Hadtudományi Szemle
13. évfolyam (2020) 2. szám 111–127. • DOI: 10.32563/hsz.2020.2.9

Balázs Kárász[1]

Social Aspects of Reliability and Security Issues of Authentication Solutions[2]

Azonosítási megoldások megbízhatósági és biztonsági problémáinak társadalmi kérdései[3]

Abstract

This paper marks out possible further research directions based on the research problem that security awareness or unawareness has an impact on the correct approach of society-related security issues, acting as a human risk factor. Considering technically emerging reliability problems of authentication solutions (focusing on biometrics) as vulnerabilities, the author makes suggestions upon implementing possible risk management steps. Elements of the complex answer given to security questions related to private and organisational (employee) behavior can be an increase of the level of leadership commitment, evolvement of the organisational security awareness and continuous improvement of problem handling process.

Keywords: *authentication, reliability, biometrics, security awareness.*

Absztrakt

Jelen közlemény lehetséges kutatási irányokat fogalmaz meg annak a tudományos problémának mentén, hogy a biztonságtudatosság vagy annak hiánya humán kockázati tényezőként gyakorol hatást az egyes társadalmi érintettségű biztonsági kérdések helyes megközelítésére. Az egyes azonosítási (köztük kiemelten a biometrikus) megoldások technikai jellegű megbízhatósági problémáit támadhatóságként értelmezve a szerző

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz – University of Public Service, Doctoral School of Military Engineering, PhD student, e-mail: karaszb@gmail.com, ORCID: 0000-0003-2065-4928

[2] This research was supported by the ÚNKP-19-3-I-NKE-14 New National Excellence Program of the Ministry for Innovation and Technology.

[3] Jelen tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-19-3-I-NKE-14 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

javaslatot tesz lehetséges kockázatkezelési utak megvalósítására. A magánéleti és szervezeti (munkahelyi) viselkedéssel kapcsolatos biztonsági kérdésekre adott komplex válasz pillérjeit a vezetői elkötelezettség növelésében, a szervezeti biztonságtudatosság kialakításában és a problémakezelés folyamatos fejlesztésében határozza meg.

Kulcsszavak: *azonosítás, megbízhatóság, biometrikus elemek, biztonságtudatosság.*

1. Introduction and research details

Biometrics are applied wide-spread among authentication methods in various industrial sectors through information technology solutions as well as radio-frequency devices, thanks to their primary advantages in terms of being unique, universal, permanent, and measurable.

1.1. Scientific research problem

Based on the above-mentioned issues, the following question arises: what kind of impact does security unawareness – as a human risk factor – have on the correct approach of socio-related security issues, especially from the aspect of authentication, when it comes to using solutions based on biometrical elements?

1.2. Research objective

The objective of this research is to outline possible risk management methods to improve organisational security awareness, through analysing military concepts of cyberspace operations and tools in the civil context when facing similar problems. The expected results will be useful for continuing research in the topic in military context.

1.3. Research methods

The author used theoretical and empirical research techniques, partly with the method of synthesis. Related scientific literature from Hungary, as well as abroad, from both military-related and civil professionals will be widely mapped and elaborated.

2. Situation and role of authentication in the context of cyberspace

In this chapter, the author locates authentication and its role within *cyberspace operations*. This term refers to all activities that, on the one hand, analyse and assess information environment, and on the other hand, harmonise influence, countermeasures and defence.

2.1. Dimensions of information environment and cyberspace layers

Information environment can be described as everything surrounding information that has an impact on it and influences its existence and function. Three dimensions of information environment can be defined. First, the *physical dimension* includes all places where information or its impact appears or is forwarded, such as Command and Control Systems, key managers and related infrastructure, communication devices and so on. Secondly, the *information dimension* describes the 'how?' through which the content and the flow quality can be influenced: all processes that collect, handle, store, forward and protect information. Thirdly, the *cognitive dimension* focuses exclusively on the human factor, herein, the following characteristics of either individuals or groups can all be included: information processing ability, preconceptions, judgment, the manner of making decisions – obviously influenced by social habits, habits of mind, religion, education, moral and motivation.[4]

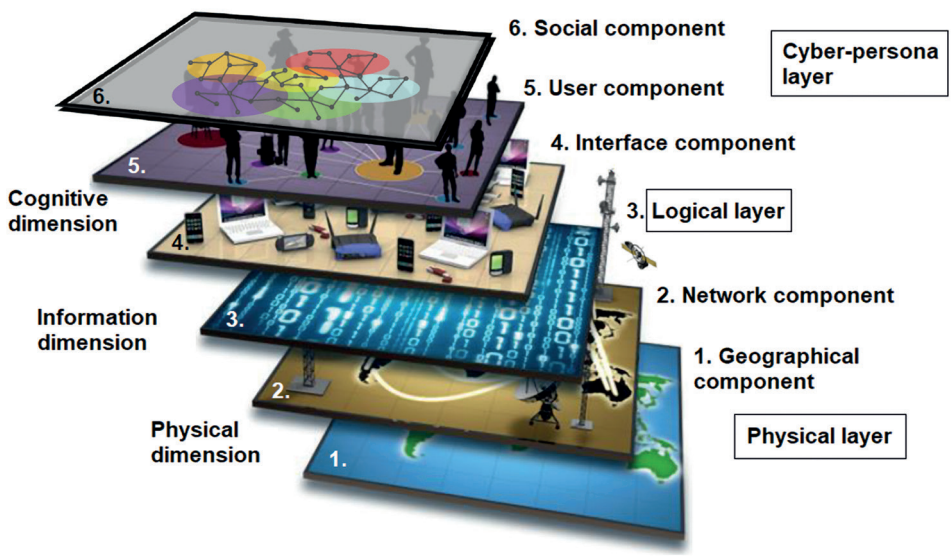

Figure 1. *Dimensions of information environment and components of cyberspace layers*
Source: compiled by the author based on Haig, Információs műveletek.

Cyberspace can be described as a mixture of virtual environment and physical or non-physical components. Physical components are part of the cyberspace and the physical domain at the same time. Military / defence context applies the total of components to the situational awareness concerning cyberspace, which defines the list of elements of the situation.

[4] Zsolt Haig, *Információs műveletek a kibertérben* (Budapest: Dialóg Campus, 2018), 151-152.

Three layers can be defined within cyberspace, which represent (and exist parallel to) the dimensions of information environment, and the layers can be further split into components. From the point of view of this research, the focus is to be put onto the *cyber-persona* layer, adequate to the cognitive dimension of information environment, acting as the digital representation of the network users.[5] Cyber-persona is simply a virtual identity used for collecting information or influencing others, while hiding the actor's real identity.

2.2. Connection to cyberspace operations

Since cyberspace consists of an environment created by information devices, the toolset of information technology will be able to modify cyberspace by creating new component types, administering, modifying or removing existing ones – these possible steps are called cyberspace operations. The purpose of *cybersecurity* is therefore the detection of such activities, and taking countermeasures in order to reduce and eliminate consequences.

According to FM 3-12, there is complex categorisation of *cyberspace actions* executed by cyberspace forces.[6] The main categories are *Defense, Security, Attack, ISR* and *OPE*, where authentication is applied to Defense and Security purposes. I would like to highlight that *cyberspace operations* were formerly classified as a support capability within *inform and influence activities*, among others, cyber electromagnetic activities. In a more holistic view, several interrelations of *cyberspace operations* with the following capabilities supporting information purposes can be discovered: *psychological operations, presence-posture-profile, information defense, deception,* and *civil–military cooperation*. All the above mentioned capabilities can have impact on the cyber-persona layer, what is crucial from the point of view that authentication process is a basic element of all components within this layer, connecting the physical user to its virtual pair that effectively has access to the virtual data domain.

2.3. Role of authentication

As Figure 1 shows, layers and their components are related to each other through various means despite that they are distinct. What is important here is that authentication plays a significant role in making understandable how relations between layers are built up. Authentication is not limited exclusively to the cyber-persona layer, connecting the interface with the users and enabling them to build social networks, although its roots can be found in the user component (unique user addresses, IP and e-mail

[5] Veronika Deák, 'Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során,' *Hadtudományi Szemle* 12 (2019), 3. Available: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/HSZ_2019_3-6_Deak_95-111.pdf. (28. 01. 2020.)

[6] *FM 3-12: Cyberspace and Electronic Warfare Operations*, Washington, D.C., Headquarters, Department of the Army, April 2017. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20-WEB%201.pdf. (15. 01. 2020.)

addresses and so on). It can be considered much more as a strong link towards the logical layer (elements such as information, transfer protocols, software applications, user data, internet domain names belong here) and moreover, towards the physical layer (some relevant elements of which are servers, radiofrequency transfer devices, electromagnetic spectrum).

3. Authentication solutions using biometrics

In this chapter, the author gives an overview of authentication methods and technologies based on measuring biometrical elements, including a comparison with regard to the characteristics of each solution.

3.1. Overview of biometrics

Biometrics are inherent characteristics of human beings as well as most of the animals that relate to *primary* (physical representation, e.g. shape of body) or *secondary* (pattern of behavior – often influenced by social factors) attributes. Biometrics can be described by a number of hard criteria, most important of which is that these attributes have to be able to be physically perceived either by sense organs or collected/measured by devices using radiofrequency or imaging technologies. Apart from *measurability*, six further requirements must be met in order to call a biometrical attribute applicable for authentication.[7]

Firstly, it has to be unique, universal, and permanent. A biometrical attribute is *unique* if it can be unambiguously assigned to a certain individual, *universal* if it can be interpreted in context of the entire (observed) society or community, and *permanent* if it remains unchanged through long enough time or forever. Its secondary characteristics are those of *acceptability* and *circumvention,* as well as several *performance* metrics can be related. A biometrical authentication technology can be called acceptable from the point of view of individuals in the relevant population if they are willing to have their biometric trait captured and assessed. Circumvention in this context means how easily biometrical elements might be imitated using an artifact or substitute. Performance metrics are used to describe the reliability of biometric systems with indices, rates concerning the steps of an authentication technology, for instance, enrollment, capture, match or capacity.

A crucial advantage of biometrics can be found in its inherent nature, as thanks to it, biometrics can be integrated into multi-factor authentication as an inherent factor, paired with either knowledge-based or possession-based factors, or both. Some of the arising security issues may find a solution clue by emphasising the significance of this property of biometrics.

[7] *Biometrics: Personal Identification in Networked Society,* ed. by A. K. Jain, R. Bolle and S. Pankanti (Kluwer Academic Publications, 1999).

3.2. Early precedents

Early precedents of using biometrics can be mentioned from both ancient times and World War II. The biblical patriarch Isaac wants to bless his firstborn son Esau, but being blind, he can only rely on Esau's primary characteristics (hairy arm) which he can touch. We can see right here an example of how this 'authentication method' could be spoofed by Esau's brother Jacob. Some decades later, in a story depicting a conflict between Gilead and Ephraim, two ethnic groups, the defenders ask the troops arriving in incognito to pronounce a certain word 'Shibboleth'. Since they pronounced it wrong, they were revealed as invaders and the defenders concluded this immediately.[8]

The second example has been widely used in many ethnic or military conflicts throughout history. A collection of so-called *shibboleths* repeatedly turned up, starting from Western Europe in the 13th century, through various occasions in the 20th century, connected to the World Wars; and it has not ended, as nowadays dialects are commonly used to tell foreigners apart.[9] As these examples show us, the phenomenon of *shibboleth* is based on a secondary type of human characteristics and can be used for authentication to a certain extent – to be analysed in the next subchapter.

3.3. Compatibility of biometrics with authentication

According to the facts and taking into consideration the aspects mentioned above, I collected in the table below all available data concerning the topic of biometrics that are relevant to the research work (see Table 1). The assessment factors are based on the previously mentioned classification.[10] Below the table, the most important findings will be explained in detail. In the table, criteria only partly fulfilled have a significantly deteriorating attribute that makes its use questionable as an authentication method.

I would like to point out first that in spite of being used world-wide, speech voice alone does not meet the requirement of uniqueness, it is only paired with the language used and partly the dialect that we can consider it as a reliable solution. Since speech voice changes in the long run to a minor extent, it is also partly valid to call it permanent. Nevertheless, speech tone can also be analysed on a high standard, so many useful applications and devices use various technologies to use it in part or at a certain step of an authentication process. Apart from the above concerns about speech, we can also mention the fact that although DNA would be able to meet all other requirements, it would hardly be technically feasible, and the lack of acceptability in the case of DNA, according to the current social environment, overwrites the concept of use in everyday life.[11]

Finally, the significance of signature should not be left out from the explanation. As we can see in the table, signatures are only partly used in authentication, mostly

[8] R. Anderson, *Security Engineering* (Indianapolis: Wiley Publishing, 2008), 261.
[9] O. Gramling, *Free Men are Fighting: The Story of World War II* (New York: Farrar & Rinehart, 1942).
[10] *Biometrics.*
[11] Anderson, *Security Engineering,* 273.

paired with ID cards and personal presence of the user, still it is most widespread in banking. Technologies of today enable banks already to follow the evolution of the user's signature, this way making up prognoses of the expected further shapes and types related to that particular user.

Table 1. *The fulfilment of hard requirements by biometrical elements*

✔ = *valid,* ⊖ = *partly valid,* ✖ = *not valid*

Biometrical element	Fulfilment of hard requirements			Used in authentication
	Unique	Universal	Permanent	
Signature	⊖	⊖	✖	⊖
Face geometry	✔	✔	✔	✔
Palm geometry	✔	✔	✔	✔
Vein geometry	✔	✔	✔	✔
Fingerprint	✔	✔	✔	✔
Iris pattern	✔	✔	✔	✔
Speech voice	⊖	✔	⊖	✔
Dialect	⊖	⊖	✔	✖
Handwriting	✔	⊖	✖	✖
Keystroke dynamics	✔	⊖	✖	✖
DNA	✔	✔	✔	✖
EEG signal	✔	✔	✖	✖
ECG signal	✔	✔	✖	✖

Source: compiled by the author

4. Reliability and security issues

In this chapter, the author enlists various problematic issues concerning the reliability of authentication solutions, focusing on the ones based on biometrical elements, enriched with examples for overcoming nowadays' technical, legal, and human challenges.

4.1. General and solution-specific weaknesses

The reliability of a biometrical authentication solution can be influenced negatively by numerous sorts of external effects (which have an impact generally on the technology applied), as well as factors which have roots in the biometrical element or the solution that is used. All these phenomena impact all layers of cyberspace where authentication plays a significant role, being a defence technology. Biometrics have the ability to improve user-friendliness and reliability of authentication methods, still, threats on related weaknesses should be thoroughly overviewed and analysed.

Generally, environmental issues may occur when the reliability of an authentication process is discussed. Such examples are dirt, noise, lack of (back)light or radio waves that

can easily modify the result of authentication by having an impact on the technology. One of the most general problem researchers face is insufficient data – since biometrics are not like QR codes, damage over a certain percentage cannot be overcome by standard solutions (not to mention AI at this point). These general problems can be easily interpreted as solution-specific problems according to the following:

- Fingerprint can be damaged or worn by manual labor – therefore law enforcement organisations and armies have limited opportunities to use fingerprint in authentication for investigation purposes unless scanning all available fingerprints.
- Fingers, iris and other body parts can be seriously damaged or removed by an accident – which can occur on battlefield, causing a continuous challenge to armies to maintain biometric data and executing authentication at any moment.
- Both above-mentioned damages can also result in misleading authentication solutions, which can affect the outcome of an investigation or put a soldier's life at risk.
- Iris scanners can have difficulties in detecting the smallest details if one has dark eyes or wide pupils in the moment of the authentication test.
- The user can be mistaken by voice recognition systems if being drunk, stressed, having a respiratory sickness or disorder, or speaking with a strong accent.[12]

When speaking about solution-specific weaknesses, authentication system developers must also consider thoroughly the possibility of fake data to be used by intruders into information infrastructures and systems. The factor of spoofing therefore cannot be left out from the list of vulnerabilities, since it cannot be mitigated by improving only technical circumstances, but various intelligence aspects also need to be organised on high standard.

4.2. Issues affecting social and technical aspects

I called the issues analysed above consequently as weaknesses, although we can also define and categorise them as vulnerabilities, regarding their successful application results in meeting all the hard requirements in limiting biometrics, as marked in Table 1, and their capability to successfully execute operations in cyberspace. Moreover, a minor weakness can lead to social problems, involving either a smaller group of society or the entire humanity.

4.2.1. Legal issues

Not limited to GDPR of the EU and similar legal measures taken in order to manage data privacy on a higher and more secure level when dealing with biometrical elements, the

[12] Imre Négyesi, 'A mesterséges intelligencia és a hadsereg II. (Beszédfelismerő rendszerek I.).' *Hadtudományi Szemle* 10, no 2 (2017), 35–46. Available: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_035-046.pdf. (28. 01. 2020.)

reliability of biometrics is also affected by concerns that aim to protect personal data from cyberattack breaches,[13] spoofing, illegal use and cyber terrorism. This resulted in that, for example, smartphones having a fingerprint scanner (or iris scanner) used for unlocking itself store only a fragment of the biometrical data scanned at the first registration. Technology is limited to an at most 60-80% comparison of the scanned fingerprint with the stored fragment. This results in that a similarity level up to an extent of 60-80% is considered acceptable for authentication, which means that the vulnerability level of the process equals 1 minus the same percentage.

The legal aspect of administering handicapped people when using biometrical authentication first became an issue when machine-based processing spread wide, especially in public and other services that dispose of critical infrastructure elements, while not continuously being overviewed by any human contributor.

The recent scandal of FaceApp, which raised several interesting questions in summer 2019, relates to the next topic, too (besides awareness issues), but has stronger links to data privacy and legal concerns. This mobile application features filters turning the profile photo of the user into other states (on the dimensions of age, gender, outlook, hairiness etc.). This is supported by an artificial intelligence algorithm that analyses the determinative characteristics and dimensions of the face, i.e. all crucial data necessary for a biometric authentication process. By accepting the terms and conditions, the user allows the owners/developers to use that data and hand it over to third parties for any unspecified reason. The complexity of the problem derives from the security unawareness of the user influenced significantly by a social media hype, as well as the technology enhanced by AI providing the developers with an accurately detailed analysis of face geometry of the users.

4.2.2. Artificial intelligence

Among challenges that drive research of the future of cyber security, the collection of technologies using artificial intelligence (AI) is one of the biggest ones. When discussing about AI it needs to be outlined that there are several major technologies attached to AI working interdependently, including machine learning, deep learning, robotics, cloud computing, IoT, VR – all having the common characteristic that they are based on virtual networks,[14] out of which *the social component of cyber-persona layer of cyberspace* is built up.

AI can be implemented in various scales starting from wearable devices through portable tools and autonomous vehicles to intelligent buildings and further. Military researchers nowadays use a combination of VR and AI in the process of training soldiers, which gives accurate feedback on the development, makes person-specific

[13] D. Harwell and A. G. Fowler, 'U.S. Customs and Border Protection says photos of travelers were taken in a data breach,' *The Washington Post,* 10. 06. 2019. Available: www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/. (15. 01. 2020.)

[14] Imre Négyesi, 'A mesterséges intelligencia és a hadsereg I. (Beszédfelismerő rendszerek I.),' *Hadtudományi Szemle* 10, no 2 (2017), 23–34. Available: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf. (28. 01. 2020.)

suggestions of training details; nonetheless, gigabytes of data per person are stored in the process, including encrypted biometrical information.[15]

China has been developing and testing an observation and intelligence system that is based on face-recognition technologies supported by AI softwares – recently implemented (on 24 July 2020) –, which will impact the everyday life of all citizens and businesses of the country.[16] The AI used here, in line with what we said about the unreliability of biometrical authentication in sub-chapter 4.1, enhances certainty, and this way, the system provides its developers with continuous self-amelioration. Agreed that AI aims to fix technical issues, the other side of the coin, including social issues, should not be ignored.

Firstly, such professional systems can be used for malicious purposes, impacting a group of or the entire society. Secondly, the amount of data and information collected and stored needs a high cyber defence level to avoid breaches and the consequences of the previous aspect. Thirdly, deep learning technologies are now fully able to imitate the voice, style, speech habits of an executive manager via telephone (*deepfake*), in order to completely mislead a dedicated employee and make them transfer money to a certain account – stealing the amount from the company.[17]

4.2.3. Cyber terrorism

When considering cyberspace operations related to biometrical authentication, it must be clearly seen that terrorists also learn new tactics and ways of taking part in the evolution of hybrid warfare.[18] Without a detailed analysis of this serious factor influencing cyber defence, I would like to point out only one professional area where biometrics is used, which I have not mentioned yet. It seems that *healthcare* is threatened by cyber terrorists from many points of view. What should be highlighted are storage and examination of biological data such as DNA, analysed blood samples which are the basis of examination, research and healing, and also biometrical elements meeting all hard requirements, therefore the processed data based on these elements need to be stored and transferred in a digitally secure way, through authorised access only. IoT for example can also mean a significant threat exposure of healthcare data.[19]

[15] Gergely Kovács and Júlia Hornyacsek, 'Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben,' *Műszaki Katonai Közlöny* 29, no 2 (2019), 117–132. Available: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/MKK_2019_2_10_Kovacs_Hornyacsek.pdf. (15. 01. 2020.)

[16] F. Liang, V. Das, N. Kostyuk and M. Hussain, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure,' *Policy & Internet* 10, no 4 (2018), 415–453.

[17] C. Stupp, 'Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case,' *The Wall Street Journal*, 30. 08. 2019. Available: www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case- 11567157402. (15. 01. 2020.)

[18] László Kovács, *A kibertér védelme* (Budapest: Dialóg Campus, 2018), 197–203.

[19] J. D. Kilgallin, 'Securing RSA Keys & Certificates for IoT Devices,' *Keyfactor,* 2019. Available: https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era. (15. 01. 2020.)

4.3. Role of security (un)awareness

I will demonstrate the role of security awareness in everyday life through three distinct examples in areas where it is crucial for each user to be conscious of the environment, the data and possible threats. Security together with safety is the second level of needs, and belongs to the basic needs together with physiological needs.[20] This does not mean, however, that people using information technology are aware of the threats related to them, and that they do their best to protect their data, especially personal and private data, from attackers.

Thanks to the limited capacity of our own background storage on our electronic devices used for storing images, movies/videos and music or other sound files, popular free cloud service providers discovered the market niche in offering a free space of gigabytes. Cloud is on the one hand safe, since it stores data encrypted and distributed, but on the other hand, when used for free, the data is sold to third parties anonymously to serve either simple database widening or machine learning algorithm enhancing purposes. In that case, the product is the user and their data, which is precious if analysed and used for targeted marketing actions, for instance. If the cloud service is paid for, its providers are interested in protecting the stored data, since in this case, the service itself is the product, providing the user with a safe and reliable environment.

Multiple research results show that the culture of password and PIN-code usage is on a very low level. As knowledge-based authentication methods are commonly used worldwide on information technology devices and many other services (for example mobile phones, smart televisions, access control systems, digital customer services logging in to the personalised interface of any website), it is still a struggle to convince users to use multi-factor authentication (to be discussed below) and to change their password or PIN-code to something more sophisticated than neighboring keys on the keyboard – either numbers or letters. Password '123456' has been leading the top 25 common passwords list since 2013 and had a high position beforehand, while the second most popular is simply 'password'.[21] It is still less known by users that solutions were invented to store password safely on the computer, while it is not needed to even remember or know the password. The automatically generated passwords are safe not just from the point of view that they contain special characters, upper and lower case letters and numbers, but if the password itself remains hidden even from the user, the risk arising when written down somewhere else than a safe storage is mitigated to zero.

Besides codes and passwords, there are other innovative ways on smart devices to enlarge the circle of possible knowledge-based authentication methods. The smartphone can be set up to require the user to do a certain order of moves, which are

[20] A. H. Maslow, 'A theory of human motivation,' *Psychological Review* 50, no 4 (1943), 370–396.

[21] M. Ehrenkranz, 'The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius,' *Gizmodo,* 12. 13. 2018. Available: https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705. (15. 01. 2020.)

detected using its accelerometer.[22] This works similarly to the pattern drawn onto the display, and the principle behind it is the same as with the codes and passwords, the authentication method takes the correct order of bit-level information into account.

5. Suggestions to manage risks

In this chapter, the author collects suggestions with the help of which the human risks collected and highlighted above can be successfully managed, focusing on security aspects appearing in the context of organisational structures and interactions.

5.1. Multi-factor authentication

The principle (and related solutions) of multi-factor authentication is a reasonable answer to several risks related to the unreliability of the factors. We have collected the issues concerning the inherent and the knowledge-based factors so far. The possession factor is based on something that the user and exclusively the user disposes of; it can be – in some cases – the weakest of all authentication factors. It certainly needs to be complemented by another authentication method based on either of the two other characteristics or both. What underlies such a statement is that the possession-based factor consists of a physically present data carrier, among others, in form of a chipped card linked to a bank account, an electronic or RFID device authenticating its entitled user by assigning personalised data, or as a token, generating one-time utilisable code as a password.

PSD2 bank regulations implemented on 14th September 2019 in Hungary also require – among others – a second factor in authentication when transferring money or paying online by card. During the authentication process, after giving the data of the bank card (possession factor) for payment, the bank generates a one-time code of 5-6 digits sent via SMS to the phone number of the user, which has previously been recorded and acknowledged as an official communication platform between the client and the bank.[23] The code now is another possession-based authentication factor, as users must keep their mobile device by themselves to receive it. When paying online by card using the mobile device itself, it is a questionable authentication method, since it cannot be defined as MFA anymore if the two possession-based factors share the same physical device.

The use of location-based authentication as a fourth factor is gaining importance and attention; it involves the physical location of the user. This can substitute either the possession-based or the knowledge-based factor when using multi-factor authentication,

[22] A. Primo, V. Phoha, R. Kumar, A. Serwadda, 'Context-Aware Active Authentication Using Smartphone Accelerometer Measurements,' *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops,* 2014, 98–105. Available: www.cv-foundation.org/openaccess/content_cvpr_workshops_2014/W01/papers/Primo_Context-Aware_Active_Authentication_2014_CVPR_paper.pdf. (15. 01. 2020.)

[23] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 november 2015 on payment services in the internal market.

by adding another 'dimension' to the process in terms of the location. Obviously due to technical limits, a certain value of error margin should be set in this case, which on the other hand can be reduced step-by-step with the help of continuously enhanced satellite, navigation, and positioning systems.

Summarising the above-mentioned facts, we can confirm that multi-factor authentication may provide the user and the service provider with a potential in enhancing security level by adding layers to the authentication process, still it is useful to analyse the situation concerning how data should be handled and protected in each combination of the various factors used.

5.2. Organisational security awareness

Besides the technical mitigation solutions, security risks should also be monitored and handled on the human side, especially on the field of physical or digital security, for organisational purposes. In the case of physical security, the risk mitigating effects of, for instane, access control systems, metal detectors, ID check upon entrance, presence of security guards at receptions, background check of new colleagues before admission to sensitive jobs are obvious.

The latter, however, builds a bridge from purely physical security to human security with secondary attributes checked on, and this phenomenon can be perceived in the digital context as well. This is because information needs to be defended on both virtual (digital) and physical surfaces – the principles behind therefore need to be equivalent. Information systems also have virtual access control, authentication, key management to limit the users' rights in order to improve effectiveness of information protection. In parallel to physical security, human security must be controlled on top-level, having connections to Human Resources, Learning and Development as well as Security Departments or adequate organisational departments that are responsible for these areas.

Professional services such as individual or group training programs, coaching, mentoring are all based on the following three components: self-knowledge and soft skills, professional skills, teamwork. Now I would like to focus only on *training programs*, which can be defined in the context of this paper as a process within the activity of development, and which helps employees improve the execution of work in their current job with educational tools and circumstances.[24] Ideally, in case of a training program, *HR* would be responsible for the frames (soft skills, teamwork abilities), *Security* would provide relevant professional skills as it is for security awareness training programs, while *L&D* would seek solutions for coordination, personalisation, and implementation within organisational relations.

A training program would traditionally consist of the following parts (in the following order): theory, examples, conclusion, application. Optimally, it would develop to the next level: case studies and simulated situations, theory deduction,

[24] Balázs Kárász, 'Biztonságtudatossági tréningek hatékonyságának vizsgálata,' *Hadmérnök*,14, no 2 (2019), 313–324. Available: http://hadmernok.hu/192_26_karasz.pdf. (15. 01. 2020.)

application, action plan. This way, the organisation makes an attitude in its colleagues which brings forward motivation and effectiveness, supporting the purposes of the organisation in three steps:

1. Thanks to the theory deduction method, the organisation becomes able to make process-level changes to improve effectiveness.
2. Cyclical problem management process can be elaborated on each hierarchic level due to unlocked creativity and intuition potential.
3. The organisational culture can be basically renewed as consciousness and awareness hand-in-hand make up a significant part of the employees' behavior.

As for the professional side, it is necessary to follow a detailed plan to cover all crucial information security areas including the importance of the aspects below – to be continuously widened by new areas, which basically are general awareness aspects:

- role of data and information;
- physical security;
- human security;
- private life risks;
- phishing techniques;
- social engineering;
- passwords, codes;
- malicious programs, viruses;
- cloud, browsers, cookies;
- mobile and smart devices;
- social media;
- multi-factor authentication.

In all the above-mentioned facts, it needs to be taken as a basic fact that impulses influencing private life can have a significant positive effect on business life as well as behavior and mindset when acting as an employee.

5.3. Leadership and commitment

Since overall security needs to be managed by the top level in an organisation, some hard requirements must be set up to maintain the overview and control potential. It is redacted in Clause 5 in most ISO standards according to the High-Level Structure: 'Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.'[25] The effort mentioned here can be comprehensively related to all fields of security, since it is best translated as commitment – the reason for having the Clause named like that. However, the most important question is not whether the effort must be demonstrated or not, but how it can be demonstrated.

[25] 'ISO/IEC Standard No. 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.' *International Organization for Standardization*. Available: www.iso.org/standard/54534.html. (15. 01. 2020.)

Firstly, commitment to develop awareness among employees must be rooted in the awareness of the leaders themselves. Security awareness training programs therefore should not be limited to lower levels in the organisational structure, but in a different way, extended for leaders and top management, too, in order to create fundaments for effective development of awareness. The focus of top management trainings would optimally simply be around risks translated transparently to cash, this way conformed with their mindset and leadership skills.

Secondly, as a result of risks being assessed in a way that they make up value-added information, decision making processes can be optimised and much more effective, therefore the return on investment in training programs[26] can be measured more precisely, besides that its value is highly likely to increase.

Thirdly, if decisions made based on reliable information and leadership commitment are of high level in the organisation, the degree of responsibility taken for each decision by the leaders themselves – originally the highest human risk in case of leaders, a deficiency of hierarchic organisations – can be mitigated to a high extent.

6. Conclusion and further work

In this chapter, the author collects and structures conclusions and possible answers to the above issues, then gives an outlook of possible directions to be followed in the field of research related to biometrics and security engineering.

6.1. Conclusion

Based on the above overviewed scholarly concepts on cyberspace layers, the role of biometrical authentication within them can be described as a liaison between the cyber-persona and logical layers. Three major security areas can be defined where technical reliability issues should be handled: solution-specific technical weaknesses, impacts of attached external technology, and social risks. The latter being considered as depending highly on human risk factors, first, organisations and service providers, especially when it is for critical infrastructure, should mitigate risks by applying the most secure authentication methods possible and should not handle the private life of employees apart from their workplace behavior.

The second main part of the solution found by this research is – besides legal aspects – the enhancement of organisational security awareness. Achieving such purposes has roots in leadership commitment, the improvement of which can lead to a more effective problem management cycle and decision-making process implemented in the organisation – and it can be embedded in the organisation culture.

[26] Kárász, 'Biztonságtudatossági tréningek.'

6.2. Further work

In my further research, I would like to concentrate on security and reliability issues of authentication and related impacts on critical infrastructure. Since critical infrastructure always disposes of a component of information infrastructure, and organisations operating them are highly specialised on their professional area (energy, transport, public services and so on), it is exposed to malicious cyberspace operations, which expands the importance of smaller issues playing an important role thanks to their position between the layers of cyberspace.

7. Summary

This research collected international scholarly concepts about the role of authentication within cyberspace in the context of various operations as well as weaknesses, which together cause vulnerabilities, and which can be managed as security risks. The impact of security unawareness – as a human risk factor – on the correct approach of socio-related security issues has been highlighted especially in regard of biometrical solutions. The research also successfully outlined possible risk management methods to improve organisational security awareness, through analysing military concepts of cyberspace operations and tools from the civil context applied when facing similar problems. The results are a useful basis for continuing research in the topic, and are suggested to be put in military engineering context.

References

Anderson, R.: *Security Engineering.* Indianapolis: Wiley Publishing, 2008.

Biometrics: Personal Identification in Networked Society. Ed. by Jain, A. K. – Bolle, R. – Pankanti, S. Kluwer Academic Publications, 1999.

Deák, Veronika: 'Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során.' *Hadtudományi Szemle* 12 (2019), 95-111. DOI: https://doi: 10.32563/hsz.2019.3.6

Gramling, O.: *Free Men are Fighting: The Story of World War II.* New York, Farrar & Rinehart, 1942.

Haig, Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Kárász, Balázs: 'Biztonságtudatossági tréningek hatékonyságának vizsgálata.' *Hadmérnök* 14, no 2 (2019), 313–324. Available: http://hadmernok.hu/192_26_karasz.pdf. (15. 01. 2020.)

Kovács, Gergely – Hornyacsek, Júlia: 'Korszerű oktatási eszközök és módszerek alkalmazása a polgári védelmi felkészítésben.' *Műszaki Katonai Közlöny* 29, no 2 (2019). 117–132. DOI: https://doi.org/10.32562/mkk.2019.2.10

Kovács, László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Liang, F. – Das, V. – Kostyuk, N. – Hussain, M.: 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure.' *Policy & Internet* 10, no 4 (2018). 415–453. DOI: https://doi.org/10.1002/poi3.183

Maslow, A. H.: 'A theory of human motivation.' *Psychological Review* 50, no 4 (1943). 370–396. DOI: https://doi.org/10.1037/h0054346

Négyesi, Imre: 'A mesterséges intelligencia és a hadsereg I. (Beszédfelismerő rendszerek I.).' *Hadtudományi Szemle* 10, no 2 (2017), 23–34. Available: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_023-034.pdf. (28. 01. 2020.)

Négyesi, Imre: 'A mesterséges intelligencia és a hadsereg II. (Beszédfelismerő rendszerek I.).' *Hadtudományi Szemle* 10, no 2 (2017), 35–46. Available: http://epa.oszk.hu/02400/02463/00035/pdf/EPA02463_hadtudomanyi_szemle_2017_2_035-046.pdf. (28.01. 2020.)

Internet sources

Ehrenkranz, M.: 'The 25 Most Popular Passwords of 2018 Will Make You Feel Like a Security Genius.' *Gizmodo,* 12. 13. 2018. Available: https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705. (15. 01. 2020.)

FM 3-12: Cyberspace and Electronic Warfare Operations. Washington, D.C., Headquarters, Department of the Army, April 2017. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf. (15. 01. 2020.)

Harwell, D. – Fowler, G. A.: 'U.S. Customs and Border Protection says photos of travelers were taken in a data breach.' *The Washington Post,* 10. 06. 2019. Available: www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/. (15. 01. 2020.)

'ISO/IEC Standard No. 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.' *International Organization for Standardization*. Available: www.iso.org/standard/54534.html. (15. 01. 2020.)

Kilgallin, J. D.: 'Securing RSA Keys & Certificates for IoT Devices.' *Keyfactor,* 2019. DOI: https://doi.org/10.1109/TPS-ISA48467.2019.00030

Primo, A. – Phoha, V. – Kumar, R. – Serwadda, A.: 'Context-Aware Active Authentication Using Smartphone Accelerometer Measurements.' *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops,* 2014, 98–105. DOI: https://doi.org/10.1109/CVPRW.2014.20

Stupp, C.: 'Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case.' *The Wall Street Journal*, 30. 08. 2019. Available: www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. (15. 01. 2020.)