ISSN: 2692-5079

as the most effective for a specific task method of Artificial Intelligence can be considered as basic one. In most cases, its effectiveness could be enhanced by supplementing it with another appropriate method. The set of basic and complementary methods could be called a hybrid method of Artificial Intelligence.

V. Idea for a Cocrete Application

Based on the experience gained in the study of the application of Artificial Intelligence methods in different phases of Cyber-defense, the authors intend the following steps to the experimental application of Artificial Intelligence methods in creating an Adaptive Cybersecurity Training system:

Following the so-called "Task approach" and the classification of the tasks solved by them [13], the authors focused on task B2 “Solving a classification problem” (i.e. determining the affiliation of the object to one of the components of a commonly accepted classification scheme, or identifying the object by its characteristics compared to the characteristics of certain patterns). For the initial experiments it is planned to form several courses with alternative Working Paths, composed of the modules in the respective blocks. The student passes preliminary tests, based on which the system refers him to one of the variants of the curriculum.

The analysis of relatively scarce literary sources and the experience of the implementation of Artificial Intelligence methods in Cyber Intelligence directed the team to so called Reinforcement Learning method [14], [15]. The essence of Reinforcement Learning is training through interaction. A Reinforcement Learning agent interacts with its environment and, upon observing the consequences response to rewards received. This paradigm of trial-and error learning has its roots in behavior psychology, and is one of the main foundations of Reinforcement Learning. The other key influence on this method is optimal control, which has lent the mathematical formalisms (most notably dynamic programming) that underpin the field.

The best sequence of actions is determined by the rewards provided by the environment. Every time the environment transitions to a new state, it also provides a scalar reward Rt+1 to the agent as feedback. The goal of the agent is to learn a policy (control strategy) that maximizes the expected return (cumulative, discounted reward) (Fig. 4).

Unlike the Controlled Learning usually implemented in Neural Networks, Reinforcement Learning is realized using previously collected examples or a set of data for training that is not suitable for Interactive Learning. That’s why the bulk of the training can be accomplished by analyzing a collection of existing incidents, identifying key attributes that have patterns of correlation to categories, and creating a model to make predictions from these patterns. In this situation, the main purpose of the agent is to maximize the remuneration achieved in the long run, i.e. the sum of the awards received from all situations or conditions that will be reached in the future:

$$R_t = r_{t+1} + \gamma r_{t+2} + \gamma^2 r_{t+3} + \cdots . = \sum_{k=0}^{\infty} \gamma^k r_{t+k+1} \qquad (1)$$

where r is a consequence of an action that results in a digital reward for each time step and Y represents the reported discount rate to show how important the future reward is.

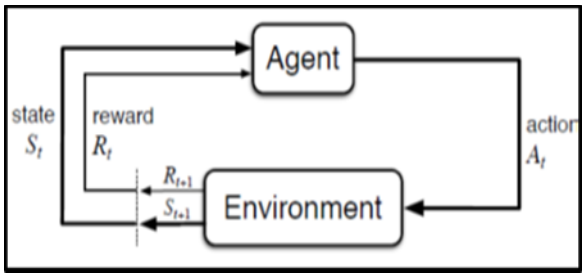

Fig. 4. Agent-Enivrinment interaction

As mentioned above, the basic method of Reinforcement Learning can be supplemented with another appropriate method. The authors assume that as such can be selected the so-called Fuzzy Armor Learning [16]. It is considered that in case of an anomaly, Fuzzy Armor Learning analyzes and updates the Q-value of the learning agent by applying computational intelligence and anomaly-based knowledge management techniques in a recursive iteration of the execution cycle.

VI. Conclusion

Having in mind the utmost importance of Cyber-security (respectively, the Cyber-security Education) for the economy, society and privacy, serious efforts are needed to develop sufficiently effective education programs, in particular, comprehensive, consistent and dynamic framework for building and improving such programs.

This article reflects attempts to improve education by introducing dynamic principles and personalization in the curriculum realizing Adaptive Learning Systems managed by methods of Artificial Intelligence. In this study, the authors used their experience in the application of these methods in the field of Cyber-security.

Acknowledgment

This research is realized under the National Science Program “Information and Communication Technologies for common digital market in science, education and security” financed by Ministry of Education and Science in Bulgaria.

References

[1] ITU National Cybersecurity/CIIP Self-Assessment Tool ITU April 2009

[2] National Initiative for Cybersecurity Education(NICE). Cybersecurity Workforce Framework Special Publication 800-181 August 2017

[3] Network Information Security in Education ENISA January 2012

[4] Brokerage model for Network and Information Security in Education ENISA 2013

[5] A Role-Based Model for Federal Information Technology / Cyber Security Training Special Publication 800-16 Revision 1 NIST 03/14/2014

[6] https://cybereducationscheme.org/the-global-ace-scheme#main-content

[7] Cybersecurity A Generic Reference Curriculum NATO Emerging Security Challenges Working Group September 2016

[8] Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity Joint Task Force on Cybersecurity Education Version 1,0 Report December 2017

[9] P. Brusilovsky, C. Peylo. Adaptive and Intelligent web-based Educational systems, Intl. J. of Artificial Intelligence in Education, 13, pp. 156-169.

[10] S. Stoyanov, P. Kirschner. Expert Concept Mapping Method for Defining the Characteristics of Adaptive E-Learning: ALFANET Project Case, Educational Technology, Research & Development, vol. 52, no 2, 2004, pp. 41- 56.

ISSN: 2692-5079

[11] V. Stefanova-Stoyanova. New Model of Conception for Building Adaptive Systems for Distance Electronic Learning (ASDEL) Cax Technologies,Issue No 5, December 2017.

[12] R. Trifonov, S.Manolov, R. Yoshinov , G. Tsochev, G. Pavlova. An adequate response to new Cyber Security challenges through Artificial Intelligence methods. Applications in Business and Economics, WSEAS Transactions on Business and Economics, 14 (2017) pp. 272 - 281

[13] Trifonov, R., S. Manolov, G. Tsochev, G. Pavlova, Recommendations Concerning the Selection of Artificial Intelligence Methods for Increasing of Cyber-Security, CompSysTech '20, June 19–20, 2020, Ruse, Bulgaria, ISBN 978-1-4503-7768-3/20/06

[14] R.S. Sutton. Reinforcement Learning. An Introduction. Cambridge University Press, 1998

[15] K. Arulkumaran, M.P. Deisenroth, M. Brundage, A.A. Bharath. A Brief Survey of Deep Reinforcement Learning. IEEE Signal Processing Magazine Special Issue on Deep Learning for Image Understanding, November 2017

[16] C. Mohan. An Introduction to Fuzzy Set Theory and Fuzzy Logic, Second Edition, MV Learning, 2018