Oleksandr Burov
Dr.Sc., Senior Researcher, Leading Researcher
Institute of Information Technologies and Learning Tools,
Department of Technologies of Open Learning Environment, Kyiv, Ukraine
ORCID: 0000-0003-0733-1120
ayb@iitlt.gov.ua

CYBERSECURITY IN EDUCATION ENVIRONMENT

Abstract. Problems of cyber security of the educational process participants are discussed. It is articulated that these problems are not limited to the technical aspects of the protection of information resources, and solutions must include in their entirety legal, technical, informational, organizational and psychological types of protection. Among the psychological tools for securing, it is proposed to distinguish cognitive ones, as the general population, and especially children and youth, increasingly become targets of cyber-attacks.

Keywords: security, networks, education.

1. INTRODUCTION

At present, our lives are being built more and more around digital networks. Interventions to these networks pose a real threat to humans and to the country [1]. In order to keep abreast with the rapidly changing threat landscape and maintain a robust cyber defense, civilian and military organizations at the national and international levels try to adopt their new enhanced policy accounting new challenges appeared over last two years with the main focus to a human as the weakest link in the working system [2].

The problem statement. The top priority is the protection of the communications systems owned and operated by a human. Cyberspace is, and will continue to be a very important part of the battlefield of ideas and civilizations. Lesson learned from Ukraine-Russia conflict allows to argue that most future operations will (at least) start in cyberspace and operations will most probably be conducted within it during the conflict, increasing the importance of its control, with special attention to the cognitive activity, that is a main part of the lifespan learning process [3].

Analysis of recent studies and publications.

While technical/technological solutions are being developed in response to cyber-attacks [4], there is increasing awareness that the role of human performance and decision making in cyber security is critical to increase the effectiveness of responses to developing threats [5]. Especially it is significant from viewpoint of future manpower, because young people are especially sensitive to external influence and are the most active part of "network population", as well as especially sensitive to the increasing cognitive workload under different internal and external factors during learning and job performance [6].

The article's goal. Conceptual assessment of key problems and tasks of the cyber security (CS) of the educational process participants.

2. THE theoretical BACKGROUNDS

The human factor may be a systems weakest link, but at the same time it may also be a powerful resource to detect and mitigate emerging threats. Several areas of most critical and urgent needs as well as the knowledge gaps to address in cyber research agendas of NATO and the nations can be defined as: psycho-social, cultural, conceptual and organizational dimensions of cyber security.

Cyber objects *(humans)* can be: decision makers, key defence specialists, financial managers, key industry managers, creators of knowledge, population (including future military and defence manpower).

Successful cyber security involves accounting for all groups of remedies. Ignoring any of them can lead to loss of: government control, military control, financial control, industry control, manpower control, data.

Taking into account last years' trend in hybrid war, the cognitive war needs a special attention, because its goal is not a prompt military operation and fight for territorial or economic resources, but for people. Moreover, not only the highest level's decision makers, but also the entire population of the target country, since it must perceive and support state leaders controlled by the aggressor, as events in Ukraine and other countries demonstrated over last years. In such a context, defence is a means of countering and neutralizing cognitive weapons. Cognitive weapon is a control of the intellectual environment of the country of the enemy by false scientific theories, paradigms, concepts, strategies, influencing its governance towards weakening the defence of significant national capacities. Main features of the cognitive war are as follows:

1. *Military strategy* is suppressed and subordinated the consciousness of the enemy. Opponent is programmed cognitively to self-destruction.
2. *Goal* is implanting to the enemy a thought that the struggle itself does not exist.
3. *Result* consists in enemy's cognitive damage which features can be characterized as: represented false theory affects national science, relevant scientific schools and generations, corresponding defective frames are programmed to misconceptions about the most important management paradigms, development of the country, this reproduce generations of students and graduate students of the corresponding grade, they saturate the relevant reference structures of government and decision-makers, accordingly, there is an erroneous destructive state management policy.

To date, there is a gap between the traditional approach to cyber security (the solution of technical and information tasks) and the need to take into account the human factor. Understanding of this leads to changes in the training of specialists in cyber security and general population.

THE RESULTS AND DISCUSSION

The educational environment (EE) is one of the cornerstones of education. There are many different definitions and classifications of the EE. It has a multifactorial influence on subjects of the educational process, changing both in time and in space. And this is true both for the traditional learning environment and for the synthetic one.

One can note that the learning environment in the content plan always arises as a dynamic process of forming a network of relations in the subject of learning, to which (not always consciously) selectively involve the various elements of the external and/or internal environment, and this dynamic process is characteristic of any learning environment, but in immersive and virtual EE, it becomes even more acute due to a more profound immersion of the student into the learning process.

Cyberspace can be considered as a triad, which includes: 1) information in its digital representation: static (files recorded on the storage medium) and dynamic (packets, threads, commands, queries, etc.); 2) technical infrastructure: ICT, software, databases and knowledge bases; 3) information interaction of entities using received (transmitted) information and processing through technical infrastructure. This notion is bound with the notion of cyber security as the protection of the vital interests of man and citizen, society and state when using cyberspace.

The threats' spectrum from open cyberspace is constantly expanding. If ten years ago the hazard to schoolchildren could be reduced to a relatively small number of groups (viral attacks, cybercrime, threats of Internet surfing), at present, the diversity of threats and hazards is constantly increasing, affecting all possible human actions in the network.

The threats coming from networks can be divided into the following types: active and passive, open and hidden, current and deferred.

As a rule, national legislations related to CS do not consider the sphere of education as the critical area for the protection of which they are aimed. However, today's pupils and students in the short term can work in those areas. Therefore, they already need protection and appropriate training as well as an understanding of the general possible target groups of cyber security. For example, by the following classification [3]: pupils/students, teachers, education managers, children/youth (in general), population (in general, as a social environment).

Depending on the means of action, the problems (and appropriate means) of cyber security can be classified into five groups: Legal, Technical, Information, Organizational, Psychological.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

The problems of cyber security are not limited to the technical aspects of the protection of information resources; they must include in their entirety the following types of protection: legal, technical, informational, organizational and psychological. Among psychological means of securing cyber security, it is expedient to distinguish cognitive ones. Further research of the problem should focus on the detailed development of types of threats to the participants in the educational process, as well as methods of counteraction.

REFERENCES

[1] K. Nemchynova. «Cyber security and cyber weapons as a challenge to the State of Ukraine». http://www.liga.net/print/opinion/255595_kiberbezopasnost-i-kiberoruzhie-kak-vyzov-gosudarstvu-ukraina.htm. 26.10.2015 (In Ukrainian)

[2] Z.Yan, T. Robertson, R. Yan, Sung Yong Park, S. Bordoff, Q. Chen, and E. Sprissler. «Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?», Computers in Human Behavior, ISSN: 0747-5632, Vol: 84, Page: 375-382, 2018.

[3] O. Ju. Burov, «Educational Networking: Human View to Cyber Defense», *Information Technologies and Learning Tools*, 52, 144—156, 2016.

[4] B. Bystrova, «Comparative analysis of curricula for bachelor's degree in cyber security in the USA and Ukraine, *Comparative professional pedagogy»,* 7(4), 114–119, 2017.

[5] L. D. Saner, S. Campbell, P. Bradley, E. Michael, N. Pandza, and M. Bunting. «Assessing aptitude and talent for cyber operations». In D. Nicholson (Ed.), *Advances in Human Factors in Cyber security* (pp. 431–437). *Advances in Intelligent Systems and Computing*, Vol. 501, Springer International Publishing, 2016.

[6] H. Veltman, G. Wilson, O. Burov. «Cognitive load». In: NATO Science Series RTO-TR-HFM-104, Brussels, 97–112, 2004.