised for this purpose. The suggested definition of a soft target is based on performed statistical analysis of 275 cases of terrorist attacks aimed against soft targets in the European Union from 2000 to 2015. In the definition, a soft target is characterised based on the probability of a terrorist attack occurrence and the expected number of casualties caused by the attack.

Keywords: *soft targets, terrorist attacks, crisis management, definition.*

Introduction

Recently, great attention has been paid to the issue of soft targets and measures for the increase of their security. In the United States (US) and Europe, there is an increasing number of violent attacks on soft targets in order to injure as many people as possible. Due to their attractiveness, ease of access and accessibility, terrorist groups increasingly seek them. Libicki, Chalk and Sission [1] presumed that this trend is caused by the hardening of prominent targets such as the Pentagon or White House after September 11, 2001. The difficulty of attacking these prominent targets leads terrorist groups to focus their attacks against soft targets, which are far more vulnerable.

Unfortunately, there is no universally recognised definition of soft targets to date. According to Fagel and Hesterman, [2] a soft target is generally “any person or thing that is vulnerable to attack but not protected”. Recently, in its *Fourth progress report towards an effective and genuine Security Union*, the European Commission [3] defined soft targets as locations that “are vulnerable and difficult to protect and are also characterised by the high likelihood of mass casualties in the event of an attack”. Nevertheless, both definitions are very common, which does not allow their use in the process of soft targets identification. The creation of more specific definition of soft targets would significantly facilitate the process of soft targets identification and contribute to a better understanding of terrorist aims and targets selection.

¹ The work was created as a commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled “Public Service Development Establishing Good Governance”.

² Ph.D., assistant Professor, Department of Military Science Theory, Faculty of Military Leadership, University of Defence, Brno, Czech Republic; e-mail: tomas.zeman2@unob.cz; ORCID ID: 0000-0001-7269-4994

In terms of soft targets, the greatest attention nowadays is paid to objects or events that involve a large number of people in relatively small areas such as temples, schools, universities, hospitals, sport events, concerts, restaurants, hotels, bus/train stations etc. Although all these facilities or events are similar in many aspects, “not all such targets are equally vulnerable”, as noted by Asal et al. [4] In addition, it can be assumed that individual soft targets differ also in their popularity among terrorists. Unfortunately, practically no quantitative research of soft target vulnerability and their preferences by terrorists has been performed apart from the notable exception of the above mentioned study by Asal et al. [4]. The aim of this article is to contribute to the formulation of a soft target specific definition based on the identification of soft targets with the highest vulnerability and/or the highest probability of a terrorist attack. In order to achieve this goal, a statistical analysis of data about terrorist attacks committed in the European Union (EU) between 2000 and 2015 was performed.

Methods

The Global Terrorism Database [5] was utilised as a data source. All terrorist acts committed in the EU between 2000 and 2015 were selected from the Global Terrorism Database (GTD). Furthermore, only terrorist acts targeted against targets listed in the Table 1 were selected using the variable “targsubtype1” according to the GTD Codebook. [6] The result of this selection was 275 cases of terrorist attacks against soft targets from 19 target categories according to the GTD. [5] On the other hand, there were no documented terrorist attacks against targets from the Civilian maritime and Port categories according to the GTD in the given period. For this reason, these two categories were excluded from further statistical analyses. The number of casualties were calculated as the sum of persons killed or wounded during the attacks based on the variables “nkill” and “nwound” from the GTD.

For each terrorist attack, additional information (i.e. occurrence of the attacker’s attempt to penetrate the structure, success of this penetration and evidence of some terrorist group engagement during preparation of the attack) were traced in publicly available sources, particularly from websites of news media such as BBC News, The New York Times etc.

Penetration of a structure is any technique of entering a structure with the intention of committing a terrorist act, e.g. armed assault with a rifle, as well as walking into a structure with a hidden bomb. On the other hand, cases when a terrorist attack was committed outside the building, such as the explosion of a bomb placed in a garbage bin near its entrance or the throwing of a Molotov cocktail into the building from the street were not considered as a penetration attempt.

A terrorist attack is considered to have been organised by a terrorist group in two cases: *a)* A terrorist attack is claimed by the group and this claim is not questioned by any relevant source, e.g. conclusions from a police investigation; *b)* Involvement of a terrorist group is proved during a police investigation. In cases when two or more terrorist groups claim one terrorist attack, but it is not clear which claim is true, the terrorist attack is considered to have been organised by a terrorist group. Any other terrorist act not corresponding to any of the aforementioned criteria is not considered to have been organised by a terrorist group. This procedure leads to the division of all terrorist attacks into two

groups: a) terrorist attacks demonstrably organised by a terrorist group; b) terrorist attacks committed by an individual, i.e. lone wolves or lone actors, and terrorist attacks organised by a terrorist group, but with a lack of evidence of the terrorist group's engagement.

Table 1. *Coding of selected soft targets according to the GTD Codebook [6], with the number of incidents and the mean number of casualties between 2000 and 2015. (Based on data from GTD [5].)*

Coding	Target	Number of incidents	Mean number of wounded	Mean number of dead
2	Restaurant/bar/café	29	3.759	1.345
8	Hotel/resort	19	3.353	0.278
11	Entertainment/cultural/stadium/casino	36	9.629	2.6
44	Airport	8	0.375	0
49	School/university/educational building	15	2.333	0.733
57	Civilian maritime	0	0	0
60	Port	0	0	0
74	Marketplace/plaza/square	7	5	0.143
78	Procession/gathering	4	5.75	0.25
79	Public areas	23	0.957	0.087
81	Museum/cultural centre/cultural house	6	0	0.667
86	Place of worship	63	0.27	0.016
96	Tour bus/van/vehicle	1	30	6
99	Bus (excluding tour bus)	9	0.111	0
100	Train/train tracks/trolley	44	40.977	4.341
101	Bus station/stop	2	0	0
102	Subway	3	0	0
103	Bridge/car tunnel	1	0	0
104	Highway/road/toll/traffic signal	5	0	0
	Total	275	8.989	1.28

Note: Mean numbers were calculated as the sum of wounded or dead people divided by the number of incidents.

Based on research samples consisting of data from GTD [5] and the aforementioned additional variables, a statistical analysis was performed for soft targets categories with at least 15 cases. All calculations were performed in statistical software R [7]. The relationship between variables was assessed using Spearman's rank correlation coefficient (R).

Results and Discussion

Regarding the type of used weapon, bomb attacks are by far the most frequent (Table 2). Terrorist attacks carried out with explosives or an incendiary constitute 90.2% of all attacks against soft targets in the EU between 2000 and 2015. Based on the results of performed analysis, train/train tracks/trolley, entertainment/cultural/stadium/casino, restaurant/bar/

café and hotel/resort are the soft targets with the highest number of victims caused by terrorist attacks (see Figure 1, Table 1).

Table 2. *Relative frequencies of weapon type in the sample. (Based on data from GTD [5].)*

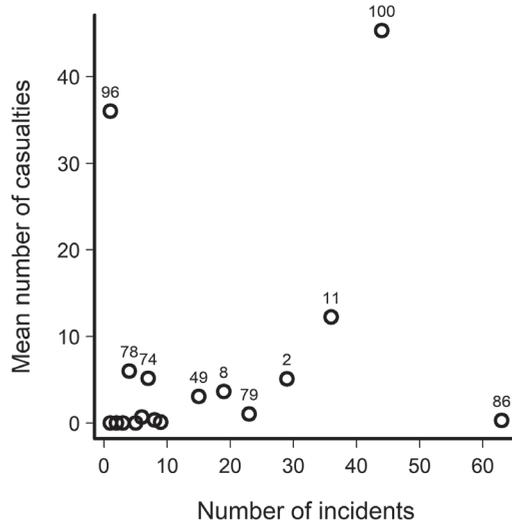
Weapon type	%
Explosives/bombs/dynamite	64.4
Incendiary	25.8
Firearms	4.7
Melee	2.9
Others	2.2

Note. Frequencies based on variable “weaptype1” from GTD [6].

As can be seen in Figure 1, the highest number of victims was caused by terrorist attacks against soft targets from the GTD category train/train tracks/trolley. Almost all documented victims were killed or wounded as the result of the terrorist attacks in Madrid on 11 March 2004, where a series of ten bomb explosions occurred on trains on Madrid’s commuter line during the morning rush hour. As seen in Table 1 and in Figure 1, the number of attacks against targets from this category is also very high. There were 44 attacks documented by the GTD [5] between 2000 and 2015. The absolute majority of them was bombing (70%) or arson (27%) attacks as seen in Table 2. Nevertheless, most of these attacks were either unsuccessful or with no intention to kill. This directly correlates with the fact that most of the bomb attacks were performed at night or in the early morning hours. Bomb attacks against rail lines (36%) or train stations (36%) are the most frequent *modus operandi*, whereas direct assaults against trains are relatively rare (18%).

Terrorist attacks against soft targets from the entertainment/cultural/stadium/casino category are very frequent ($n = 36$), although not highly devastating. These attacks are most frequently bomb attacks against nightclubs, discotheques or bars (44%), however, stadiums are also a relatively frequent target (14%). The remaining cases represent attacks against various targets such as concert halls, museums, galleries, sport facilities etc. Attacks against targets from this category are usually not highly lethal. In fact, in most cases, there is evidently no intention to kill: Bomb devices are usually detonated at night outside opening hours and are often preceded by a telephone call of the upcoming bomb attack. In some cases, these attacks are more like vandalism. The reason why these soft targets have the second highest mean number of casualties caused by terrorist attacks can be found in the Paris attacks on 13 November 2015, specifically the Bataclan concert hall massacre. The Bataclan attack has shown the vulnerability of this kind of soft target. In this case, three perpetrators armed with firearms were able to penetrate the building with six security agents on duty that night being unable to stop them. The massacre led to 90 people killed and 217 wounded according to GTD. [5] On the other hand, security measures proved to be effective at another terrorist attack performed by ISIL that day in Paris, the suicide bombing at Stade de France, when three suicide bombers attempted to get inside the stadium where 79,000 people were watching a friendly football game between France and Germany. This plan failed after a security guard discovered the suicide vest of the first bomber and prevented him from entering the stadium. As a result, instead of hundreds of dead, only one

person was killed, when all three perpetrators detonated themselves near the entrance gates to the stadium.



(Each type of soft target marked uses the coding of variable “targsubtype1” from GTD, for details see Table 1.)

Figure 1. Number of terrorist attacks against soft targets and the mean number of casualties (persons killed or wounded during the attacks) in the European Union between 2000 and 2015. (Based on data from GTD [5].)

Another very common target is a restaurant/bar/café. In these places, it is very unlikely that there are security guards, cameras, etc. that could prevent a terrorist attack. According to the GTD, [5] there were 29 terrorist attacks against these types of soft targets. However, the actual reasons why these targets have the third highest number of victims are due to the Paris attacks on 13 November 2015, specifically on restaurants in the area of the 10th arrondissement. The remaining terrorist attacks against the targets from this category were far from being so devastating. The *modus operandi* of these attacks was quite similar to the attacks against targets from the entertainment/cultural/stadium/casino category: In most cases, some kind of explosive device was used (76%). The bomb attacks were often performed outside opening hours indicating that the primary goal of these attacks was not to kill civilians. In six cases, the attack was announced in advance, usually by an anonymous telephone call.

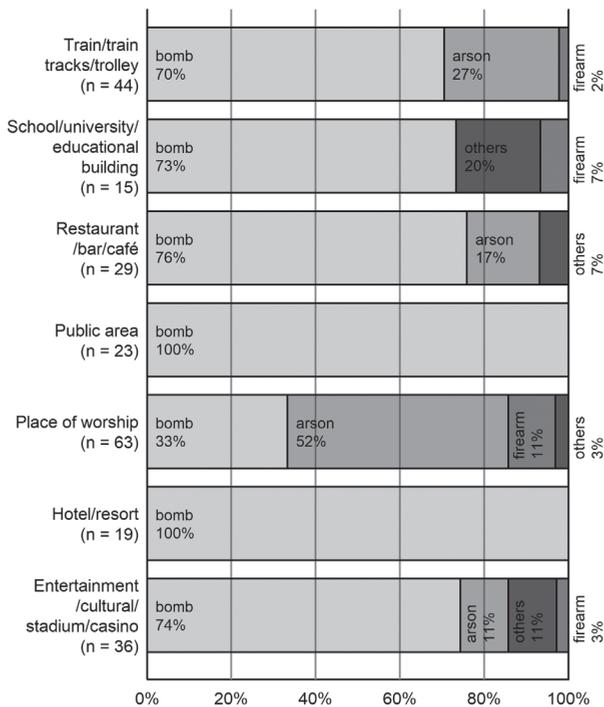


Figure 2. Frequencies of different techniques of terrorist attacks against seven types of soft targets most frequently exposed to terrorist attacks. (Based on data from GTD [5].)

Other relatively frequent targets of terrorist attacks were soft targets from the GTD category hotels/resorts (n = 19). [5] Interestingly enough, the most frequent targets were Spanish or French hotels or resorts. This corresponds with the fact that in most cases the attacks were carried out by Basque or Corsican separatist groups, e.g. ETA (Euskadi ta Askatasuna). Spanish hotels/resorts were targeted in 53% and French hotels/resorts in 37% of the cases. Detonated explosives were used as the primary technique of attack in all cases. It is quite easy to get explosives inside the hotels/resorts because the main entrance is usually unguarded and there is no luggage check of the guests.

Regarding the tour bus/van category, there was only one documented terrorist attack between 2000 and 2015, however, with many fatalities. It was a suicide bomber attack on an Israeli tourist bus in Burgas, Bulgaria, claimed by Hezbollah. This attack resulted in 6 dead and 30 injured passengers.

There were several documented terrorist attacks against soft targets from the GTD category school/university/educational buildings with moderate lethality. For the most part, they were bomb attacks (73%). [5] However, there is also a relatively high percentage of direct assaults carried out by assailants armed with firearms or knives (20%). So far, probably the worst attack against school/university/educational buildings was performed by a teenage

Finnish student on 7 November 2007 at the Jokela High School, when a student carried out a school shooting and killed seven students, a teacher, and himself with a handgun.

There were only seven documented terrorist attacks against targets from the marketplace/plaza/square category; however, one of them led to a great number of casualties. It was a bombing attack that took place in a supermarket in the central part of Riga on 17 August 2000 and resulted in 1 dead and 34 injured. The other six attacks were only slightly lethal, together leading only to one wounded person.

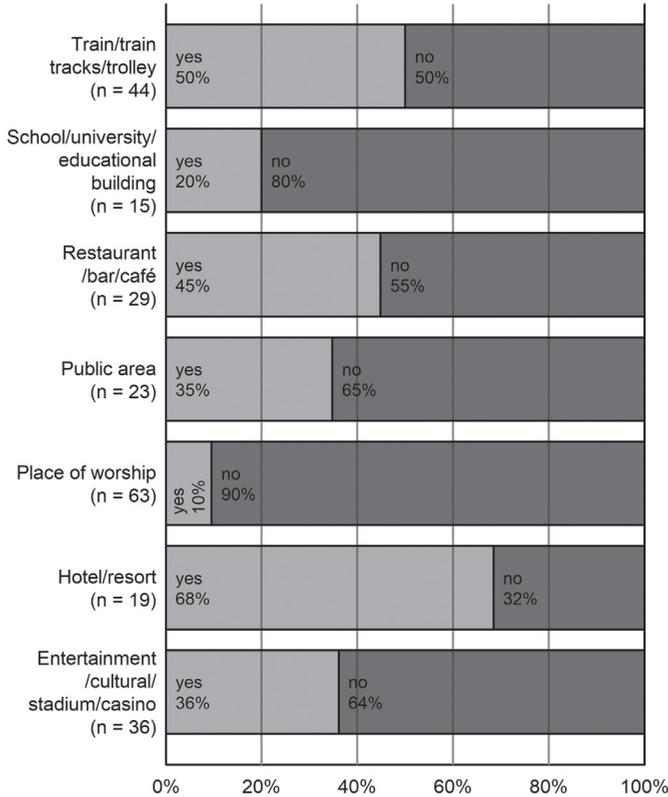


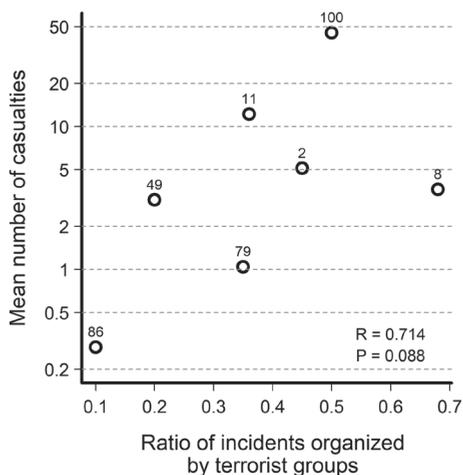
Figure 3. *Frequencies of terrorist attacks apparently organised by terrorist groups in seven types of soft targets most frequently exposed to terrorist attacks.* [Edited by the author.]

One common soft target that terrorist organisations choose as their target are public areas (gardens, parking lots, garages, beaches, public buildings and camps). These places are very attractive to terrorists because they are public, often completely unguarded and as a rule, there is a large number of people on site. However, despite the large number of terrorist attacks in public areas (n = 23), their lethality is relatively low (0.087 dead and 0.957 wounded people per attack). Similarly, terrorist attacks against places of worship as a soft target are frequent in all over Europe (n = 63), they are in fact the most frequently attacked soft targets. In spite of this, their lethality is very low (0.016 dead and 0.27 wounded people per attack). Regarding these soft targets, an interesting geographical distribution can

be observed: attacks against places of worship in France and Germany give 52% of all the terrorist attacks against these types of soft targets. The most targeted places are synagogues (30%) and mosques (43%) in all of Europe. In most cases, no terrorist organisation claimed responsibility for these attacks and there was no convincing evidence indicating that the attack was committed by any terrorist organisation (90%) as seen in Figure 3. The most widespread techniques of attack were explosives and arson attacks (setting fires or throwing Molotov cocktails). In contrast, terrorist attacks against processions/gatherings are very rare; in fact, only four such terrorist attacks were documented in the selected period; however, for this category the third highest mean number of casualties among all soft targets categories has been reported (0.25 dead and 5.75 wounded people per attack).

The frequency of terrorist attacks against all other types of soft targets categories or the number of casualties caused by these attacks proved to be very low.

The positive correlation between terrorist group involvement and the number of casualties, as seen in Figure 4, indicates that terrorist attacks organised by terrorist groups are deadlier than terrorist attacks committed by individuals. This is apparently caused by a higher rate of bomb attacks in terrorist attacks committed by terrorist organisations (83% of all terrorist attacks organised by terrorist organisations) compared to terrorist attacks committed by individuals or by an unknown perpetrator (58% of all terrorist attacks performed by individuals or an unknown perpetrator).



(“R” represents Spearman’s rank correlation coefficient and “P” the respective p values. Each type of soft target marked uses the coding of variable “targsubtype1” from GTD, for details see Table 1.)

Figure 4. Relationship between ratios of terrorist attacks prepared by terrorist groups and the mean number of casualties. (Based on data from GTD [5]).

There are also significant differences in the rate of penetration attempts into structures in selected soft target categories (Figure 5). There is a very high penetration attempt rate

in targets from the train/train tracks/trolley, school/university/educational building and the restaurant/bar/café categories. This rate is slightly less than that of the category of public areas, which includes public gardens, parking lots, beaches, camps etc., [6] relatively low in targets from the categories of place of worship and hotel/resort and very low in the category of entertainment/cultural/stadium/casino. This trend apparently corresponds with the extent of security measures which are usually adopted for soft targets from each category. For example, there are no security measures in fact that could prevent anyone from tossing a bomb, incendiary or firearm into a train, trolley, school or restaurant. Unlike these objects, many soft targets from the category of entertainment/cultural/stadium/casino and some targets from the categories of hotel/resort and place of worship usually perform personal entrance checks. This demonstrates the importance of such security measures in the prevention of terrorist attacks. The best example of this is the foiling of the suicide bomber during a personal check at the entrance into Stade de France during the 13 November terrorist attacks in Paris, which consequently saved tens or maybe hundreds of lives.

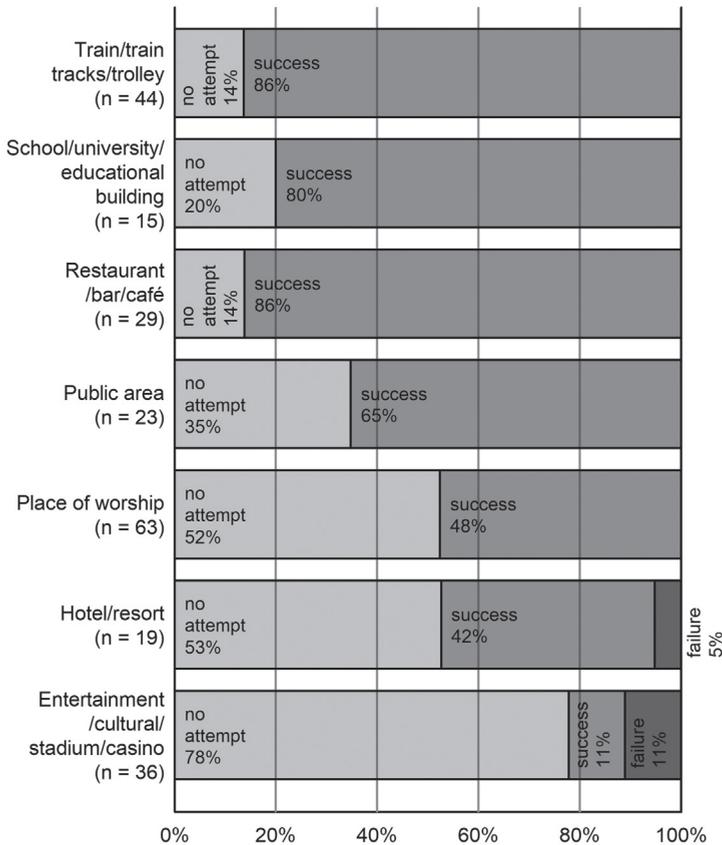


Figure 5: Frequencies of attempts to penetrate a structure and success of the penetration in seven types of soft targets most frequently exposed to terrorist attacks.

Conclusions

Based on the results of the statistical analysis, it was found that different types of soft targets vary greatly concerning the risk of terrorist attack. One of two basic features of soft targets according to the common definitions is vulnerability. In this study, vulnerability was measured by lethality, i.e. the mean number of casualties caused by terrorist attacks against each soft target category. Vulnerability is given by the concentration of people, efficiency of security measures and quality of terrorist attack performance. There were four soft target categories with no casualties at all and four others with the mean number of casualties lower than one person per attack. A good example of this type of soft target is places of worship. During the selected period of sixteen years, the GTD [5] contained 63 terrorist attacks against soft targets from this category in the EU. However, all these attacks ended with the death of only 1 person and 17 people wounded. Besides the low level of professionalism of these terrorist attacks, it is also due to the fact that the density of people at places of worship is usually relatively low. Despite this, places of worship are a very popular target due to their symbolic meaning. However, it is questionable if the structure from this group should be classified as a soft target.

On the other hand, there are target categories that are rarely hit by terrorist attacks, even though these attacks are extremely deadly. A good example is targets from the GTD category of tour bus/van/vehicle. There was only one terrorist attack against these targets in the selected period in the EU, i.e. the suicide bomber attack on an Israeli tour bus in Burgas, however, with great impact (six people killed, 30 wounded). [5]

For these reasons, both the frequency and lethality of terrorist attacks against soft targets were considered as valuable variables for soft target identification. Together, they reflect all the important aspects of terrorist attacks against soft targets, i.e. the concentration of people on site, the efficiency of security measures and the target preferences of terrorists. Based on the results of this study, the provisional two-criterion definition of a soft target is suggested: "A soft target is a location where the probability of a terrorist attack incidence per year exceeds 0.001 % and the expected number of casualties caused by the attack exceeds 1 dead or wounded person."

This specific definition can be used for the preliminary classification of an object as a soft target. The expected number of casualties can be estimated based on GTD [5] as the mean number of casualties for the selected GTD category of soft targets, e.g. the hotel/resort category in a region, e.g. the EU. The probability of terrorist attacks for the selected soft target in the region can be approximated as the number of terrorist attacks in the region in the selected period divided by the period length in years and the total number of soft targets of this type in the region, e.g. the total number of hotels and resorts in the EU.

It can be seen that by this procedure the probability of a terrorist attack for one object from a given soft target category can be calculated. This probability was deliberately preferred over the probability of a terrorist attack against the entire category of soft targets. This approach was used because the probability for an individual object reflects not only the target preferences of terrorists, but also the possibilities of the target's protection. For example, even though the frequencies of terrorist attacks against targets from the categories of marketplace/plaza/square and airport are similar, the possibilities for their protection are utterly different due to their numbers. At the same time, several hundreds of civil airports

operate in the EU; there are at least tens of thousands of markets in the same territory, which makes their protection practically impossible.

However, the proposed procedure is based solely on historical data. As such, it cannot be perfect and should only be considered temporary. The *modus operandi* of terrorist attacks, as well as target preferences of terrorists, changes quickly. For this reason, soft target identification based solely on historical data is necessarily not entirely accurate. Moreover, the method used for determination of the probability of a terrorist attack against individual soft targets is only approximate. In fact, the probability of a terrorist attack differs not only among soft target GTD categories, but also between two soft targets from one GTD category. For example, the marketplace in the capital or large city has a significantly higher probability of a terrorist attack than a marketplace in a village. More sophisticated methods for the determination of both probability of a terrorist attack and the mean number of casualties should be elaborated in the future. In particular, the method should allow for the assessment of terrorist attack probability for an individual soft target taking into account its position, size and adopted security measures.

References

- [1] LIBICKI, M. C. – CHALK, P. – SISSION, M.: *Exploring Terrorist Targeting Preferences*. Santa Monica, RAND Corporation, 2007. www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG483.pdf (Downloaded: 22.11.2017)
- [2] FAGEL, M. J. – HESTERMAN, J.: *Soft Targets and Crisis Management: What Emergency Planners and Security Professionals Need to Know?* New York, Routledge, 2016. DOI: <https://doi.org/10.4324/9781315451091>
- [3] COM/2017/041 final. *Fourth progress report towards an effective and genuine Security Union*. Luxembourg, Publications Office of the EU, 2017.
- [4] ASAL, V. H. – RETHMEYER, R. K. – ANDERSON, I. – STEIN, A. – RIZZO, J. – ROZEA, M.: The Softest of Targets: A Study on Terrorist Target Selection. *Journal of Applied Security Research*, 4 3 (2009), 258–278. DOI: <https://doi.org/10.1080/19361610902929990>
- [5] *Global Terrorism Database (GTD). National Consortium for the Study of Terrorism and Responses to Terrorism*, 2017. www.start.umd.edu/research-projects/global-terrorism-database-gtd (Downloaded: 22.11.2017)
- [6] *Global Terrorism Database – Codebook: Inclusion Criteria and Variables. June 2017. National Consortium for the Study of Terrorism and Responses to Terrorism*. Maryland, University of Maryland, 2017. www.start.umd.edu/gtd/downloads/Codebook.pdf (Downloaded: 22.11.2017)
- [7] R Development Core Team: *R: A language and environment for statistical computing*. Vienna, R Foundation for Statistical Computing, 2017.

Authors' Guide

AARMS is a peer-reviewed international scientific journal devoted to reporting *original research articles* and *comprehensive reviews* within its scope that encompasses the military, political, economic, environmental, social and public management dimensions of security.

NUPS standards for articles

I Essential principles

- 1 The publication should be of benefit to its readers.
- 2 We do not engage in redundant publication.
- 3 Authors must take responsibility for the content, equity, accuracy and style of their paper.
- 4 We consider submissions which are sent according to this guideline.

II General requirements

- 1 Proposals should be submitted with an abstract, up to ten key-words, as well as author's affiliation and e-mail address.
- 2 Only relevant and well-formatted tables and figures can be used, and must be sent in separate files and at the right resolution. If the submitted material contains any table or figure that has not been originated by the author(s) of the proposal, you must get permission to use it from the copyright holder, and have to refer to it.

III Style guide and examples

A Formatting

The proposal must be formed with Times New Roman font type (the body of the text at 12 point font size, footnotes at 10 point), normal margins, single space and justified in a standard, single-column format.

B Structuring

Text should contain a logical sequence of main sections, preceded by a heading. To use sections and sub-sections, you should have at least two of them at any level. Keep headings and sub-headings short. Use sentence-style capitalization.

Praesent ad accumsan velit

John Doe

I Lorem ipsum dolor sit amet: Consectetur adipiscing elit

Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.¹ Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi aliquip ex commodo consequat . . .

A Duis aute irure dolor in reprehenderit²

In voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum . . .

(i) Sed ut perspiciatis unde omnis

Iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae sunt . . .

a) Nemo enim ipsam voluptatem

Quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt . . .

b) Integer condimentum mauris ut lacus facilisis iaculis

Praesent sed fermentum neque. Proin porta sagittis tortor sit amet luctus. Suspendisse ut gravida sem. Quisque vestibulum et neque condimentum, vitae efficitur dolor pretium . . .

(ii) Neque porro quisquam est

Qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem . . .

B Suspendisse vulputate consectetur nunc vitae suscipit

Quisque efficitur vestibulum pellentesque. Phasellus tempor massa purus, vitae viverra orci ultricies at. Morbi nibh nisi, molestie id rutrum eu, efficitur ut arcu . . .

II Nunc nec ex interdum, blandit lacus imperdiet, bibendum ex

Nullam lobortis, nulla sed accumsan ornare, est arcu scelerisque nisi, sed malesuada mi turpis in purus. Morbi scelerisque dui fringilla volutpat ultricies . . .

¹ Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur?

² Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Quotations

Punctuation follows the closing quotation mark, unless the whole sentence is a quotation. The footnote marker comes last. If you add emphasis to a quotation, put '(emphasis added)' into the footnote.

Incorporate quotations of up to five lines into the text, within single quotation marks. Quotations longer than five lines should be in indented paragraphs; leave additional line spacing above and below indented quotes. For quotations within short quotations, use double quotation marks.

Citation

Either directly or indirectly citing any source, put the reference in footnote. Do not use endnotes.

David Hume, in the section Of the Origin of Our Ideas of *A Treatise of Human Nature*, wrote that

All the perceptions of the human mind resolve themselves into two distinct kinds, which I shall call *impressions* and *ideas*. The difference betwixt these consists in the degrees of force and liveliness, with which they strike upon the mind, and make their way into our thought or consciousness. Those perceptions, which enter with most force and violence, we may name impressions: and under this name I comprehend all our sensations, passions and emotions, as they make their first appearance in the soul.¹

Shortly after this definition, starting to prove the precedency of our impressions or ideas,² he put that 'our ideas are images of our impressions, so we can form *secondary ideas*, which are *images* of the primary'.² Arguing that [...]

¹ David Hume, *A Treatise of Human Nature* (London: John Noon, 1739), 1.

² *Ibid.* 6 (emphasis added).

Books:

First note:

¹ John Dewey, *Logic: The Theory of Inquiry* (New York: Henry Holt, 1938).

² Jean-Pierre Changeux and Paul Ricoeur, *Ce qui nous fait penser – la nature et la règle* (Paris: Odile Jacob, 1998), 14–34.

³ Klaus Wettig (ed.), »*Ich wohne nicht in stehenden Gewässern*«. *Der politische Günter Grass* (Göttingen: Steidl, 2018), 120–21.

⁴ Christoph E Düllmann et alii (eds), *Nuclear Physics A: Special Issue on Superheavy Elements* (Oxford: Elsevier 2015), 13, 23, 79–101.

Subsequent notes:

¹¹ Dewey, *Logic*, 123.

¹² Changeux and Ricoeur, *Ce qui nous fait penser*.

¹³ Düllmann, *Nuclear Physics A*, 74–76.

Chapters and other parts of edited books:

First note:

¹ Clinton Tolley, ‘Hegel’s Conception of Thinking in His Logics’, in *Logic from Kant to Russell: Laying the Foundations for Analytic Philosophy*, ed. by Sandra Lapointe (New York: Routledge, 2019).

Subsequent notes:

⁷ Tolley, ‘Hegel’s Conception of Thinking’, 84.

Journal articles:

First note:

¹ Louis D Brandeis and Samuel D Warren, ‘The Right to Privacy’, *Harvard Law Review* 4, no 5 (1890), 193–220.

² Karl Schlieker, ‘Lufttaxis gewinnen an Flughöhe’, *Allgemeine Zeitung*, November 29, 2019.

Subsequent notes:

⁴ Brandeis and Warren, ‘The Right to Privacy’, 201.

⁵ Schlieker, ‘Lufttaxis’.

Online works:

First note:

¹ Sophia Chen, ‘Physicists Take Their Closest Look Yet at an Antimatter Atom’, *Wired*, February 19, 2020, <https://www.wired.com/story/physicists-take-their-closest-look-yet-at-an-antimatter-atom>.

Subsequent notes:

² Chen, ‘Physicists’.

If a paper you are linking to has an associated Digital Object Identifier (DOI), please use the <http://dx.doi.org/> address to link to it instead of the publisher's address.

Cases: Citing cases in the body text, at first, use the ‘*Doe v Wade*’ form, later on, an unambiguous short version is enough (‘in *Wade*’). In footnotes, when it is first mentioned, give the name of the case in full – thereafter it may be shortened, but provide a cross-citation in brackets to the footnote in which the full citation can be found. Do not forget to give the law report and page or paragraph number.

¹ *Virginia v Black* 538 US 343 (2003).

...

¹⁴ *Virginia* (n 1) 345.

Citing sources of law, use full forms in the body text (for example, Article 8 and Section 9(1)(a) of Human Rights Act 1998), and abbreviations in footnotes (Human Rights Act 1998, art. 8 and s. 9(1)(a)).

R v Secretary of State for the Home Department [2000] AC 115
Connolly v Director of Public Prosecutions [2007] EWHC 237
Hill v Great Tey Primary School [2013] ICR 691
Smith Kline & French Laboratories (Australia) Ltd v Secretary to the Department of Community Services and London Artists Ltd v Littler [1969] 2 All ER 193
Rofe v Smith's Newspapers Ltd [1924] 25 SR (NSW) 4
Australian Broadcasting Corp. v O'Neill [2006] HCA 46
Abrams v. United States 250 US 616 (1919)
Lingens v Austria (1986) 8 EHRR 407
Health (1990) 22 FCR 73
Burnett v National Enquirer, Inc. 144 Cal. App. 3d 991 (1983)

Schenck v United States 249 US 47, 52 (1919)
R (on the application of ProLife Alliance) v British Broadcasting Corporation [2003] UKHL 23, [91]

Case C-154/19 *Kypriaki Kentriki Archi v GA* (ECLI:EU:C:2019:888)

Von Hannover v Germany no 59320/00
Von Hannover v Germany (No 2) nos 40660/08 and 60641/08

Arrêt n°1113 du 19 décembre 2019 (18-25.113)
BVerfGE 120
Cass. civ. 13 aprile 2000, n. 4790

Footnotes

Footnotes can be a form of citation or can provide relevant additional information. Indicate footnotes with a superscript number which should appear after the relevant punctuation in the text – for the clarity, it can also be put directly after the word or phrase to which it relates. If a subsequent citation immediately follows, use ‘Ibid.’ Separate citations with semi-colons. Pinpoints to pages come at the end of the citation. If the page numbers have the same hundreds or thousands digit, do not repeat it when listing the final page in the range. Close footnotes with a full stop. Italicise titles of books – all other titles should be within single quotation marks and in roman. Capitalise the first letter in all major words in a title. Footnotes must contain all available data of the cited sources. Do not insert ‘at’, ‘page’, ‘p’ or ‘pp’, and avoid ‘ff’. Use ‘Press’ referring to university publishing houses (for example, Edinburgh University Press).

¹ Henry Petroski, *To Engineer Is Human: The Role of Failure in Successful Design* (New York: St. Martin's, 1985); Henry Petroski, *Design Paradigms: Case Histories of Error and Judgment in Engineering* (Cambridge: Cambridge University Press, 1994); Tom Jackson (ed.), *Engineering: An Illustrated History from Ancient Craft to Modern Technology* (New York: Shelter Harbor, 2016).

² Simon Winchester, *The Perfectionists: How Precision Engineers Created the Modern World* (New York: Harper Perennial, 2019).

³ Ibid. 74.

⁴ Petroski, *Design Paradigms*, 122–34.

⁵ Petroski, *To Engineer Is Human*, 27.

⁶ Winchester, *The Perfectionists*, 76.

Italicising

For laying emphasis on a word or some words, use italics. Avoid over-emphasis. Italicise foreign words and phrases as well, but not quotations and words that are in common usage in English. Referring to foreign terms, next to the English translation, provide the original expression in brackets.

The being-in-the-world (*in der Welt-Sein*) . . .
The expression ‘general rule’ (*à la règle générale*) . . .
Everyday autarky (*αὐτάρκεια*) in this context means . . .

Listing

Lists with less than five items preferably should be in paragraph format, and marked with numbers ((1); (2); (3); (4)). If necessary, use vertical lists with en dashes instead of bullets. Put a period at the end of items in a vertical list only if the items are complete sentences. Otherwise, omit terminal periods, even for the last item, and do not capitalise the first words.

Punctuation and abbreviation

Use as little punctuation as possible. Abbreviations and initials in authors’ names do not take full stops. Nevertheless, mentioning for the first time, full names should be used at first.

Cass R Sunstein, in his paper *The Power of the Normal*, analyses the stigmatisation by categorisation as well. He, like Erving Goffmann, uses these words . . .
Sunstein argues that . . .

The European Union (EU) is an international organisation comprising 27 European countries. Originally, the EU confined to western Europe . . .

Contractions ending with the same letter as the original word do not take terminal full stops (Mr, edn), but abbreviations where the last letter of the word is not included do (ch., ed.) – except the abbreviated forms of ‘versus’ and ‘note’. The abbreviations ‘etc.’, ‘i.e.’ and ‘e.g.’ should be replaced by ‘and so on’, ‘that is’ and ‘for example’.

article, articles	art., arts
chapter, chapters	ch., chs
number, numbers	no, nos
paragraph, paragraphs	para., paras
part, parts	pt, pts
section, sections	s., ss

Commas should be omitted before the final ‘and’ and ‘or’ in lists unless they help understanding.

Introducing a span or range with words, do not use the en dash. Use en dash reporting contest scores or results, and between words representing conflict, connection or direction.

Omissions should be indicated by ellipsis, in which each dot should be separated from its neighbour by a non-breaking space (. . .). If the omission comes at the end of a sentence, use a full stop and an ellipsis.

Winston Churchill in his historic speech, ‘We Shall Fight on the Beaches’, said that

That was the prospect a week ago. . . . The King of the Belgians had called upon us to come to his aid. Had not this Ruler and his Government severed themselves from the Allies, who rescued their country from extinction in the late war, . . . the French and British Armies might well at the outset have saved not only Belgium but perhaps even Poland.

Symbols

Instead of using % symbol, write ‘per cent’.

Use & symbol only if it is a legacy, for example, in titles and names (*William & Mary Quarterly*, Simon & Schuster).

Contents

Gábor BENCSIK: Are We Really Lacking the Effectiveness of Financial Resource Management in the Defence Sector?	5
Tamás BEREK, László FÖLDI, József PADÁNYI: The Structure and Main Elements of Disaster Management System of the Hungarian Defence Forces, with Special Regard to the Development of International Cooperation	17
Mihály BODA: Erasmus and István Magyari on the Justification of War	27
Stefany CEVALLOS: Public Service Management in Ecuador	37
Tamás HÁBERMAYER, Péter HORVÁTH: Voluntary Rescue Service in Hungary: The HUSZÁR Team	45
Gergely HERCZEG, Ágoston RESTÁS: Solutions for the Accessibility of Water Sources for Fire Extinguishment	55
Ferenc KOCZKA: Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment	65
Tamás SZÁDECZKY: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000	83
Szilveszter SZELECZKI: Outlining a Set of Theory-based Requirements for the Future Digital Soldier	95
Tomáš ZEMAN: Soft Targets: Definition and Identification	109