Cybersecurity in Educational Networks

Oleksandr Burov[1(&)], Svitlana Lytvynova[1(&)], Evgeniy Lavrov[2(&)], Yuliya Krylova-Grek[3(&)], Olena Orliyk[4(&)], Sergiy Petrenko[4(&)], Svitlana Shevchenko[5(&)], and Oleksii M. Tkachenko[6(&)]

[1] Institute of Information Technologies and Learning Tools, 9 Berlinskoho Str., Kyiv 04060, Ukraine
burov.alexander@gmail.com,s.h.lytvynova@gmail.com

[2] Sumy State University, Sumy, Ukraine prof_lavrov@hotmail.com

[3] State University of Telecommunications, Kyiv, Ukraine
yulgrek@gmail.com

[4] Scientific-Research Institute of Intellectual Property, Kyiv, Ukraine
e.orliyk@ndiiv.org.ua,inprolex@i.ua

[5] Borys Grinchenko Kyiv University, Kyiv, Ukraine
s.shevchenko@kubg.edu.ua

[6] National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
oleksii.tkachenko@gmail.com

Abstract. The paper discusses the possible impact of digital space on a human, as well as human-related directions in cyber-security analysis in the education: levels of cyber-security, social engineering role in cyber-security of education, "cognitive vaccination". "A Human" is considered in general meaning, mainly as a learner. The analysis is provided on the basis of experience of hybrid war in Ukraine that have demonstrated the change of the target of military operations from military personnel and critical infrastructure to a human in general. Young people are the vulnerable group that can be the main goal of cognitive operations in long-term perspective, and they are the weakest link of the System.

Keywords: Cyber-security Cognitive performance Education Social engineering

1 Introduction

A constantly increasing number of cybersecurity-related publications demonstrates a growing comprehension of this complex challenge facing the Globe and the necessity to consider wider spectrum of issues. Unfortunately, technical and informational solutions cannot satisfy humans' safety and security of life and activity. Since it is an on-going process, specialists in this field are lack of current information and feel the

need to change the training programs of cybersecurity (CS) that should focus "on the social, economic, and behavioral aspects of cyberspace, which are largely missing from the general discourse on cybersecurity" [1, p. 2]. First of all, new training programs should take into account the human features and a person's functional state as well as

© Springer Nature Switzerland AG 2020
T. Ahram et al. (Eds.): IHSI 2020, AISC 1131, pp. 359–364, 2020.
https://doi.org/10.1007/978-3-030-39512-4_56

cognitive resilience due to the increasing role of cognitive warfare [2]. The cognitive war must deserve particular attention as its primary goal is not a prompt military operation and fight for territorial or economic resources, but it is a battle for people [3] aimed at affecting public opinion, radicalizing young people, infiltrating and corrupting enemy's information systems. Since the information in the global network exists out of space and time, the Net itself becomes an active human influencer [4], especially in social networks [5].

One of the human dimensions of extensive change involves the transition from producing predominantly material issues to intellectual ones and alterations in competitive target resources. Intellectual capital (first of all, human capital includes abilities, talents, knowledge, ideas, etc.) is becoming the most in-demand resource and the target of diverse cyber-attacks [6]. At present, digital networks are taking more and more crucial place in our everyday routine. Therefore, interventions to these networks pose a real threat to both humans and the state. By saying "humans" we don't mean just military (including cyber-)specialists, but everybody, since the cyberspace is a worldwide electronic medium facilitating social interaction. Undoubtedly, transformations in the forms, methods, and means of education are related to and accompanied by changes in learners' behavior by transition from traditional classroom education to network activities with unproductive consequences of the information received and its safety. However, at the same time, a human is still the weakest link in cybersecurity systems [7].

Purpose. To analyze potential hazards associated with learners' participation in online activities in digital education.

2Method

Considering learning as a type of activity in human-system integration, today's learner may be viewed as an operator-researcher who acts in the digital environment. Successful learning involves mutual adaptation between a human and activity tools [8] using individual cognitive abilities measurement [9, 10]. On the other hand, it is possible to use ergonomics' methods and techniques to assess a learner's safety in the education system.

3Results and Discussion

The core directions of cybersecurity analysis in the education field should be focused on the following issues: CS levels, role of social engineering in providing CS in education, and so-called "cognitive vaccination".

Cyber Security Levels. The paper deliberates about the problems of learners' cybersecurity in the educational process. It emphasizes the fact that the given problems are not limited to the technical aspects of protecting information resources, which must include such types of protection as legal, technical, informational, organizational, and psychological ones [4, 11].

The legal maintenance covers (but not limited) [12]:

- National and international legislation in the field of cybersecurity.
- Appropriate international legal agreements, conventions, and standards.
- Intellectual property rights.
- Protection of computer programs and databases [13].
- Personal data protection.
- Legal support of victims of cyber-attacks and expert opinions on the results of the computer-technical examinations.
- Legal support of a human right to know and get access to verified information (a person's education and development cannot be achieved without realizing selfconcept).
- Legal literacy for young people regarding actions in digital networks.

Cybersecurity technical aspects imply the security of diverse technical means and tools (computers, networks, databases, information resources, etc.).

Information tools can be categorized according to the tasks solved by the users [11, p. 321]: Protection/Remedies, Awareness, Content, Learning to use, Security, Lifespan, Avoiding threats.

Organizational tools for solving cybersecurity issues comprise Awareness, Learning the cybersecurity culture, CS professional staff and the general population, Creation of CS special means, Distribution of CS facilities, Control of use.

Psychological means can be grouped depending on the personal and interpersonal level: National, Public, Group, Individual, Cultural, Cognitive, Intellectual, Habits.

Among the psychological tools aimed at achieving cybersecurity, the cognitive ones are the most vital. Recent cybersecurity research shows that information technology tools in this field are constantly being refined and hacker attacks become more human-centered [14]. This is extremely important because of the urgency of personal safety and the results of its activities. As shown in [4], the common accessibility of the information space leads induces that a person becomes a target of other participants' activity, while working in the information environment. Harmful activities force a person to read or to respond to the "wrong" information or to make other mistakes that leave his/her system vulnerable to cyber attacks, information leakage, etc.

These days, not only huge corporations or governing bodies are usual targets of cyber attacks, ordinary people, especially children and young adults, suffer from them as well. Their cognitive sphere is the most vulnerable (weak) link in the persontechnology network [7], in particular, due to the extending usage of group work

(project-oriented activity). In this regard, it is reasonable to exploit the operators' experience of preventing against cyber threats in the education field [15], accounting that in anthropocentric networks, which make up an ever-increasing share among common networks, the network itself acquires new properties, acting as an independent component (in addition to such factors as the network unit, interface, and links) acting beyond time and space [6].

Role of Social Engineering in Providing CS in Education. The spectrum of hazards from the open cyberspace is continuously expanding. If ten years ago, the hazards for schoolchildren could be reduced to a relatively small number of groups (viral attacks, cybercrime, the hazards of Internet surfing), then the diversity of hazards and threats is increasing over time, affecting all possible human activities online [11]. Threats coming from networks can be divided into the following types: active and passive, open and hidden, current and delayed [11, p. 309]. The greatest danger to students is hidden hazards of the Internet and especially the social engineering methods [16, 17].

The shift of cybercrime goals from technical (information) objects to the human link led to the emergence of social engineering (SE) as methods and technologies for obtaining the necessary access to information based on the characteristics of human psychology. Social engineers, for instance, use fear, interest or trust to manipulate, to change the behavior or perception of others. Sad to say, nowadays everybody can master the art of gaining access to computer systems or personal data [18]. Yet it is possible to resist SE impact if to follow nine recommendations:

- User credentials are the school property.
- Conduct introductory and regular training sessions for staff and students to increase information security skills.
- It is mandatory to have safety regulations and instructions that the user must always have access to.
- Users' computers must always have up-to-date antivirus software and firewall installed.
- Systems of detection and prevention of attacks should be used in any corporate network. Confidential information leakage prevention systems should be employed as well.
- It is necessary to restrict users with administrative privileges for operating systems and applications as much as possible.
- You need to be vigilant about the source requiring sensitive information.
- You should never open the contents of applications or follow the link without examining all the details and your own experience.
- It is also important to be critical of the messages received: how plausible can the information be?
- It is recommended to report such dangers to other family members, first of all, the elderly, who have no experience of using electronic means and are not aware of SE issues.

We believe that psycholinguistic tools could be useful to recognize SE interference and the ways to affect human cognition and safety, especially the cognitive weapon (mass-media, politicians' impact, textbooks, etc.) [19]. If a person knows, realizes and is aware of these tools, he/she can obviously resist them, which is the most effective way of providing cybersecurity.

"Cognitive Vaccination". In 2002, UN General Assembly adopted resolution 57/239 "Elements to Create a Global Cybersecurity Culture" [20] to identify nine fundamental complementary elements of the global cybersecurity culture, including awareness; responsibility; response; ethics; democracy; risk assessment; design and implementation of security measures; security management; revaluation.

The Resolution and cybersecurity elements relate to five levels of CS mentioned above. At the same time, it can be noted that psychological means (which relate directly

to each person separately) involve only behavioral aspects, i.e. responsibility and ethics; in other words, it is a manifestation of the social attitude to cybersecurity expressed by a person, who is considered as a relatively passive element of the cybersecurity system. Moreover, since no means guarantee 100% of human protection, it is advisable to determine the range of individual abilities to produce personal protection, except for the above.

The analysis of the curriculum and training programs implemented in pedagogical educational institutions has demonstrated that traditional education does not pay enough attention to the development of students' critical thinking skills related to the use of the Internet.

We propose to introduce "cyber vaccination" as part of the cybersecurity-related training. It can increase the human's safety level by a wide array of means: to accept rules for safe and responsible use of the Internet, to improve critical thinking skills, to train the participants of the network activity and to inform them about possible impact of the cyber environment, to model and to simulate cyber threats in relatively closed systems such as corporate and educational ones, to teach how to confront with the cyber threats for gaining the practical experience of behaving and restoring after cyber vulnerabilities, including assessing the person's current state and necessary adjustments to optimize his/her cognitive workability, and cyber survival trainings aimed at recognizing the threat or possible dangerous action in the network and the rational psychological and behavioral compensation for this action.

4 Conclusion

The analyzed features of teaching and learning in contemporary digital environment and recommendations could be an influential tool to improve the security and safety of educational process by adapting students' activity depending 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. Ahram, T., Karwowski, W.: Advances in Human Factors in Cybersecurity. Proceedings ofthe AHFE 2019 International Conference on Human Factors in Cybersecurity, Washington D.C., USA, 24–28 July 2019. Springer, Cham (2019)
2. Bienvenue, E., Rogers, Z., Troath, S.: Cognitive Warfare (2018). https://cove.army.gov.au/article/cognitive-warfare
3. Pocheptsov, G.: The War in Cognitive Space (2017). https://nesterdennez.blogspot.com/2017/08/global-permanent-war_39.html
4. Burov, O.: Educational networking: human view to cyber defense. Inf. Technol. Learn. Tools 52, 144–156 (2016)
5. Lytvynova, S., Burov, O.: Methods, forms and safety of learning in corporate socialnetworks. In: Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, 15–18 May, pp. 406–413 (2017). http://ceur-ws.org/Vol-1844/10000406.pdf
6. Bykov, V.Yu., Burov, O.Yu., Dementievska, N.P.: Cybersecurity in digital educationalenvironment. Inf. Technol. Learn. Tools 70(2), 313–331 (2019)
7. Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E.: Finding theweakest links in the weakest link: how well do undergraduate students make cybersecurity judgment? Comput. Hum. Behav. 84, 375–382 (2018). ISSN 0747-5632
8. Veltman, J.A., Jansen, C., Hockey, G.R.J., Gaillard, A.W.K., Burov, O.: Differentiation ofmental effort measures: consequences for adaptive automation. NATO Sci. Ser. Sub Ser. I Life Behav. Sci. 355, 249–259 (2003)
9. Basye, D.: Personalized vs. Differentiated vs. Individualized Learning. ISTE 1/24/2018 (2018). https://www.iste.org/explore/articleDetail?articleid=124
10. Veltman, H., Wilson, G., Burov, O.: Operator Functional State Assessment. Cognitive Load.NATO Science Series RTO-TR-HFM-104, Brussels, pp. 97–112 (2004)
11. Burov, O.Iu., Kamyshin, V.V., Polikhun, N.I., Asherov, A.T.: Technologies of networkresources' use for young people training for research activity, Monograph. In: Burov, O.Iu. (ed.) Informatsiini Systemy. TOV, Kyiv (2012). (in Ukrainian). 416 p.
12. Orlyuk, O.: On the development of a policy on intellectual property in national universitiesand the role of profile departments of intellectual property. Theory Intellect. Prop. 5, 61–69 (2017)
13. Petrenko, S.A.: Protection of the Computer Program as an Intellectual Property Object: Theory and Practice, Monograph, p. 172. Research Institute of IP at NA-PrNU, "LazuritPolygraph", Kyiv (2011)
14. https://www.computerweekly.com/news/252448101/People-top-target-for-cyber-attackersreport-confirms
15. Lavrov, E., Pasko, N., Tolbatov, A., Tolbatov, V.: Cybersecurity of distributed informationsystems. The minimization of damage caused by errors of operators during group activity. In: Proceedings of 2nd International Conference on Advanced Information and Communication Technologies (AICT 2017), pp. 83–87 (2017). https://doi.org/10.1109/AIACT. 2017.8020071
16. Savchuk, T.: Social Engineering: How Fraudsters Use Human Psychology on the Internet(2018). https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html. Accessed 30 Aug 2018. (in Ukrainian)
17. A Powerful Tool for Social Engineering. https://www.trustedsec.com/social-engineertoolkit-set/#
18. SecurityLab. https://news.rambler.ru/other/39395044-nazvany-glavnye-problemy-bezopasnosti-web-resursov-v-2017-godu/
19. Krylova-Grek, Yu.: Psycholinguistic peculiarities for application of the symbol-words in thepolitical communication. Adv. Educ. 7, 129–134 (2017). https://doi.org/10.20535/24108286.99321(2017)

20. UN General Assembly Resolution 57/239 Elements to Create a Global Cybersecurity Culture (2002). http://www.un.org/en/documents/declconv/conventions/elements.shtml