Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods

Roumen Trifonov  
Faculty Computer Systems and Technologies  
Technical University of Sofia  
Sofia, Bulgaria  
r_trifonov@tu-sofia.bg

Ognian Nakov  
Faculty Computer Systems and Technologies  
Technical University of Sofia  
Sofia, Bulgaria  
nakov@tu-sofia.bg

Slavcho Manolov  
Faculty Computer Systems and Technologies  
Technical University of Sofia  
Sofia, Bulgaria  
slav1943@gmail.com

Georgi Tsochev  
Faculty Computer Systems and Technologies  
Technical University of Sofia  
Sofia, Bulgaria  
gtsochev@tu-sofia.bg

Galya Pavlova  
Faculty Computer Systems and Technologies  
Technical University of Sofia  
Sofia, Bulgaria  
raicheva@tu-sofia.bg

Abstract—The Faculty of Computer Systems and Technologies of the Technical University of Sofia has chosen a development strategy for Cyber-security Education based on: international standardization documents; conceptual model developed by the Joint Task Force on Cybersecurity Education; good practices of the modular structure and dynamic building principles allowing rapid changes to the content. Based on the principles of the "Knowledge Areas" and "Application Areas", each discipline is intended to be developed as a workflow for a particular application area composed of modules representing the appropriate areas of knowledge. Decisively improve education by introduction of dynamic principles and personalization in the curriculum can be realized through so-called Adaptive Learning Systems. In addition, the management of adaptation can be realized through methods of Artificial Intelligence, in the use of which the authors have experience in their application in the field of Cyber-security.

Keywords—Education Continuum, International, Knowledge Areas, Application Areas, Adaptive Training, Artificial Intelligence methods

I. INTRODUCTION

The course "Technologies for Network and Information Security" has been taught at the Faculty of Computer Systems and Technologies of the Technical University of Sofia for eight years now. The course has options for both the bachelor's course at the University and the master's one. The material is structured in 34 modules. During the last one year and a half year, within the National Science Program "Information and Communication Technologies for common digital market in Science, Education and Security" managed by the Ministry of Education and Science, the Faculty has been conducting research aimed at creating a qualitatively new basis for conducting of this training in accordance with the most modern technologies in this field and on the basis of International Standardization in this complex discipline, combining not only technological problems, but also a number of components such as regulatory, organizational, educational, psychological, and so on.

On the other hand, the Faculty of Computer Systems and Technology of the Technical University - Sofia undertook in 2013 research in the field of application of Artificial Intelligence methods in Cyber-security. Since 2017, these studies have been supported by the Research Fund under the Ministry of Education and Science. During the project, its contractors experimented with the effective use of theoretically selected Artificial Intelligence methods to detect attacks, prevent intrusions, and more typical actions in Cyber Defence of Information Systems. In the 14 publications and reports to authoritative international conferences the constructed models, the experimental installations and the results of the experiments are described in detail. The summary of these results is presented as a set of recommendations.

The project proved that the selection of methods of Artificial Intelligence, effective for a given class of tasks, requires formulation of criteria for the selection based on both literature sources and specific research and experiments.

The above two areas of research have prompted the authors to try to build a new philosophy and organization of Cyber-security education based on the use of artificial intelligence methods.

II. INTERNATIONAL REQUIREMENTS AND STANDARDS IN THE FIELD OF CYBER-SECURITY EDUCATION

It should be noted that in recent years we have witnessed unprecedented international coherence, unification and standardization of all elements of Cyber-protection, including its crucial element - the Cyber-security Training. The authors' research pays special attention to initiatives such as:

a) the “National Cybersecurity and Protection of National Critical Information Infrastructure Self-Assessment Tool” of the International Telecommunication Union (ITU) [1];

b) the “American National Initiative for Cyber-security Education (NICE)” [2], led by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce - a partnership between government, academia, and the private sector working to energize and promote a robust network and an ecosystem of Cyber-security education, training, and workforce development (Fig. 1).
The international standardization documents related to the different levels and forms of training in the field of Cybersecurity outline the so-called "Cybersecurity Education Continuum" on the base of the general principles of learning gradation and its continuity over time. In the most consistent and exhaustive form, this "continuum" is formulated in the US National Institute for Standardization and Technology (NIST) standardization document: Special Publication (SP) 800-16 [5] (Fig. 2).

In the JTF CSEC2017 model, the following areas of knowledge are included:

- data security;
- software security;
- component security;
- security of communications;
- system security;
- staff security;
- organizational security and
- social security.

III. PECULIARITIES OF THE APPROACH TO CYBERSECURITY TRAINING AT THE TECHNICAL UNIVERSITY - SOFIA

The intention of the Faculty is to form three disciplines related to the training in Cyber-security: for Bachelors, for Masters of General Computer Science and Cyber-security Masters (plus one auxiliary course for masters who have not passed the bachelor's course at TU-Sofia).

It has already been mentioned about the complex nature of the discipline, which in addition to purely technological aspects includes another fields, such as: normative, organizational, psychological, etc. This leads to the differentiation of the so-called "Blocks" in each of the above disciplines. For example: regulatory and standardization frameworks, policies and services, cryptography and cryptanalysis, identification and authorization, access control, resilience of networks and systems, reporting and handling of incidents and vulnerabilities, etc.

The practice indicates the efficiency and relevance of the modular structure, combined with a completely new organization of curricula.

Considering all of the above, the team developing the framework for Cyber-security Training program for students in engineering specialties related to computer systems and technologies has chosen a development strategy based on:
modules have to be modified to -
creating an Artificial
adapting the parameters presented in the user model;
are:
knowledge, interests and more. The main technologies
levels are two different ways of hypermedia adaptation and
adaptability of the blocks is expected
to the parameters presented in the user model;

Based on the principles of the "Knowledge Areas" and
"Application Areas", each discipline is intended to be
developed as a workflow for a particular application area
composed of modules representing the appropriate areas
of knowledge. These workflows are developed on two levels,
with the above-mentioned "Blocks" on the upper level and on
the second level, the modules from which each of the blocks
is created. In addition, the workflow of the blocks is expected
to be constant, and the modules - adaptive. Some of the
modules will be involved in all workflows for relevant
application areas, some of which will only be part of them. In
addition, some of the modules have to be modified to
participate in certain workflows of application areas.

The dynamic principle mentioned above will be achieved
by changing the content of the workflow (replacing one
module with another) and modifying some of these modules.
The dynamic modular design chosen by the team could bring
some potential benefits in case of future development as
follows:

- ability to convert part of the modules into an
  interactive "on-line" format, and thus creating "hybrid
courses";
- possibility for individualization of the curricula in the
disciplines depending on the measurable
characteristics of the students.

It is known from practice that the dynamic principles and
personalization in the curriculum can be realized through the
so-called Adaptive Learning Systems.

IV. ADAPTIVE TRAINING AND METHODS OF ARTIFICIAL
INTELLIGENCE

According to [9], "... the Adaptive Learning System
(ALS) is an interactive system that personalizes and adapts
learning content, pedagogical models and interactions
between participants in order to meet the needs and
preferences of users, if and when they arise." As per [10],
two things can be adapted in ALO - the content of the study pages
and the hyperlinks between them, i.e. there are two levels of
adaptation - at the content level and at the link level. These
levels are two different ways of hypermedia adaptation and
are called Adaptive Presentation and Adaptive Navigation,
respectively.

The purpose of Adaptive Navigation is to help the learner
find his or her most appropriate path in hyperspace by
adaptively presenting the links in it according to his or her user
model. It helps the learner to choose how to move from the
current page to the next, depending on his needs, level of
knowledge, interests and more. The main technologies for this
are:

a) Direct Guidance - can be applied in any system that can
decide which is the next "best" node for the learner, according
to the parameters presented in the user model;

b) Curriculum Sequencing - the aim is to provide a
curriculum that includes an appropriate for each learner
sequence of learning units that he must acquire, as well as a
sequence of learning tasks that he must solve. This works on
a principle similar to Direct Guidance, but guarantees long-
term consistency without limiting hyperspace.

Practically [11], the Narrative Graph presents an adaptive
training course, i.e. it is necessary that the Working Path it is
tailored so that for each learner there is at least one suitable
path, regardless of the Learner's Model. Its design should
enable each learner to go through a Working Path without
loops in the nodes and with a test in the output node. All
possible settings of the Module for Adaptation Strategies
Management are made in accordance with the Pedagogical
Strategy set in the Adaptive Course.

The term "Artificial Intelligence", introduced by John
McCarthy in 1956 at a conference at the University of
Dartmouth, is not directly related to the analogy of Human
Intelligence. According to McCarthy, researchers in Artificial
intelligence can use methods necessary to solve specific
problems by creative functions, which are traditionally
considered the prerogative of human. World practice already
notes a significant number of various applications of Artificial
Intelligence. Without attempting a comprehensive
classification, we could divide these applications into two
main directions [12]:

A. Conditionally called "distributed" or "network" methods:
   A1. Multi-agent systems of intelligent agents;
   A2. Neural Networks;
   A3. Artificial immune systems and genetic algorithms,
etc.;
B. Conditionally called "compact" methods:
   B1. Machine Learning systems, including: associative
      methods, inductive logic programming, Bayesian
classification, etc.
   B2. Image recognition algorithms;
   B3. Expert systems;
   B4. Fuzzy logic, etc.

According to a number of experts, one of the important
directions of fundamental and applied research in the field of
Artificial Intelligence, and above all, in its general theory - this
is the so-called "task approach" to research and development
of Artificial Intelligence theory. Its general idea is that the
entire activity of the subjects interacting in the processes of
application of Artificial Intelligence can be described,
modelled and designed as a system of processes for solving
various tasks. Therefore, the qualitative and quantitative
characteristics describing the tasks, as well as the means and
ways to solve them, are of great importance for the creation of
effective Artificial Intelligence systems.

The selection of the goal for creating an Artificial
Intelligence system is one of the most important creative
stages in solving various problems with these methods. To
justify the application of a certain method of Artificial
Intelligence to solve a specific task, the authors use a
fundamental conclusion made when experimenting with
applications in Cyber-security: the selected by certain criteria
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 CONCRETE 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 $R_{t+1}$ 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:

$$R_t = R_{t+1} + \gamma R_{t+2} + \gamma^2 R_{t+3} + \ldots = \sum_{k=0}^{\infty} \gamma^k R_{t+k+1}$$  \hspace{1cm} (1)

where $\gamma$ 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-Environment 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

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


