

Diverse approach of Cybersecurity culture in Education

Judit Módné Takács
Alba Regia Technical Faculty
Obuda University
Szekesfehervar, Hungary
modne.t.judit@amk.uni-obuda.hu

Monika Pogatsnik
Alba Regia Technical Faculty
Obuda University
Szekesfehervar, Hungary
pogatsnik.monika@amk.uni-obuda.hu

Nikoletta Tolner
Alba Regia Technical Faculty
Obuda University
Szekesfehervar, Hungary
tolner.nikoletta@amk.uni-obuda.hu

Abstract— Cyberspace has become a required living space in modern society in the 21st century. Technological developments at the global level increase social vulnerability. Human is a critical element in creating security. Creating complete safety is an impossible mission, so the emphasis should be on resilience and prevention. There is an increased need for safety awareness and training development, which should be extended to all relevant participants to increase resilience. In this process, education could be effectively involved and provide long-term problem-solving. For Z and Alpha generation young people, cyberspace is their natural medium. However, it is far from comfortable living space for the generation that prepares, mentors, and educates them. Without the development of a proper cybersecurity culture, all participants are exposed to dangers, which could only be promoted through cooperation and proper cyber hygiene. The perpetual cyber threat that affects our everyday lives has also rewritten the expectations of the necessary competencies, skills, and abilities in recent years. There is a growing demand for security professionals in this rapidly evolving digital world. Education, on the other hand, cannot support this need, so it needs complete reform. IT education does not adequately support the development of digital and STEM competencies. The issue of safe living needs to be addressed regardless of gender, ethnicity, profession, or education. Thus, education requires special attention, including effective teaching methods that can adapt to the needs of the generation and the effective development of cyber defence and cyber-attack prevention capabilities.

Keywords— *cybersecurity, education, security culture, cybersecurity professions.*

I. MAIN AREAS OF CYBERSECURITY, PAST AND PRESENT IN EDUCATION

Cyber security, cyberspace or even cyberculture has been a part of our lives for a very long time. These concepts involved are often unclear, closely related, but still difficult to define. Because the daily life of a 21st-century person is already taking place in cyberspace, social life and business relations push traditional communication channels into the background. There are several reasons for this progress, cost-effectiveness, changed habits, generational differences, and rapid technological development. The further training of our digital society from a cyber security and material point of view has become critical, an integral part of which is the cyber hygiene capability of those involved and its development. [1] In this way, education is a priority for national security and business economics.

The European Parliament's proposal for a resolution on cyber defence (2018/2004 (INI)) [2] draws attention to similar issues. The motion highlights that “*resilient cyberspace requires impeccable cyber hygiene*” and emphasizes that a 21st-century cyber defence education and training system would significantly reduce threats.

The European Network and Information Security Agency identify five main areas that define cyber security: security and protection of the communication system, operational security, safety of stored and transmitted data and information, physical security of the system, protection against cyber threats. [3]

II. KEY CONCEPTS

The list of concepts related to the topic is very diverse and long. Consider some relevant, clearer terms in cybersecurity.

A. Cybersecurity

The National Cybersecurity Strategy [4] defines the cybersecurity concept and its relationship with education in Hungary in 2013 as follows: “*Cybersecurity is the continuous and planned use of political, legal, economic, educational and awareness-raising and technical tools to address risks in cyberspace, transforming cyberspace into a reliable environment for the smooth functioning and operation of social and economic processes, ensuring an acceptable risks level in cyberspace.*” Examining the educational side, they want to achieve the field of cyber security by integrating IT into education.

In 2020, Magyar Közlöny (Hungarian Gazette) published the renewed National Security Strategy. This paper outlines the concept of security in a much more complex way, including cyber security. An important fact appears in this document, the higher education and information technology sector's key role. There are no specific points of contact with education, only the formation and development of citizens' sense of responsibility and security-minded thinking as a strategic interest appears as a strategic goal. [5]

B. Cyber resilience

Cyber resilience is the ability to continuously achieve the desired result, despite the unfavourable cyber events surrounding it, to achieve an adequate level of security for the organization and individual. The main difference between cybersecurity and cyber resilience is alternately a difference

in approach. *"Resilience is built into organizations and IT systems, rather than added as separate functions."* [6]

"Cyber resilience is the most important feature of any cyber system, especially during the transition to the sixth technological stage and related Industry 4.0 technologies." [7]

Because cyberattacks are a very serious threat worldwide. Besides, preventing cyber-attacks, organizations focus on an immediate and consistent cyber-attack response (they can minimize disruptive effects on operations). This capability can be called cyber-resilience. [8]

C. Cyber hygiene and Cyber security culture

There are also several definitions on the Internet to define this concept, but there is no clear definition. Maennel et al [9] attempted to gather definitions of Cyber Hygiene by researching the scientific literature. Finally, the authors of this article suggest a definition of cyber hygiene: *"Cyber hygiene is a set of practices aimed at protecting from negative impact to the assets from cyber security-related risks."* So cyber hygiene exists in different forms. It is understood from the creation, control, and maintenance of the online security of individuals and organizations, considering their risk assessments and the technologies they use.

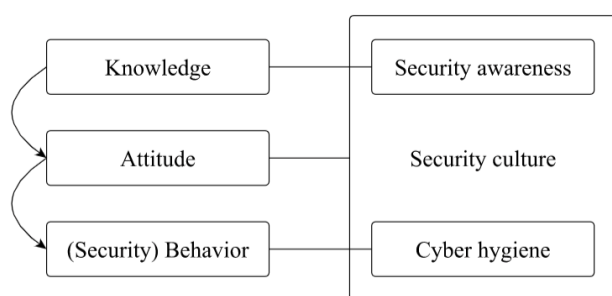


Fig. 1. Cyberhygiene and related terms [9]

Others see cyber hygiene to encourage users to have a safe online presence. The presence of cyber hygiene persuades individuals to follow processes to protect themselves and others. From this perspective, the focus is on user awareness and training. [10]

In another view, *"Cyber hygiene is the establishment and maintenance of an individual's online safety. It is the online analogue of personal hygiene and encapsulates the daily routines, occasional checks and general behaviours required to maintain a user's online "health".* " [11]

Overall, therefore, cybersecurity culture includes cybersecurity awareness, safe behaviour, and cyber hygiene. [9]

III. CYBER SECURITY EDUCATION IN THE 21ST CENTURY, TAKING INTO ACCOUNT Z GENERATIONAL SPECIFICITIES

A. Cyber security education in Hungary

Nowadays - the epidemic situation has also contributed to this - we live a big slice of our lives in cyberspace. We work online, study, bank, buy, do business. There are daily attacks in this space, whether against individuals or larger groups, states. For our security, it is important to keep up with cybercriminals and prepare for and even prevent attacks.

However, this requires properly trained professionals and increased security awareness for all participants in cyberspace. Security itself is part of digital competencies, but its weight has appreciated over the past year and a half. Based on the European Union Reference Framework (2006), 8 key competencies have been identified, one of them is digital competence.

According to Ferrari [12], "digital literacy can be broadly described as the confident, critical, and creative use of ICT (information and communication technologies) to achieve goals in the areas of work, employment, learning, leisure, social inclusion and/or participation. Digital literacy is a transversal key competence which as such enables the acquisition of other key competences (e.g., language, mathematics, learning to learn, cultural awareness). "According to Yuhyun Park [13], there are 7 important basic digital skills:

1. digital literacy,
2. digital communication,
3. digital emotional maturity and intelligence,
4. digital security,
5. knowledge of digital rights,
6. our digital "individuality"
7. digital use ("use" includes digital healthcare, community activity and other off-screen activities).

Demand for IT professionals, including cybersecurity professionals, has doubled in the last 5 years. [14,15,16] NET Internetkutató és Tanácsadó Kft has prepared a comprehensive labour market survey on behalf of the Ministry of Innovation and Technology, IVSZ and the Government Informatics Development Agency. The research carried out under the Economic Development and Innovation Operational Program (Ginop) surveyed 3,140 companies, 2,159 IT professionals, 1,785 high school and 2,170 drop-out students, and analysed almost 11,000 job advertisements. Research shows that the demand for IT professionals will exceed the number of professionals issued by educational institutions for years to come. In our rapidly changing world, the development of information technology is constantly rewriting needs, and educational institutions are unable to respond immediately to these rapidly changing needs. In the following, we will look at the trainings in the field of information security and cyber security in Hungarian higher education (Source <https://www.felvi.hu>, and the websites of the universities, <http://uni-obuda.hu/>; <https://www.uni-nke.hu/>; <https://www.elte.hu/>; <https://gdf.hu/>).

NATIONAL UNIVERSITY OF PUBLIC SERVICE Faculty of Military Science and Military Training

- Basic training course in military infocommunication: The aim of the training is to train military info-communication specialists.
- Undergraduate course in International Security and Defence Policy: The training is mainly in the fields of national defence, military, and security. During the training, students will learn how to analyse and evaluate professional problems in security policy and defence issues, and how to create organizational conditions.
- Undergraduate course in national security for those belonging to the personnel of the Military National Security Service or the reconnaissance professional officers of the Hungarian Armed Forces, as well as

the personnel of the special operational forces and the professional organizations cooperating with them. The aim of the training is to train national security experts for special-purpose national security services, as well as other clients, who can effectively fulfil the requirements and tasks of their jobs in the organizations of the national security field using their up-to-date theoretical and practical knowledge.

- Master's Degree Program in Défense Infocommunication Systems Design: The aim is to train professional and civilian professionals who are suitable for the Hungarian Armed Forces, law enforcement agencies, national security services, defence administration, and the wider defence sphere - especially those cooperating with NATO systems, the secure operation of its infocommunication systems, including the design, organization, management, supervision and control, and the provision of conditions for cooperation between such systems.
- Master's Degree Program in International Security and Défense Policy: The aim of the course is to train professionals who are able to work in the activities and international relations of the defence administration system, especially NATO, the EU, the UN and the OSCE, as well as countries and partners with Hungary.
- Master's degree program in National Security: Graduates are trained to prepare current security and defence policy and special strategic analysis, to assess security and crisis situations, and to professionally apply the human resources, special tools and methods required for effective professional activity.

NATIONAL UNIVERSITY OF PUBLIC SERVICE Faculty of Law Enforcement

- Crime-Cyber Investigation Specialization: During the training, students get to know the basics of the operation of information systems, the IT, special legal, forensic, and criminal service knowledge necessary for the detection and proof of cybercrime.
- Master's degree in security management: the aim of the training is to train security managers who, in cooperation with state and municipal law enforcement, security and security management professionals, can develop and operate integrated (physical and information) security systems for private entities and public institutions. fully manage the area within an organization or as an external service provider.
- Civil Master's Degree Program in Civil Security: the aim of the training is to train national security professionals who are suitable to perform managerial and expert tasks in the administrative, military, law enforcement, scientific sectors, and to assess, analyse and solve national security problems based on their professional knowledge and practical skills.

NATIONAL UNIVERSITY OF PUBLIC SERVICE Faculty of Political Science and International Studies

- Master's Degree Program in Cyber Security: The program is primarily aimed at training professionals in the public service who are responsible for cyber security and who plan to work in the field of international relations, information security of state and municipal organizations, and protection of critical IT systems. In addition to these, of course, students are also prepared for market challenges. After acquiring the basic legal and IT knowledge in the field, students get acquainted with the basics of security organization, risk assessment and physical protection, and the basics of information security.
- Further training in electronic information security management: The main goal of the training is to transfer the professional competencies necessary for the performance of the tasks of the persons responsible for the security of the electronic information system defined in Act L of 2013 on electronic information security of state and local government bodies and to develop a security-conscious approach.

UNIVERSITY OF ÓBUDA Donát Bánki Faculty of Mechanical and Safety Engineering

- Bachelor's degree in safety engineering: The aim of the training is to train safety engineers who are suitable for the operation and maintenance of the equipment of safety systems, the introduction and application of related new technologies.
- Master's Degree Program in Security Engineering: The aim of the training is to train security engineers who, can design, organize, operate, perform maintenance tasks, through their acquired high-level technical, IT and organizational knowledge, as well as the related skills.
- Specialized in-service training: A form of training based on a bachelor's and master's degree (or a college or university degree under the previous system) that provides training for specific tasks without changing the level of the degree.
- Information Security Engineer / Specialist: the aim of the training is to provide interdependent, up-to-date professional knowledge and marketable knowledge to professionals working in jobs related to information security.

UNIVERSITY OF ÓBUDA János Neumann Faculty of Informatics

- Cyber Security Engineer / Specialist: The curriculum includes modern IT security procedures and their application possibilities; IT security risk analysis; general characteristics of threats in cyberspace; methods and tools for detecting and neutralizing IT incidents; methods and possibilities of IT security modelling and complex examination; aspects and possibilities of cyber defence; etc.

GÁBOR DÉNES COLLEGE

- Data protection and information security manager: During the training, students acquire the knowledge elements necessary for the management of the data protection and information security monitoring system supporting corporate economic security.

EÖTVÖS LORÁND UNIVERSITY Faculty of Law

- Data security and data protection lawyer: the aim of the training is to prepare lawyers in the field of data security, data protection, freedom of information and legal data management, private data management, building on the practice of NAIH, and the proper conduct of litigation and non-litigation.
- Data Security and Data Protection Law Specialist: the aim of the training is to prepare holders of a degree entitling them to internal data protection responsibility activities, based on the practice of NAIH, to recognize and manage legal problems in the field of data security, data protection, freedom of information and public and private data management.

B. Z generational specificities

After a more thorough study of the training topics, we can see that these trainings do not affect every single area of information security and cyber security. The core business of the school largely determines which segment of cybersecurity is given priority during training. Somewhere the study and knowledge of the legal background is important, elsewhere the IT background is stronger. It would be very important to make this area attractive to applicants. The age of those entering education also greatly influences who chooses this field. Generational differences, different basic skills influence the choice.

For the purposes of this paper, we will focus only on Generation Z [17]. This is the age group most represented in university education today. There are several definitions of generational boundaries. According to Pais [18] members of Generation Z were born between 1996 and 2009. This generation is characterized by the author as follows: “They live their lives connected to the Internet, sort of wired”. Their excellent intellect and highly advanced problem-solving ability are associated with an excellent technical sense that generates a strong practical need.” Tari [19] classifies young people born between 1995 and 2009 into Generation Z. McCrindle (2014) [20] considers the age group born after 2000 to be Generation Z. This generation is also called “digital natives”. They do not know life without the World Wide Web. For them, using a computer, a smartphone, the World Wide Web is a completely natural thing. This generation poses new challenges to educators because they are unwilling to accept traditional methods, they want to acquire knowledge in interactive, interesting lessons. Members of the generation use technical innovations with ease, but their safety awareness is inadequate. They are not fully aware of the dangers in cyberspace. Coercive measures caused by the COVID epidemic included the implementation of education online. The transition from attendance education to online education had to be resolved so quickly that the issue of security was not much addressed. Young people who had previously used the online space for other purposes were suddenly forced to live in this space almost their entire lives. There are many sources of danger in cyberspace that most young people find difficult or unnoticed. It would be important for safety awareness to appear in education and have a much greater weight. According to a survey, 60% of 8–12-year-olds were exposed to some form of cyber risk during online education [21]. More than 84% of school-age children were involved in online education worldwide. These children and their parents, as well as the teachers who teach them, also need to develop their

digital competencies. There are aspirations and regulations for these at the international level.

IV. NEEDED COMPETENCIES AND SKILLS FOR A CYBERSECURITY SPECIALIST

A. Security awareness in the light of digital competencies

The Comprehensive Framework for the Assessment of ICT Competences [22] defines five main areas of competence:

1. Accessing, evaluating, and managing information and data
2. Sharing information and communicating
3. Transforming and creating information and digital content
4. Problem-solving in a digital context and computational thinking
5. Appropriate use of ICT (online security, safety and risk awareness and skills)

Online security competencies include the appropriate use of ICT in multiple environments and platforms. With increased information sharing, students need to be aware of how to handle and protect personal information. Basic security knowledge includes the use of strong passwords, anti-virus measures, and the protection of personal information.

Decision-makers' interest in assessing students' ICT-related safety and security competencies is reflected in the widespread inclusion of such competencies in school curricula in education systems. As the use of ICT in the classroom and beyond becomes more common, a wide range of issues related to online safety are being included in school curricula. These online security topics include safe online behaviour, privacy, cyberbullying, downloading, copyright, safe use of cell phones, and contact with strangers. It is becoming increasingly important to integrate online security practices into ICT education, in addition to understanding existing knowledge of security and safety issues related to ICT access and use [24], [25].

Among the competencies, stress tolerance and resilience appear little in the literature as important elements. Stress tolerance is much needed because of the ability to respond appropriately in an emergency cybersecurity situation. Resilience is the ability to adapt to changing situations, which is important for proper adaptation to security situations.

B. Needed skills for a cybersecurity specialist

Based on the description of the Cyber Security Guide [23], the following are typical for a cybersecurity professional. A cybersecurity professional takes care of the security of the company and its employees in cyberspace. They ensure continuous monitoring of systems, secure operation, and protection against attacks by software and hardware devices. They are also responsible for training and educating employees, passing on their experience and strengthening safety awareness. They design and implement firewalls and security systems by the latest security standards. “People in this role are often hired as much for their soft skills as their technical ability.” [23]

Needed skills include, in addition to the appropriate level of training, good communication skills, teamwork, the ability to work in an “emergency”, stress tolerance and problem-solving skills, the ability to adapt to the needs and attitudes of

employees, a kind of flexibility skills. Rapid response, analytical thinking, and continuous learning skills are essential in this field.

"In terms of skills, experience, and general mindset, a cybersecurity specialist needs to be like a Swiss Army knife of the digital world. A person in this role needs to be multi-disciplinary and adaptable to a wide variety of situations."[23]

V. SUMMARY AND FURTHER RESEARCH

Our study was prepared with the aim of assessing the literature, clarifying the most important conceptual issues and directions in the field of IT competencies, including IT security knowledge, for our empirical research.

Although IT competencies are highlighted in many documents, education at BSc, MSc and specialist training levels is provided at several universities in Hungary, but education in this important area is not yet sufficiently represented in lower and secondary institutions. In the case of the growing Z and alpha generation, the priority development of these competencies is necessary, especially regarding the development of the soft skills required for the development of a safety awareness attitude, safety culture, resilience, and cyber hygiene. In addition, in a later study, it would be worthwhile to examine the proportion of students graduating from the training places listed in the article in the field of IT security. How can I compensate for the lack of IT security specialist companies in Hungary? What methods do companies and organizations use to fill the gap?

REFERENCES

- [1] Fekete-Karydis K., Lázár B.: A kibervédelmi stratégiák fejlődése, kibervédelmi kihívások, aktualitások (2.): Az Európai Unió kiberbiztonsági szabályozása 2013-tól napjainkig (Development of cyber defense strategies, cyber defense challenges, current events (2.): European Union cyber security regulation from 2013 to the present) *Honvédségi Szemle: A Magyar Honvédség Központi 147. évfolyam: 2019/5. szám* pp. 60-72., 13 p. (2019) URL: <https://kiadvany.magvarhonvedseg.hu/index.php/honvselemle/article/view/224> (Last viewed: 2021.08.12)
- [2] Az Európai Parlament állásfoglalására irányuló indítvány a kibervédelemről (Motion for a European parliament resolution on cyber defense) (2018/2004(INI)) (2018) URL: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_HU.html (Last viewed: 2021.08.25).
- [3] Beláz A., Berzsényi D.: Kiberbiztonsági Stratégia 2.0 – A kiberbiztonság stratégiai irányításának kérdései. (Cyber Security Strategy 2.0 - Issues of Strategic Management of Cyber Security) *Elemzések. Budapest, Stratégiai Védelmi Kutatóközpont* (2017). URL: <https://bit.ly/3C2zWuS> (Last viewed: 2021.09.19)
- [4] 1139/2013. (III. 21.) Kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 5. és 10/g pont (Government Resolution on Hungary's National Cyber Security Strategy) URL: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (Last viewed: 2021.09.10)
- [5] 1163/2020. (IV.21.) Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról. (Government Decision on the National Security Strategy of Hungary.) URL: <https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/megtekintes> (Last viewed: 2021.09.19)
- [6] Björck F., Henkel M., Stirna J., Zdravkovic J.: Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353. Springer, Cham.(2015) DOI: https://doi.org/10.1007/978-3-319-16486-1_31 (Last viewed: 2021.08.27.)
- [7] Sergei P.: Cyber Resilience, *River Publishers* (2019)
- [8] Sepúlveda Estay D. A., Sahay R., Barfod M. B., Jensen C. D.: A systematic review of cyber-resilience assessment frameworks, *Computers & Security*, Volume 97, (2020), 101996, ISSN 0167-4048, DOI: <https://doi.org/10.1016/j.cose.2020.101996>, (Last viewed: 2021.08.27.)
- [9] Maennel K., Mäses S., Maennel O.: Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) *Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science*, vol 11252. Springer, Cham. (2018) DOI: https://doi.org/10.1007/978-3-030-03638-6_18, (Last viewed: 2021.08.27.)
- [10] Pfleeger L., Sasse M. A., Furnham A.: From weakest link to security hero: Transforming staff security behavior, *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, pp.489–510, (2014)
- [11] Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J.E.: Cyber hygiene: The concept, its measure, and its initial tests. *Decis. Support Syst.*, 128. (2020)
- [12] Ferrari A., 2013, Report EUR 26035 EN https://www.deaweb.hu/images/bongeszde/digcomp_teljes_hun_1512_31.pdf, (Last viewed: 2021.08.27.)
- [13] Yuhyun Park: 8 digital life skills all children need and a plan for teaching them. World Economic Forum, Global Agenda, 2016, <https://bit.ly/2Zcgbmw> (Last viewed: 2021.08.26.)
- [14] XXI. Fialat Műszaki Tudományos Ülésszaka, 2016. Kolozsvár, 313–316. <http://hdl.handle.net/10598/29092>; Security awareness in context of digital competence: Nyikes Zoltán, Óbudai Egyetem, Biztonságtudományi Doktori Iskola, (Last viewed: 2021.08.26.)
- [15] Berzsényi D.: The Human Side of Cybersecurity, *Nemzet és Biztonság* 2017/2. szám 54–67. <https://bit.ly/3aWvlyy>; (Last viewed: 2021.08.27.)
- [16] Csutak, Zs.: Kiberbiztonsági kihívások a 21. században. In: Móra Akadémia, (5). pp. 360-375. (2018); <https://bit.ly/3C250uU>; (Last viewed: 2021.08.27.)
- [17] Molnár L. – Kovácsné Havelant Kinga Digitális kompetenciák a Z-generációban; Észak-magyarországi Stratégiai Füzetek XVIII. évf. 2021 különszám, https://www.strategiaifuzetek.hu/files/216/SF-2021-k_136.pdf; (Last viewed: 2021.08.29.)
- [18] Pais E. R. (2013) Y és Z generáció mint a jövő munkavállalói. <http://docplayer.hu/2100822-Y-esz-generacio-mint-a-jovo-munkavallaloi.html>, (Last viewed: 2021.08.29.)
- [19] Tari A.: Z generáció TERICUM KÖNYVKIADÓ. ISBN:9789639633926, Nyelv:MAGYAR, Kiadás éve:2011.
- [20] The ABC of XYZ: Understanding the Global Generations, October 2018, Mark McCrindle, ISBN: 978 0 9924839 0 6
- [21] Joshua A. Jackman, Douglas A. Gentile, Nam-Joon Cho & Yuhyun: Addressing the digital skills gap for future education, Published: 11 March 2021 <https://www.nature.com/articles/s41562-021-01074-z>
- [22] OECD (2018): Pisa 2018 ICT Framework
- [23] Cybersecurity Guide: How to Become a Cybersecurity Specialist (2021). URL: <https://cybersecurityguide.org/careers/security-specialist/> (Last viewed: 2021.09.23)
- [24] Károly A., Elek R., Haidegger T., Széll K., Galambos P. (2019): Optical flow-based segmentation of moving objects for mobile robot navigation using pre-trained deep learning models. In: IEEE (szerk.) 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) Piscataway (NJ), pp. 3060-3066.
- [25] Redjimi H., Galambos P., Tar J., Széll K. (2019): The Effects of Simultaneous Noise and Missing Information in Fixed Point Iteration-based Adaptive Control. In: IEEE (szerk.) 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). Piscataway (NJ), pp. 1430-1435.