Hadtudományi Szemle
13. évfolyam (2020) 3. szám 71–86. • DOI: 10.32563/HSZ.2020.3.6

Balázs Kárász[1] – Imre Négyesi[2]

Information Security Responsibilities of Critical (Information) Infrastructures in the Aspect of Human Risk Factors

Kritikus (információs) infrastruktúrák információbiztonsági feladatai a humán kockázati tényezők tükrében

Abstract

With regard to the threats of information society nowadays, the digital asset management and the safety of the related information systems as well as critical infrastructure elements became highly important. The defence of cyberspace itself evolved as a social necessity. This paper aims to provide an overview of how each of the occurring human risk factors influence the effectuation of information security purposes of firms and/or organisations operating critical infrastructure or critical information infrastructure, as well as the engineering of their data processing and data analytics procedures. Moreover, the helpful role of the possible methodological toolset (connected to HR, management and risk management) is also assessed in the context of managing and improving information security awareness.

Keywords: *critical infrastructure, information security engineering, human risk factors, artificial intelligence, security awareness*

Absztrakt

A napjaink információs társadalmát érintő fenyegetések miatt kiemelten fontossá vált az elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve

[1] Doktorandusz, Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola – University of Public Service, Doctoral School of Military Engineering, PhD student, e-mail: karaszb@gmail.com
[2] Dr., egyetemi docens, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar – University of Public Service, Department of Military Sciences and Officer Training, PhD, Associate Professor, e-mail: negyesi.imre@uni-nke.hu

a létfontosságú információs rendszerek és rendszerelemek biztonsága. Társadalmi elvárássá fokozódott a kibertér védelme. Jelen tanulmány áttekintést kíván nyújtani arról, hogy a kritikus infrastruktúrát vagy kritikus információs infrastruktúrát üzemeltető vállalatok és/vagy szervezetek információbiztonsági törekvéseinek megvalósíthatóságát és adatfeldolgozói, adatelemzői folyamataik szervezését mely humán kockázati tényezők milyen módon befolyásolják, ezek közül milyen hatékonysággal és milyen (HR-, menedzsment és kockázatkezelési vonatkozású) módszertani eszköztár segítségével kezelhető és fejleszthető az információbiztonság-tudatosság.

Kulcsszavak: *kritikus infrastruktúra, információbiztonsági tervezés, humán kockázati tényezők, mesterséges intelligencia, biztonságtudatosság*

1. Introduction and research details

Due to current threats on information society, as well as the growing need of dynamic development in safety culture, it became pronouncedly important to protect electronic data assets, the information systems managing them, and the security of critical information systems and system elements. In Hungarian, the judicial terminology[3] prefers using *essential/vital systems and establishments*, instead of the scientifically and professionally wide-known terminus critical infrastructures. On the one hand, this paper does not make a distinction between these two expressions (even in parts), and regards them as being synonyms, according to recent scientific records. On the other hand, the problem emerging from the difference is discussed in Chapter 4.1.

1.1. Scientific research problem

Based on the above-mentioned issues, the following question arises: how can organisations operating critical infrastructures effectively react to cyber threats by applying civil methods of HR and risk management, as well as security awareness development?

1.2. Research objective

The objective of this research is to synthesise possible methods and tools to improve organisational information security awareness, through analysing the available literature. As a second step, the research aims to outline major responsibilities of critical infrastructures, which can be effectuated as reactions to the effects of human risk factors. The expected results will be useful for continuing research in the topic in military context.

[3] Act CLXVI of 2012 *on the identification, postulation and protection of vital systems and establishments* does not use the term 'critical infrastructure'.

1.3. Research methods

The authors 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 are widely mapped and elaborated, in terms of review papers, monographs, conference publications, laws and internet sources.

2. Threats to information security

In this chapter, the authors locate information security and its role within *cyberspace*, referring to the human dimension and all cyberspace operations that influence it.

2.1. Information security within cyber warfare

The content of military engineering sciences is currently dynamically and constantly widening, now already covering information security, protection of energy safety and the protection of critical infrastructures. *Act L of 2013 on the electronic information security of state and local government organisations* pronounces that it is a social expectation – besides being crucially important in favour of the nation – to protect cyberspace.[4] Minister of Defence Tibor Benkő has also outlined in May 2018, on the shared audition of Committees, that beyond conventional military activities, new challenges can be seen in hybrid warfare including cyber warfare, and he emphasised the importance of Hungary's participation in the cyber defense distribution platform, too.[5] Postmodern or new generation or hybrid warfare of nowadays features in general the non-conventional forms of warfare, appearances with a wider toolset, and indirect, exhausting warfare, and is characterised by digitisation and comprehensive approach.

2.2 Cyberspace and information security

The first chapter of the book *Electronic warfare*[6] interprets and analyses the aspects of new generation warfare in the context of information and cyberspace operations. Since information battlefield (connected to conventional theaters of war) and electronic warfare are inseparable, questions discussed later in the monograph also cover the concepts of information supremacy, cyberspace operations, intelligence, support, defence and countermeasures.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Available: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (27. 04. 2020.)

[5] Gergely Tóth, 'Leendő honvédelmi miniszter: A honvédséget az alapoktól kell újraépíteni.' *Index.hu,* 14. 05. 2018. Available: https://index.hu/belfold/2018/05/14/benko_tibor_honvedelmi_miniszter_meghallgatas_orszaggyules_bizottsag/ (27. 04. 2020.)

[6] Zsolt Haig, László Kovács, László Ványa and Sándor Vass, *Elektronikai hadviselés* (Budapest: Nemzeti Közszolgálati Egyetem, 2014).

Nowadays, cyberspace network technologies entirely permeate and determine human lives. Besides conventional use of networks, the role of physical devices interconnected via internet is becoming more important, new generations of network technologies appear in cyberspace and moreover, being active in social media, users become part of the network itself. It is particularly important and apposite to conduct reasoning and discussion about how security awareness of users can be enhanced. Thanks to all that, the interpretation of cyberspace transforms, and the definition of threats appearing within is widening, since complex information operations can be effectuated in cyberspace. The risk effect potential of human factors also significantly grows in parallel.

For confirmation of such facts, another monograph titled *Information operations in cyberspace*[7] introduces milestones in the development of info-communication technologies, describes current directions of development concerning main network technologies, and further on, through a complex analysis, outlines trends of evolution, improvement and transformation of the above. Finally, certain opportunities are specified upon cyberspace appearances and the application of particular information operation capabilities.

The Defence of Cyberspace,[8] on the contrary, outlines especially the possibilities of cyberspace security and defence, with an international outlook. Attention is drawn to the personae of cyberspace, among which we can overview in detail the operation of hacktivists, cyber criminals, and terrorists. These actors are specified as the risk factor of highest importance, apart from different tools and methods, from the perspective of organisational security awareness.

2.3. Cyber terrorism

Parallel to and opposing physical attacks that have terroristic motivation, information terrorism or cyber terrorism gains more and more significance, thanks to being performed in a remote, cheap, non-traceable way and with lower overall risk level despite achieving a greater effect. Since during these attacks, the attacker faces lower defence level compared to physical defence lines and measures, it is particularly recommended to build up security appropriately in cyberspace.

These aimed attacks motivated by information hunger are carried out with the help of social engineering techniques (to be discussed in Chapter 3.1), and in general, they take advantage of the inappropriate practice of access management of the information system users or other human risk factors. On the opposite side, attacks against critical infrastructures aim actually to have greater *impact* instead of to gain higher *financial profit*, which affects the entire society through the interruption of certain processes and supply chain continuity – thus it results in a higher risk level in politics and national security. At present, cyber terrorism uses cyberspace

[7] Zsolt Haig, *Információs műveletek a kibertérben* (Budapest: Dialóg Campus, 2018).
[8] László Kovács, *A kibertér védelme* (Budapest: Dialóg Campus, 2018).

technologies for the purposes of propaganda, recruitment or financial acquisition, although no aimed cyber terrorist attack was carried out yet.

The reason why access management (including authentication solutions) means a key to the solution was mentioned above. According to FM 3-12, there is complex categorisation of *cyberspace actions* executed by cyberspace forces.[9] The main categories are Defence, Security, Attack, ISR (Intelligence, Surveillance and Reconnaissance) and OPE (Operational Preparation of the Environment), where authentication is applied to Defence and Security purposes. In a more holistic view, several interrelations of cyberspace operations with capabilities supporting information purposes can be discovered; these capabilites are psychological operations, presence-posture-profile, information defence, deception and civil–military cooperation. All the above mentioned capabilities can have impact on the cyber-persona layer, which 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.[10]

Considering cyberspace operations related to authentication solutions, we must notice that terrorists develop themselves by new methods and participate in the evolution of hybrid warfare.[11] We would like to highlight a professional area where biometrics is used: it turns out that from many points of view, *healthcare* as critical infrastructure is overall significantly threatened by cyber terrorists. We speak about the storage, examination and research of biological data such as DNA or analysed blood sample used in medical treatments, all of which can also be interpreted as biometrical elements, therefore the processed data based on these elements need to be stored and transferred in a digitally secure way, granting access to authorised personnel only. IoT also exposes healthcare data to high risk.[12]

3. The impact of human factors on information security

In this chapter, the authors give an overview of the human side of security issues, which are influenced significantly by artificial intelligence (further referred to as AI) technologies; related fields include training, authentication, intelligence and various digital solutions, among others.

[9] *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.).

[10] Balázs Kárász, 'Social aspects of reliability and security issues of authentication solutions.' Prospective appearance: *Hadtudományi Szemle* 13, no 2 (2020).

[11] Kovács, *A kibertér védelme*.

[12] 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.).

3.1. The role of social engineering

Social engineering comprises all sorts of techniques, with the help of which a manipulator breaks up and/or infects information systems having basic protection (gets access to sensitive data and databases), through cheating users using interpersonal and in-group interactions, previously having mapped and learned about human nature and relationships as well as their dynamics. Kevin Mitnick security consultant refers in his book[13] to his previous experiences gained as an attacker, interpreting social engineering as the art of deception in an authentic and trustworthy way. As possible solutions for protection, we can take into consideration raising awareness about the possibility of an attack, restriction of entry (in case of a physical establishment), professional office waste management, as well as regulated use of working platforms and info-communication devices. All this can come to realisation if the organisation has coordinated data security and privacy strategy, enabling it to implement changes in regulations and improvements in organisational and process-related context.

Deák makes a difference in her paper between techniques based on informatics toolset and human suggestibility.[14] This research points out that the first pillar of building up defence is mapping the current situation, having vulnerabilities in focus, since for the introduction of any precautionary measure, the areas exposed to threats need to be defined. As a next step, applied processes should be continuously reviewed and revised, followed by the mapping of vulnerabilities caused by human risk factors with vulnerability analysis or break-in test. According to the experiment conducted during this research, differences were found between security awareness level of university students depending on the course type (full-time or correspondence, in favour of the latter). Finally, it is concluded that knowing the attack methods, leakage and unauthorised use of information can be significantly reduced, and in the meantime, the security of personae of society and economy, as well as the stability of the operation of state organisations, can be enhanced.

3.2. The role of artificial intelligence (AI) and related ethics

Expansive spread of AI has generated not only serious security issues but significant ethical questions as well, since it became an inseparable part of our everyday life recently. Since control and even the decision right is given over to AI in a growing number of problems, it is exceedingly urged to build in safeguard elements which can assure that AI do not put human life at risk. Accordingly, ethical questions with military relevance should be also investigated related to AI, which is also confirmed by the fact that in 2019, AI ethics were discussed more than in the previous years together. Dozens of organisations prepared AI ethical directives and there is no AI conference lacking ethics in the program besides programming issues.

[13] Kevin D. Mitnick and W. L. Simon, *The Art of Deception. Controlling the Human Element of Security* (Indianapolis: Wiley Publishing Inc., 2002).

[14] Veronika Deák, 'Biztonságtudatosság az információs környezetben,' Katonai *Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

So far, at least the following questions emerged connected to AI:

- What AI decisions can be considered equitable?
- How can private life be protected?
- How does AI avoid gender or any other kind of bias in the moments of decision?
- How will AI take into consideration the diversity of different people's values?
- If AI needs that quantity of data, how can individual rights be protected?
- How can media be trusted in the mirror of algorithmically produced and distributed disinformation?

The importance of AI is shown clearly by the decisions made at top governmental levels. In the USA, the White House published ten principles for State Agencies,[15] which they are enforced to comply with when making suggestions for AI-related decrees valid for private sector. Complying with the White House principles, the U.S. Department of Defense published a document emphasising AI ethics in the context of military applications, entitled *Summary of the 2018 Department Of Defense Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity,*[16] a certain part of which is exclusively dedicated to the connections between AI and ethical issues.[17]

According to this document, each scholar and engineer must have at all times envisaged the ethical questions of their occupation. When it comes to AI development, these questions become significantly sharper. For instance, the next general questions can emerge:

- Would the success of AI mean the end of human race?
- Can people lose their job?
- Will people dispose of too much (or too little) freedom/independence?
- The application of AI systems also generates the questions of impeachment (possibly challenging responsibilities).
- Could people lose some of their individual rights?

Since critical (information) infrastructures also use AI to a growing extent, investigation and research of ethical questions became obligatory for today, instead of remaining optional.

3.3. Connections between social engineering and AI

Human risk factors are highly influenced by current technology trends, both from the aspect that vulnerability surface grows by an exponential pace, and regarding that most of novelties aim to favour user-friendliness, thus increasing popularity and the

[15] Viktor Justin, 'Az USA kiadta a mesterséges intelligencia tízparancsolatát,' Rakéta, 29. 01. 2020. Available: https://raketa.hu/az-usa-kiadta-a-mesterseges-intelligencia-tizparancsolatat (15. 02. 2020).

[16] *Summary of the 2018 National Defense Strategy of the United States of America.* Available: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (15. 02. 2020.)

[17] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy.* Available: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (15. 02. 2020.)

pace of spreading. We can take authentication as an example, since it is a crucial point in every technology solution linking the user with the network, the physical layers of cyberspace with the virtual ones;[18] it serves as a proof for improving user-friendliness and reliability.

Biometrics and AI-supported solutions have become more and more popular in the last few years, and while biometrics-based solutions on their own lack reliability at various crucial points, AI aims to enhance stability and reliability thanks to deep learning and so on. For example, dirt, noise, damage, lack of (back)light or radio waves can easily modify the result of biometrical authentication by having an impact on the technology. Users can be easily mistaken by voice identification solutions if the user is drunk or stressed, has a respiratory disease, or speaks a rare dialect of the default language.[19]

Taking into consideration the variety of challenges that motivate research on the future of information security, technologies supported by AI are definitely to be considered as major challenges. By the time AI is discussed, it is necessary to emphasise that many trending technologies deriving from AI work already in a mutually dependent way, such as machine learning, deep learning, robotics, cloud computing, IoT, virtual reality and augmented reality – moreover, all share the attribution of being based on virtual networks,[20] out of which the social component of the cyber-persona layer of cyberspace is built up.

AI can be applied on a vast scale that proceeds from wearable through portable devices and autonomous vehicles to intelligent network of buildings and further. Current military researchers combine VR and AI to support the training of soldiers, giving this way continuous and accurate feedback on their development, making personalised recommendations of training details.[21] On the other end of the scale, China succeeds in developing and implementing an observation and intelligence system throughout the entire country, affecting all citizens, depending significantly on face-recognition solutions supported by a virtual network-based AI software.[22] AI technology eliminates uncertainty, self-ameliorating its developers continuously – according to the pattern of deep learning functions.

If we agree in that AI aims in the first place to avoid technical issues, social issues should not be ignored, either. Professional systems and networks like that can be applied in favour of criminal intentions impacting groups of individuals, or even an entire society. Moreover, the amount of data and information collected and stored need a high protection level to avoid breaches and the derivatives of the previous aspect.

[18] Haig, *Információs műveletek*.

[19] 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.)

[20] Imre Négyesi, 'A mesterséges intelligencia és a hadsereg 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.)

[21] 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.)

[22] 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.

In addition, deep learning and deepfake solutions are capable of imitating a leader via telephone, to mislead the attacked employee to transfer money to a dedicated account[23] – practically stealing from the company.

Also making a bridge between data privacy and legal concerns, social engineering and related security unawareness supported by a social media hype and artificial intelligence used to counterfeit data, FaceApp generated issues lately in summer 2019. Being a mobile app, it comes with AI-driven filters that turn the profile photo of the user into other states (according to the dimensions of age, gender, outlook, hairiness and so on). It analyses the determinative characteristics and dimensions of the face, that is, all crucial data necessary for a biometric authentication process. The legal aspect appears when the user accepts terms and conditions and allows the owners to use that data for any unspecified further reason.

4. Critical (information) infrastructures

In this chapter, the authors give an overview of the legal aspects and regulation directions of the protection of critical infrastructure, with a special attention to information elements related. Attacks related to cyber terrorism are also in focus.

4.1. Legal regulation of critical infrastructures in Hungary

It is paragraph 1, point f) of Act CLXVI of 2012 that defines critical infrastructures as an element of a device, establishment or system, described as belonging to a classified economic sector, which is inevitable in supplying vital social responsibilities – especially healthcare, personal and wealth protection of inhabitants, guarantee of economic and social public services – and the interruption of which would cause significant consequences due to the lack of continuity in fulfilling these responsibilities.[24]

Both critical infrastructure management and cyber security related professional areas look back to a history of only a few decades.[25] Here one can see the complexity of the protection measures of critical infrastructures, and in parallel, the relevant research potential. By definition, which was made in 2012 in Hungarian law concerning critical infrastructures, they need deep understanding and professional approach, because of the interdependence between particular areas, which means that it is uninterpretable to protect one vital system element on its own. The protection will cover other elements, systems, establishments, or even entire infrastructures. For instance, the interruption of oil and energy infrastructure would immediately impact all subsystems of the transportation infrastructure, and it would also indirectly affect food supply and the continuity of further public services.

[23] 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.)

[24] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.*

[25] Kovács, *A kibertér védelme*.

With regard to the above mentioned facts, in accordance with the EU regulations, it gains importance to define critical infrastructure in European sense as follows: a vital system element determined by law, the interruption of which would significantly impact – including consideration of effects due to the interdependence of economic sectors – at least two EEA Member States.

4.2. Information infrastructures

When defining an infrastructure or system element as critical, it is important to perform a full contextual analysis, which does not always happen in practice. Observing the interdependence of any economic sector, information transfer and communication will be constantly necessary. It is true for production as well as planning, finances, transport coordination, energy supply, public services, defence and so on.

It is only paragraph 1, point 3) of the Hungarian Government Decree 65/2013 upon the execution of Act CLXVI of 2012 that defines in addition the term 'critical information infrastructure' as follows: network-based, physical and virtual systems, devices and methodologies of society, that are either already vital system elements themselves regarding the necessity of continuous supply of information and the business continuity of information conditions, or are inevitable for the operation of other identified vital system elements.[26]

Regarding the issues of current regulations, we should clearly see that it is a great achievement to have laws and decrees finalised that deal with critical infrastructures. It needs to be emphasised, however, that regulations should follow dynamically changing and developing technical background circumstances and adapt to it.[27] In order to realise such a regulation system approach, a flexible institutional structure and logic process mapping helps judicial level to achieve conceptual reasoning.

4.3. Cyber context of critical infrastructures

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 countermeasures in order to reduce and eliminate consequences.[28]

[26] *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.*

[27] Kristóf Kralovánszky, 'A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész),' *Nemzetbiztonsági Szemle (Online)* 7, no 3 (2019), 40–57.

[28] Zsolt Haig and László Kovács, *Kritikus infrastruktúrák és kritikus információs infrastruktúrák* (Budapest: Nemzeti Közszolgálati Egyetem, 2012).

Cyberattacks against critical infrastructures – as mentioned already in Chapter 2.3 – originally do not have economic intentions, but cause well perceivable problems or interruptions. Carrying out a successful attack can either block substantial supply of society or generate instability if not managed or eliminated properly. Regarding that information terrorism disposes of a different toolset than conventional terrorism, and an extraordinary experience level and wide professional knowledge, it is of highest importance that the same is necessary on the side of defence and countermeasures. Suitable reactions are of vital importance.

According to Kralovánszky, in most of those cases the attacker or the members of the attacker group remain unknown, and their characteristics anticipate that the executors are related to state background, such as the lack of profit-related motivation despite the vast financial resources needed to carry out the attack, the uniqueness of the used programs and devices, and the long preparation of the operation, supported by secret service tools.[29]

5. Information security risk management at critical infrastructures

In this chapter, the authors cite standardisation principles concerning information security and collect 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. Standardisation of security risk management

For the unification of information security measures, a possible way is to implement a standardised and certified information security management system (further referred to as ISMS). Standard family ISO 27000 sets the fundaments, according to which the operation of an ISMS serves the organisation by ensuring an appropriate security level. Beyond defining basic principles, it gives directions for certified companies concerning management of certain fields. According to recent summary data, Hungary is the 17th out of 170 countries in having obtained the most ISO IEC 27001 certifications in number as of December 31, 2018.[30]

After deep consultation with experts from two companies running certified ISMS (without naming the companies, which themselves are not operating critical infrastructures but strongly connected to the sectors of *energy* and *public service supply*) and gaining insight to the regulatory documents, we present below the most important pillars to construct an effective ISMS, based on an effectively operating risk management system.[31]

[29] Kralovánszky, 'A villamosenergia-rendszer,' 53, note 27.

[30] Laurent Charlet, 'Certification & Conformity – The ISO Survey 2018,' *ISO*. Available: www.iso.org/the-iso-survey.html (21. 04. 2020.)

[31] Lajos Muha and Tamás Szádeczky, *Irányítási rendszerek* (Budapest: Nemzeti Közszolgálati Egyetem, 2014).

The concept of information security must be clearly seen and kept in mind, which is summarised in the so-called CIA triad meaning the effectuation of *confidentiality, integrity, and availability* together and under all circumstances according to the following reasoning:

a) Confidentiality = only the authorised personae can access the particular pieces of data or information in the manner prescribed;
b) Integrity = the data or information is genuinely authentic and undeniable, while also no changes are performed;
c) Availability = thanks to the continuous and reliable operation, the data and information can be accessed by the authorised personae at any time.

Risks should be identified, assessed, analysed, managed, monitored and reviewed according to the PDCA cycle used widely in all management system related standards. Physical and information technology risks should not be separated.

5.2. Leadership engagement

Security – parallel to several other fields pointed out – should be managed by top-level within an organisation, just as we see that sanctioning and regulation measures can also be implemented by management. According to Clause 5 of the High-Level Structure of most of ISO standards, appearing also in ISO 27001: 'Top management and line managers with relevant roles in the organization must demonstrate genuine effort to engage people in the support of the ISMS.'[32] Covering inclusively all security areas, the most important problem to be solved is not whether the leadership commitment must be transparent or not, but how it can be demonstrated.

Employee awareness originates in and is highly based on the awareness level of the management. Therefore, development training programs aiming at these goals should be extended for the entire organisation in terms of personal counselling and consulting.[33] The focus of top management development in critical infrastructure would optimally be on risks translated transparently to cash, the commitment towards clients and handling their data, the impact on shareholder value, and communication guidelines to confirm own ability of coping with a critically special situation. 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 can be mitigated to a high extent.

[32] '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.)

[33] Balázs Kárász, 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata,' *Biztonságtudományi Szemle* 2, no 2 (2020), 57–68.

5.3. Application of (key) indicators

Process review, identification of vulnerabilities and the effectiveness of security awareness development all can be facilitated by applying risk indicators. Key risk indicators and related indices are widely useful in everyday corporate practice, both from the economic and engineering perspectives.[34] Risk management process takes much advantage of simple indicators and complex indices derived from them, based on correlation or weighting. Correlations and weights can be exactly recognised after thorough analysis of the operation of the organisation. A wide variety of Key Performance Indicators (further referred to as KPI) can be designed and applied in order to help organisations come to more sophisticated and well-grounded conclusions.

Information security management functions, themselves within the context of the operation of financial companies, can also be interpreted as KPIs. Currently, corporate processes are substantially determined by confidentiality, integrity and availability of information.[35] It is desired to perform longitudinal analysis when using KPIs to measure information security aspects.

5.4. Human risk factors management

ISMSs at critical infrastructures need to be controlled by a management policy worked out in accordance with human nature. However, most systems are relying exclusively on solving technical issues, which will automate security. Human risk factors are either considered unmanageable or marginal, which is a wrong approach, since trivial tasks can be technologically addressed, leaving more demanding tasks to people. Nonetheless, the interaction between people and technology itself is the biggest security risk of all.[36]

To improve the reliability and functionality of ISMSs, a deeper consideration of the role and dynamics of human risk factors is vital. When discussing their dynamics, we mean understanding the causal structure of the problems and developing more successful policies. Concerning physical security, it is more obvious to see the risk mitigation in access/entrance control systems or background check of new colleagues before admission to sensitive jobs and so on. The latter represents the bridge built between purely physical security and human security with secondary attributes checked, which process appears in the digital context, too.[37]

Both physical and human security must be controlled by the top management, with contribution of to Human Resources, Learning & Development and Security Departments. Professional services of development share the following three

[34] Csaba Kollár, 'Mutatószámok a szervezetek életében, különösen az információbiztonság területén,' in *Digitális környezetünk fenyegetettsége a mindennapokban*, ed. by B. Bencsik and I. Sabjanics. (Budapest: Dialóg Campus, 2018), 111–125.

[35] D. Krjukovs and R. Strauss, 'Information Security Governance as Key Performance Indicator for Financial Institutions,' *Rigas Tehniskas Universitates Zinatniskie Raksti: Datorzinatne* 38, no 5 (2009), 161–167.

[36] J. J. Gonzalez and A. Sawicka, 'A Framework for Human Factors in Information Security,' WSEAS International Conference on Information Security, Rio de Janeiro, 2002. Available: http://www.wseas.us/e-library/conferences/brazil2002/papers/448-187.pdf (12. 10. 2020.)

[37] Kárász, 'Social aspects.'

components: self-knowledge and soft skills, professional skills, teamwork. For example, a training program would traditionally consist of the following parts in the following order: theory, examples, conclusion, application. Optimally, it would be improved to the following: case studies and simulated situations, theory deduction, application, action plan. This way, the organisation wins an attitude in its colleagues which brings forward motivation and effectiveness, supporting purposes of the organisation by three steps of theory deduction method, cyclical problem management process and organisational culture renewal. Moreover, as a result of risks being assessed in a way that they make up value-added information, decision making processes can be optimised and be much more effective, therefore the return on investment in training programs[38] can be measured more precisely; besides that, its value will also highly probably increase.

In all the above-mentioned facts, it needs to be taken as a fundament 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.

6. Conclusion and summary

This research collected the most recent international scholarly concepts as well as judicial regulations concerning the role of human risk factors in information security in the context of protecting critical infrastructure. The implementation of artificial intelligence – having a significant impact on human behavior beyond technical issues – generates security issues in the entire society, thus it has been highlighted with special regard to critical information infrastructure.

The research also successfully outlined possible risk management methods to improve organisational security awareness, and the results are a useful basis for continuing research in the topic of leadership responsibilities, also suggested to be considered in military engineering context.

References

Deák, Veronika: 'Biztonságtudatosság az információs környezetben,' *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle* 15, no 3 (2017), 59–76.

Haig, Zsolt – Kovács, László – Ványa, László – Vass, Sándor: *Elektronikai hadviselés*. Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Haig, Zsolt – Kovács, László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem, 2012.

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

Kárász, Balázs: 'Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata.' *Biztonságtudományi Szemle* 2, no 2 (2020), 57–68.

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

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

Kárász, Balázs: 'Social aspects of reliability and security issues of authentication solutions.' Prospective appearance: *Hadtudományi Szemle* 13, no 2 (2020).

Kollár, Csaba: 'Mutatószámok a szervezetek életében, különösen az információbiztonság területén.' In *Digitális környezetünk fenyegetettsége a mindennapokban*, ed. by Bencsik, B. – Sabjanics, I. Budapest, Dialóg Campus, 2018. 111–125.

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.

Kralovánszky, Kristóf. 'A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész).' *Nemzetbiztonsági Szemle (Online)* 7, no 3 (2019), 40–57. DOI: https://doi.org/10.32561/nsz.2019.3.4

Krjukovs, D. – Strauss, R.: 'Information Security Governance as Key Performance Indicator for Financial Institutions.' *Rigas Tehniskas Universitates Zinatniskie Raksti: Datorzinatne* 38, no 5 (2009), 161–167. DOI: https://doi.org/10.2478/v10143-009-0014-x

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

Mitnick, Kevin D. – Simon, W. L.: *The Art of Deception. Controlling the Human Element of Security.* Indianapolis: Wiley Publishing Inc., 2002.

Muha, Lajos – Szádeczky, Tamás: *Irányítási rendszerek.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Négyesi, Imre: 'A mesterséges intelligencia és a hadsereg 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

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.)

Gonzalez, J. J. – Sawicka, A.: 'A Framework for Human Factors in Information Security.' WSEAS International Conference on Information Security, Rio de Janeiro, 2002. Available: www.wseas.us/e-library/conferences/brazil2002/papers/448-187.pdf (12. 10. 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.)

Justin, Viktor: 'Az USA kiadta a mesterséges intelligencia tízparancsolatát,' Rakéta, 29. 01. 2020. Available: https://raketa.hu/az-usa-kiadta-a-mesterseges-intelligencia-tizparancsolatat (15. 02. 2020)

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

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.)

Tóth, Gergely: 'Leendő honvédelmi miniszter: A honvédséget az alapoktól kell újraépíteni.' *Index.hu,* 14. 05. 2018. Available: https://index.hu/belfold/2018/05/14/benko_tibor_honvedelmi_miniszter_meghallgatas_orszaggyules_bizottsag/ (27. 04. 2020.)

Summary of the 2018 National Defense Strategy of the United States of America. Available: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (15. 02. 2020.)

Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Available: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (15. 02. 2020.)

Charlet, Laurent: 'Certification & Conformity – The ISO Survey 2018.' *ISO*. Available: www.iso.org/the-iso-survey.html (21. 04. 2020.)