Cyber Safety in the Digital Educational Environment: External and Internal Risks

Oleksandr Burov[1], Yuliya Krylova-Grek[2(✉)], Evgeniy Lavrov[3], Olena Orliyk[4], Svitlana Lytvynova[1], and Olga Pinchuk[1]

[1] Institute of Information Technologies and Learning Tools, 9 Berlins'koho Str., Kiev 04060, Ukraine
burov.alexander@gmail.com, s.h.lytvynova@gmail.com, opinchukl00@gmail.com
[2] G.S. Kostiuk Institute of Psychologyof the National Academy of Educational Sciences, 2, Pankivska Str., Kiev 01033, Ukraine
yulgrek@gmail.com
[3] Sumy State University, Sumy, Ukraine
prof_lavrov@hotmail.com
[4] Scientific-Research Institute of Intellectual Property, Kiev, Ukraine
e.orliyk@ndiiv.org.ua

Abstract. The paper describes a novel project aimed at developing the concept and technique of cyber safety system of the education process' participants in the digital learning environment (integration of human and cyber-physical systems approach). A striking feature of the proposed approach lies in its notable difference from the one and focus on a human in the network's cybersecurity loop rather than technical aspects or human personal data. Besides, it discusses the method and way of conducting experimental studies.

Keywords: Cybersecurity · Cognitive performance · Education · Social engineering

1 Introduction

Last year, transformation in teaching and learning became an especially shared agenda among educators all over the world due to the forced and unprepared transition of education to mass digital learning with the use of network technologies [1]. It was accompanying by the unwillingness of both the education system and the state as a whole to protect subjects from information, psychological and cognitive interventions that may affect the formation of personality under such circumstances at both the substantive and personal levels [2]. New challenges of time and new directions of society development – Society 4.0, Education 4.0, penetration of the newest technologies in all spheres of life, "hybrid" war – demand to understand key problems, challenges, and questions related to the educational process security in digital learning environment (DLE), in particular, security of all direct participants, education organizers, the state as well as the security of digital educational content [3], expansion of cognitive war, whose main purpose is to alter and distort the cognitive model of life,

D. Russo et al. (Eds.): IHSI 2021, AISC 1322, pp. 364–370, 2021.
https://doi.org/10.1007/978-3-030-68017-6_54

especially of young people [4]. Accordingly, there is an urgent need to protect the cognitive, ideological, intellectual, and developmental activities of education and human capital since a human is still weakest link in the System [5].

There are new problems caused by life and activities in the securities, related factors, and ways to avoid them, as well as new tools and mechanisms. Thus, the problem of development and implementation of information and communication technologies (ICT) in education needs to be addressed [6]. However, it should be borne in mind that new information technologies lead to fundamental and global processes that transform social development. Yet, in addition to the positive impact they have, new factors and conditions naturally cause serious problems, threats and risks [7]. As noted in the materials of the World Economic Forum in Davos (2018-2020) and the United Nations Organization [8], the problem of cybersecurity (CS), which affects almost all spheres of human life and activity, is especially acute because of many reasons, but of all, in the context of full education informatization [9]. It means that a human becomes a crucial unit of the state's vital infrastructure, but it is advisable not to consider the issues of cybersecurity (of the System), but cyber safety (of a human as an element of the System).

Purpose. Development of the concept and technique of the cyber safety system of the education process' participants in the digital learning environment (integration of human and cyber-physical systems approach).

2 Methodology

Considering learning as a type of activity in human-system integration [10], present-day learner may be viewed as an operator-researcher who acts in the digital learning environment (DLE). Successful learning involves mutual adaptation between a human as a participant of the educational process (PEP) and activity tools using individual cognitive abilities in networks including social ones [11] and in changing digital environment in general [12]. On the other hand, it is possible to use ergonomics' methods and techniques to assess a learner's safety in the education process [13]. Cybersecurity issues have become a cornerstone since computer technology ceased to be the prerogative of major science centers. The advent and spread of local and global networks changed how cybersecurity, relevant trends, problems, and challenges are viewed and understood.

Networks as Active Agents of the Education Process. Over time, digital networks are becoming a focal point of our lives, and social media is turning into a new social environment. These networks pose a real threat to education and the state's security. The network components in a simplified manner can be represented as a node, interface, connection, and network [3]. The nodes are network "agents": *people* (creators of the resource and its content, resource administrators, regular or random users), *technics* (terminal stations, computers, gadgets, etc.), and *information* (databases, knowledge bases, control systems, etc.) means. Depending on their essence, the agents have their own interface and communication channels to interact with other agents that can be a target for a cyber-attack. The network acquires the features of an independent factor

that affects its properties, operation, and users, as well as the system in general. DLE is a triad-like cyberspace: (1) *information* in its digital representation: static (files recorded on media) and dynamic (packets, streams, commands, etc.); (2) *technical infrastructure* (ICT, software, databases etc.); (3) *information interaction* between subjects ("agents") via transmitted information and processing (2).

Cyberspace-Produced Threats to Participants of the Educational Process. Having in mind that today's students were born in the digital age, it can be argued that cyberspace is and will remain an extremely important part of the ideology and civilization battlefield. The range of threats from open cyberspace is constantly expanding. If a decade ago the threats for schoolchildren could be reduced to a relatively small number of groups (virus attacks, cybercrime, the dangers of Internet surfing) [14], these days the variety of hazards and threats has significantly increased and continues to grow, affecting all possible human actions online [15]. However, there has been little discussion on PEP's cognitive abilities, since most studies tend to focus on cybersecurity organizational issues [2].

It was found that the greatest threats to students are hidden active threats that can be assessed as a hierarchical set of indicators from ergonomics' standpoint: integrated (complex); three group indicators – hazard level caused by viral attacks, cybercrime and internet surfing; a set of individual indicators containing a set of certain threats [3].

Cyber Security Areas. Education is not always recognized as a critical area. However, today's students can work in areas like that in the shortest possible time mainly due the implementation of new education technologies [16] in general, including distributed [17] and adaptive ones [18], as well as augmented and virtual environment [19]. Therefore, they need protection and appropriate training. Furthermore, a neglected issue in this area is procedures of defining common possible cybersecurity target groups (for example, pupils/students, teachers, children/youth, education managers, total population of the country). Depending on the means of action, the problems (and corresponding means) of cybersecurity can be classified into five groups: legal, technical, informational, organizational, and psychological [3]. Simulation of the influence of cyber threats can be effective, if it provides the objective measurement of the individuals' reaction to this influence, i.e. psychophysiological response. We initiated the given study to model and simulate the impact of diverse factors (informational, social, psychological, cognitive, etc.) on an individual with the assessment of his state before and after. The ultimate practical goal of the study is to develop methodology to assess the impacting factors and risk-metrics, considering the individual and group features of potential objects of violence action.

3 Results and Discussion

The provisions of the project are based on the results of the authors' participation in the NATO Expert Group HFM-259 "Human Systems Integration Approach to Cyber Security" [20], previous experimental studies focused on analyzing a human cognitive work in digital space under influence of internal and external factors [21]. These results completely correspond to the present trends in cybersecurity evoked by the pandemic.

The results revealed the rapid increase in malware dissemination, ransomware/extortionware accompanied by emergence of the ransomware as a service, threat hunting as a response to malicious activity intensification in the networks, network detection and response. It was proven that attackers are constantly improving their abilities to deceive people being the biggest threat plaguing organizations in 2020 including educational institutions [22].

The focus should be shifted from personal data to PEP's state and his/her ability to resist an attack. Appropriate skills should include cybersecurity awareness, training, and cyber hygiene. The validation of results is based on:

- using metrics to measure the success of the training programs and identify the probable;
- metrics that include both short-term and long-term goals since they help to measure how participants' security posture improves over time.

Alongside evaluating the subjective response of a cyber-influenced individual, the study assesses his psychological and physiological changes including the ones caused by the latent effect on consciousness. To achieve this goal, it is planned to study the pool of volunteers and changes in their electrocardiogram and electroencephalogram due to simulated effects of both traditional gadgets (conventional devices for entering cyberspace) and individual augmented/virtual reality devices. Experimental studies imply both online and in-house observations by using the records of electrophysiological parameters, as well as virtual reality glasses and tablets. The project requires involvement of experts in various fields with strong expertise in conducting experimental research using network technologies, data analysis, as well as designing new scientific and methodological tools.

We have succeed in the following. First, we have designed a prototype (online testing software) of the cybersecurity system of PEP in DLE. Second, we have revised methods of assessing the cyber hazard impact on PEP and their risk-metrics based on indicators of psychological and physiological changes caused by cyber hazards. Then, we have developed recommendations on PEP's cybersecurity taking into account the human factor in DLE and individual/group characteristics of psychological/psychophysiological response of high school students to the cyber hazard impact. Finally, of particular interest is our proposals on the structure and scope of educational materials aimed at the formation of a general culture of cybersecurity in DLE as a component of PEP's cybersecurity system.

Our study has many effective and valuable applications in educational environment (Fig. 1).

This study is a first step towards enhancing our understanding of cyber safety in DLE.

To further our research we plan to:

- Provide methodological support for considering and mitigating the effects of hazardous factors on PEP in the digital learning environment.
- Develop a set of recommendations on cybersecurity for PEP in the digital learning environment taking into account the human-related factors.
- Explore psycholinguistic aspects of cybersecurity humanitarian component [23].

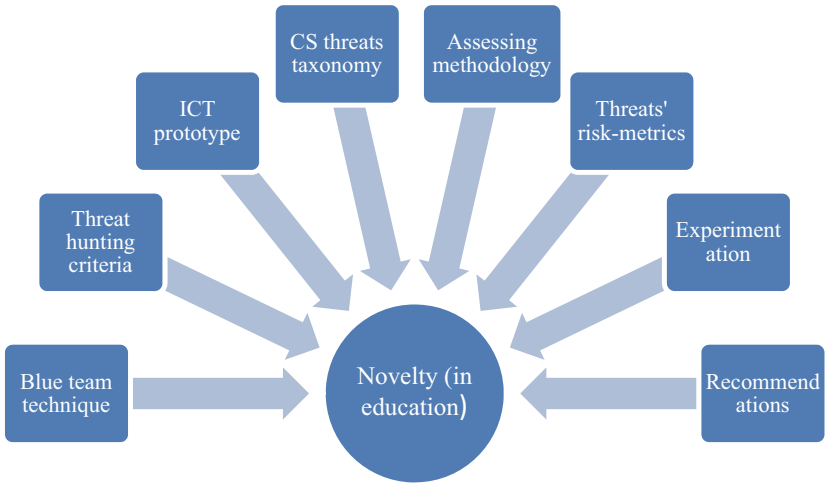

Fig. 1. Cyber safety tools for education

4 Conclusion

To sum up, our study underlined the importance of scrutinizing the present-day features of teaching and learning in contemporary digital environment. Our recommendations are a potential tool to improve the security and safety of educational process. The findings suggest the idea that the security and safety of learning is achieved by adapting students' activity, which greatly depend on his/her cognitive state in digital education, by designing intelligent individual-oriented systems and services that ameliorate human – E-technology interaction.

Acknowledgments. . This work is supported by the grant 0118U003160 "System of Computer Modeling of Cognitive Tasks for the Formation of Competencies of Students in Natural and Mathematical Subjects".

References

1. Memon, A.S., Rigole, A., Nakashian, T.V., Taulo, W.G., Chávez, C., Mizunoya, S.: COVID-19: How prepared are global education systems for future crises? Research Brief 2020-21. UNICEFInnocenti (2020). https://www.unicef-irc.org/publications/1138-covid-19-how-prepared-are-global-education-systems-for-future-crises.html
2. Coultier, R.: 10 K-12 cybersecurity must-dos. eSchoolMedia & eSchool News. Innovations in Educational Transformation (2020). https://www.eschoolnews.com/2020/06/22/10-k-12-cybersecurity-must-dos/
3. Bykov, VYu., Burov, OYu., Dementievska, N.P.: Cybersecurity in digital educational environment. Inf. Technol. Learn. Tools **70**(2), 313–331 (2019)
4. Pocheptsov G.: The War in Cognitive Space (2017). https://nesterdennez.blogspot.com/2017/08/global-permanent-war_39.html

5. Yan, Z., Robertson, T., Yan, R., Sung Yong Park, Bordoff, S., Chen, Q., Sprissler, E.: Finding the weakest links in the weakest link: how well do undergraduate students make cybersecurity judgment? Comput. Hum. Behav. **84**, 375–382 (2018)
6. Li, C., Lalani, F.: The COVID-19 pandemic has changed education forever. This is how (2020). https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/
7. Schools of the Future: Defining New Models of Education for the Fourth Industrial Revolution, 2020 WEF. http://www3.weforum.org/docs/WEF_Schools_of_the_Future_Report_2019.pdf
8. Pipikaite, A., and Davis, N.: Why cybersecurity matters more than ever during the coronavirus pandemic. WEF (2020). https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity
9. Guterres, A.: The future of education is here. Launch of the policy brief: education during COVID-19 and beyond, United Nations. https://www.un.org/en/coronavirus/future-education-here. Accessed Apr 2020
10. Pinchuk, O., Burov, O., Lytvynova, S.: Learning as a systemic activity. In: Karwowski, W., Ahram, T., Nazir, S. (eds.) Advances in Human Factors in Training, Education, and Learning Sciences. AHFE 2019. Advances in Intelligent Systems and Computing. 2019, vol. 963, pp. 335–342. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-20135-7_33
11. Lytvynova, S., Burov, O.: Methods, forms and safety of learning in corporate social networks. In: ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Kyiv, Ukraine, 15–18 May, pp. 406–413 (2017). http://ceur-ws.org/Vol-1844/10000406.pdf
12. Pinchuk, O.P., et al.: Digital transformation of learning environment: aspect of cognitive activity of students. In: Proceedings of the 6th Workshop on Cloud Technologies in Education (CTE 2018), Kryvyi Rih, Ukraine, 21 December 2018. CEUR Workshop Proceedings, # 2433, pp. 90–101 (2019)
13. Ahram, T., Karwowski, W.: Advances in human factors in cybersecurity. In: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, 24–28 July 2019, Washington D.C., USA (2019)
14. Bandara, I., Ioras, F., Maher, K.: Cyber security concerns in e-learning education. In: Proceedings of ICERI2014 Conference, IATED, 0728-0734 (2014)
15. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2020). https://doi.org/10.6028/NIST.SP.800-181
16. Frezzo, D.: The role of technology in the education of the future. 2020 World Economic Forum (2020). https://www.weforum.org/agenda/2017/05/science-of-learning/
17. Lavrov, E., Pasko, N., Tolbatov, A., Tolbatov, V.: Cybersecurity of distributed information systems. the minimization of damage caused by errors of operators during group activity. In: Proceedings of 2nd International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017), 2017, pp. 83–87 (2017)
18. Veltman, J.A., Jansen, C., Hockey, G.R.J., Gaillard, A.W.K., Burov, O.: Differentiation of mental effort measures: consequences for adaptive automation. Nato Sci. Ser. Sub Ser. I Life Behav. Sci. **355**, 249–259 (2003)
19. Iatsyshyn, A.V., et al.: Application of augmented reality technologies for preparation of specialists of new technological era. In: Augmented Reality in Education: Proceedings of the 2nd International Workshop (AREdu 2019), Kryvyi Rih, Ukraine, 22 March 2019, pp. 181–200 (2020). ISSN 1613-0073. http://ceur-ws.org/Vol-2547/paper14.pdf

20. Human Systems Integration Approach to Cyber Security. STO-TR-HFM-259. STO/NATO 2020, June 2020, 112 pp. (2020). ISBN 978-92-837-2272-4
21. Mulder, L.J.M., Van Roon, A., Veldman, H., Laumann, K., Burov, A., Quispel, L., Hoogeboom, P.J.: How to use cardiovascular state changes in adaptive automation. In: Hockey, G.R.J., Gaillard, A.W.K., Burov, O. (eds.) Operator Functional State. The Assessment and Prediction of Human Performance Degradation in Complex Tasks. NATO Science Series, pp. 260–272. IOS Press, Amsterdam (2004)
22. 2020-security-strategy-playbook. https://techtalksummits.com/2020-security-strategy-playbook/
23. Krylova-Grek, Y.: Psycholinguistic aspects of humanitarian component of cybersecurity. Psycholinguistics **26**(1), 199–215 (2019)