An adequate response to new Cyber Security challenges through Artificial Intelligence methods. Applications in Business and Economics.

ROUMEN TRIFONOV[1], SLAVCHO MANOLOV[1], RADOSLAV YOSHINOV[2],
GEORGI TSOCHEV[1], GALYA PAVLOVA[1]
[1]Technical University of Sofia,
8 Kl. Ohridski bul.,Sofia 1000,
[2]Telematics Laboratory
Bulgarian Academy of Sciences, Sofia
Akad.G.Bonchev St, bl. 8
BULGARIA
r_trifonov@tu-sofia.bg, slav1943@gmail.com, yoshinov@cc.bas.bg, gtsochev@tu-sofia.bg,
raicheva@tu-sofia.bg

Abstract: According to the opinion of the leading experts in the field of Cyber Security over the last few years there has been a transition from the stage of Cyber Criminality to the stage of Cyber War. In order to respond adequately to the new challenges, the expert community has two main approaches: to adopt the philosophy and methods of Military Intelligence, and to use Artificial Intelligence methods for counteraction of Cyber Attacks in business and economics. The present paper describes some of the results obtained in the Faculty of Computer Systems and Technology at Technical University of Sofia in the implementation of project related to the application of intelligent methods for increasing the security in computer networks. These results are shown separately in the sphere of Tactical Cyber Threats Intelligence and Operational Cyber Threats Intelligence.

Key-Words: Cyber Security, Advanced Persistent Threats, Cyber Intelligence, Intelligent Agents, Echo State Networks, Network Gateway Monitoring System

1 Introduction

The remarkable Cyber-Threat study conducted by European Network and Information Security Agency (ENISA) [1] is complemented by a series of conclusions and recommendations addressed to policy makers, business and research community. The first two research conclusions read as follows:

- definition of research roadmaps for Artificial Intelligence in Cyber Threat Intelligence. This could include (but not restricted to) attack pattern recognition and knowledge discovery and enrichment of cyber-threat context;
- development of security models based on agility/dynamics of Cyber Threats. This should also include the use of Cyber Threat Intelligence to assess efficiency and performance of implemented security controls.

These conclusions adequately reflect the radical changes over the past three-four years in the Landscape of the Cyber Threats Defense, expressed in two distinct trends.

The first one is concluded in the following: the conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology became insufficient for certain actors because of the evolution in the goals and sophistication of computer network intrusions. A new class of threats, appropriately dubbed the “Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a st ate of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. According to the vast majority of experts, the qualitative transition to new cyber defense tools must involve the widespread use of artificial intelligence methods to analyze information exchanged, network flows, sources of threats, and to plan effective impact measures, including proactive ones.

The other direction is the widespread use in Cyber Defense of the techniques and methods of traditional military science and military intelligence, including so-called “kill chains”. The term "kill chain" was originally used as a military concept related to the structure of the attack. The idea is to effectively counteract the opponent in the various phases of the attack or as a preventive action. The computer specialists at the Lockheed-Martin Corporation [2] are adapting this concept to information security, using it as a method of modeling penetration into a computer network. This model is gradually being adopted in the information security community for data protection by identifying cyber stages and corresponding countermeasures at each stage.

The "kill chain" model developed by Lockheed-Martin includes the following stages: Intelligence; Creation of the weapon; Delivery; Operation; Installation; Command and Control and Goal actions. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense. Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness.

Following these trends, the Faculty of Computer Systems and Technology at Technical University of Sofia began research on the application of intelligent methods for increasing the security in computer networks. An essential section of this investigation is dedicated to the Cyber Threat Intelligence. The present article summarizes some results of a research done by the project team.

2 Basic Features of the Cyber Threats Intelligence Problem Formulation

The Cyber Intelligence or, more precisely, Cyber Threats Intelligence (CTI) has the following definition in the draft Bulgarian National Cyber Security Strategy [3]:

- establishing mechanisms and technical means to maintain an up-to-date picture of possible threats of different scale, sources and character, trends in geopolitical context development and relevant national cyber picture analysis and;
- development of capabilities to help identify attribution sources and take appropriate forms of protection and counteraction.

According to the documents of INSA (Intelligence and National Security Alliance) [4, 5, 6] the preparation of the intelligence in cyber operational environment is a systematic and continuous process of analyzing potential threats to detect a suspicious set of activities that may endanger systems, networks, information, employees, or customers by providing means to visualize and evaluate a number of specific penetration sensor inputs to bring up a particular threat. This process supports the organization's risk management strategy and decision-making in the area of information security. Its application identifies potential threats and assists security and risk managers selectively implement and maximize deep defense strategies by better understanding the critical points in time and space in the operating environment.

The Cyber Threats Intelligence Cycle [7] Is a systematic, continuous process of analyzing potential threats to detect a suspicious set

of activities that might threaten the organization’s systems, networks, information, employees, or customers by providing a means of visualizing and assessing a number of specific intrusion sensor inputs and open source information to infer specific threat courses of action. The model supports the organization’s risk management strategy and the information security group’s decision-making. The application of the model identifies potential threat courses of action and helps the security and risk management leaders selectively apply and maximize a defense in depth strategy via a greater understanding of the organization’s cyber threats at critical points in time and space in the operational environment by:

a) defining the operational environment;
b) describing the operational environment effects on network defense;
c) evaluating the cyber threats, and
d) developing cyber threat courses of action

Figure 1 is a graphical representation of the Cyber Threat Intelligence Cycle.

The development of a Threat Model is an important element of Cyber Threats Intelligence - in particular, identify the capabilities, intentions, and threat technologies that manage its behavior on the network. The Intelligence Team derives this analysis from information on current and previous threat operations. The knowledge of the possibilities of threat, intentions, technology, doctrine and tactics

provides the basis for developing the Threat Model and detecting its vulnerabilities.

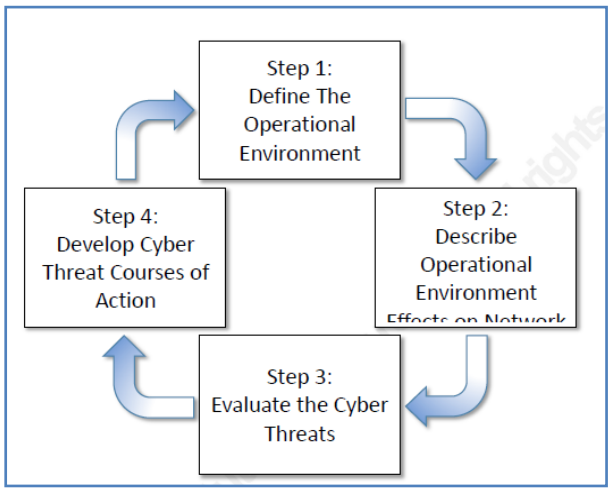

Fig. 1 *Cyber Threat Intelligence Cycle*

Cyber Intelligence data [8] is the key to providing the insight that enables proactive threat mitigation and protection of business data from theft and misuse. By understanding how IT systems are being used and the threats that surround these systems and their users, the core security and value of IT can be better ensured.

The ability to collect and analyze intelligence is realized through log file management tools, security event management, security information management, and file integrity monitoring. Security products are constantly generating log files, whilst file servers and databases maintain logs of who has accessed what and when. All this can only be made sense of in the context of access rights extracted from identity and access management systems and other contextual information.

The growing diversity and mobility of devices used to access IT applications and data add more complexity. User devices can be both a cause of data leaks and a source of security threats. Point security products, including data loss prevention (DLP), end-point security tools and encryption can help, but recognising that a known device is being used in an unusual way requires reviewing it in the context of broader network, geographic and temporal information.

Like its military analogue, the Cyber Threats Intelligence are developed at three levels: strategic, operational, and tactical. For the purposes of this study, the second two are considered:

INSA defines [6] the operational level as: "The level at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. At this level, actors build the capabilities needed to support the tactical operations. They maneuver in cyberspace to position capability where they need to in order to be effective in their tactical missions. At the operational level, an organization's operating environment can be described in terms of physical, logical, information, and social layers. The physical layer refers to the actual information infrastructure - including sensors, servers, and supercomputers - and is grounded in a specific geographic location, which further implies specific authorities and jurisdictions that may influence operations. The logical layer represents a series of platforms and services on which new capabilities are built, enabling information flow. The information layer includes the creation, processing, and storage of the vast range of data on the network - from internal, sensitive communications to systems' configurations to trade secrets and intellectual property. The social layer entails a c oncerted understanding of human behaviour at the group level regarding how the groups are influenced by their surroundings and their access.

The definition of the tactical level [6] is: "The level at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives". The tactical level of the cyber domain is where malicious actors and network defenders maneuver against each other.

In 2016, E NISA developed so called Cyber-Threat Intelligence (CTI) "Big Picture" [1] (Fig. 2). It demonstrates all the elements involved in the attack with the relevant business processes, and shows to which of artifacts (components) the assets involved in the process are targeted.

The "Big Picture" demonstrates the relations with business processes and illustrates the context of different CTI components. It should be noted that issues of detailed knowledge of business processes are key to both attack planning and incident analysis. This contributes to identifying and illustrating the relationship between the various parts associated with CTI, and it is useful for business process analyzers to assess the specific threats to their organization.

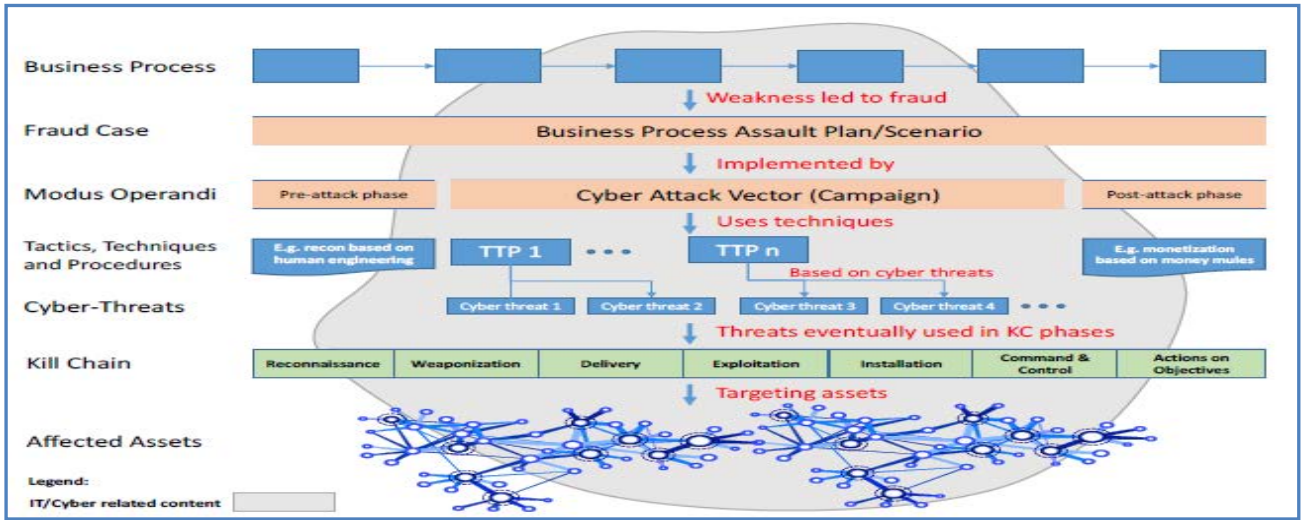

Fig. 2 *Cyber Threat Intelligence "Big Picture"*

3 Methods of Artificial Intelligence in Network and Information Security

The essence of artificial intelligence (AI) is based on the statement that people's intelligence (the potential (inborn) ability of a conscious individual to conclude on a given information) can be described so precisely that it is machine-simulated. After several decades of research, AI is not only the subject of research or planning of some movement, but also of more complex and interdependent solutions. Artificial Intelligence is defined as the intelligence displayed by machines and / or software. This is an academic field of study exploring the goal of creating intelligence. The main issues explored by AI include reasoning, knowledge presentation, automated planning and scheduling, machine learning, natural language processing, computer vision, robotics and common intelligence.

AI enables us to develop autonomous computer solutions that adapt to their context of use, using self-management, self-tuning and self-configuration, self-diagnosis and self-healing. When it comes to the future of information security, AI looks like a very promising field of research that focuses on improving cyberspace security measures.

With rapid pace of development and the desire for more effective countermeasures, artificial intelligence comes as a natural solution to the problem of coping with the ever-growing number of network attacks. Applications in the field of AI are widely accepted by the modern information society. This interdisciplinary endeavor has created a joint link between computer specialists and network engineers in designing, simulating and developing network penetration patterns and their characteristics.

As mentioned in the introduction to this article, world practice has already noted a significant number of various "Artificial Intelligence" applications in computer security. Without trying for a comprehensive classification, we could divide these methods into two main directions:

A. Conditionally named "distributed" or "network" methods:

A1. Multi-Agent Systems of Intelligent Agents;

A2. Neural Networks;

A3. Artificial Immune Systems and Genetic Algorithms, etc;

B. Conveniently named "compact" methods:

B1. Machine Learning Systems, including: associative methods, inductive logic programming, Bayes classification, etc.

B2. Pattern recognition algorithms;

B3. Expert Systems;

B4. Fuzzy logic, etc.

Having into account this variety of methods, it is of particular importance that adequate criteria are selected for the assessment and selection of a specific application for each specific solution. In the above mentioned project, the specification was carried out for two of the main sections of CTI.

4 Methods of Artificial Intelligence Suitable for Tactical Cyber Threats Intelligence in Business

The Tactical Cyber Threats Intelligence [5] aims to detect immediate threats against the business system and to provide an opportunity for their counter-

action. Because of this, the elements of artificial intelligence interact directly with the devices for technical realization of the security policy: Firewalls, Intrusion Detection / Prevention Systems, Anti-Virus Software, Web Gateways and Network Snares.

The identification of attacks is a p rocess of detecting pervasive events occurring during the operation of a business information system. Similarly to high responsability process management systems, the requirement to recognize penetrating actions arises at the time of their occurrence and not after their implementation. Simultaneously with the detection of penetration attempts, it is necessary to start a mechanism for preventive actions that are related to the containment or isolation of the action of a source of attack and the activation of an active counteraction in order to block it and bring it into an incapacity.

The type of detection of attack depends on the nature of the threats (knowns, unknowns and combinations of the two types). A set of criteria have been developed for evaluation of the effectiveness of the discovery and the level of counter-performance. It is also extremely important to achieve the right balance between false positive results and false negatives. Incorrect positive results (so-called false alarms) may be no less harmful than false negative results.

During the development of the project, a comparative analysis of different methods of artificial intelligence in view of the above mentioned criteria was performed on bi bliographic sources. It has been found that the methodology of abnormal tuned multi-agent systems [9, 10, 11, 12] outclass most traditional systems based on artificial intelligence in detecting attacks, particularly of unknown nature. The effectiveness of detecting hazards in multi-agent systems also outperforms traditional systems [13] (Fig. 3). The most important aspects of multi-agent-based Intrusion Detection and Prevention Systems (IDPS) systems are high precision, self-learning and sustainability [14, 15, 16].

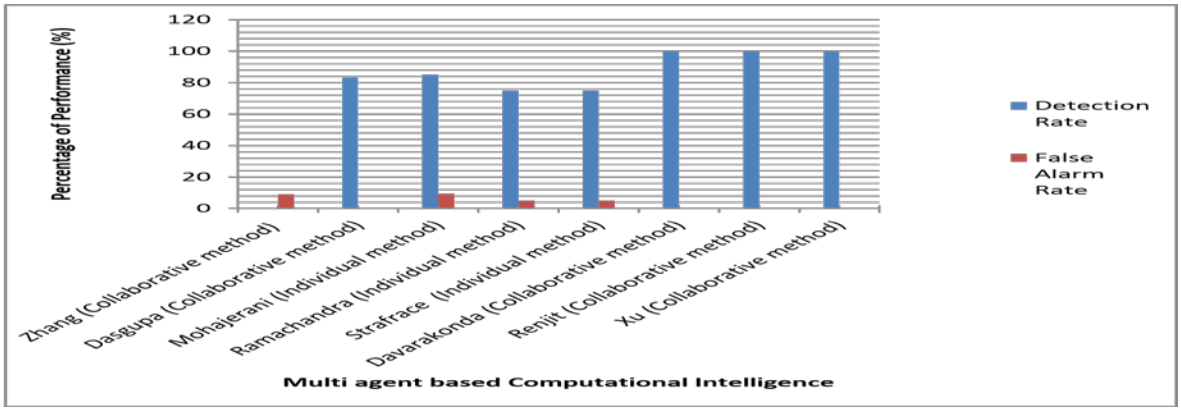

Fig.3 *Value of detection rate and false alarm rate of various multi-agent systems*

The Intrusion Detection and Prevention (IDP) can be defined as a technology that monitors computer activities to prevent attack in the first phase. This is a process of identifying and responding to malicious activity targeting a computer and / o r network. IDP technology works in the so-called "Inline" mode where traffic passes through the device, and when in cause of open threat the packets are blocked and not forwarded to other network segments. This requires OSI levels 3 a nd 4 a nalysis, but for some more complex attacks, level 7 checks are needed. The use of signatures and built-in algorithms can cause a stress of the device, slowing the exchange of information to and from internal network segments.

The IDP system consist of four main elements (Fig. 4): Data Collection, Feature Selection, Analysis and Action. In rule-based IDP systems the analysis is performed by checking the data by comparing it with a signature or model. Another method is based on an anomaly. The action determines the system's attack and response.

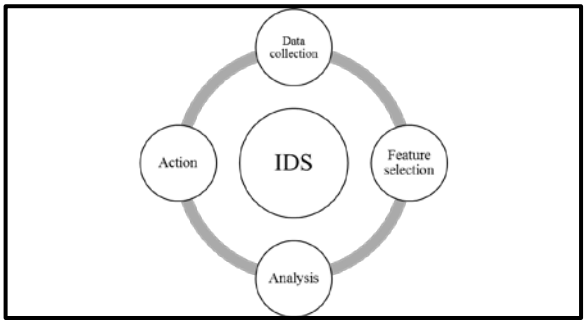

Fig. 4 *Elements of IDP system*

Detecting the attempts for intrusion can be very effective for those attacks that have been programmed into the detection system (the code of attack is present in the software library). However, it is not possible to predict all the different attacks that may occur. For this reason, it is necessary to detect anomalies. One of the problems here is that many false alarms are likely to be raised. Unusual but legitimate use can sometimes be considered abnormal. The challenge is to develop a model that perceives a v ariety of legitimate use scenarios without warning of danger but effective against real threats.

The practices described in the sources show that the results of the proper detection of threats using multi-agent-based systems are steadily increasing as the percentage of false alarms drastically decreases. Undoubtedly, multi-agent-based approaches can potentially reach increased flexibility, which will make them even more popular in the near future. Therefore, the experimental model created at the first stage of the project is a combination of multi-agent system and IDPS [17, 18, 19, 20].

Autonomous agents are computing systems that exist in a complex, dynamic environment, act independently in this environment, and thus realize a set of goals and tasks for which they are designed. The Agents have the following main features:

- autonomy - the ability of an agent to act independently without the direct intervention of people or other agents and to have control over their own actions and inner states;
- sociality - interact with each other using a communication language;
- reactivity - perceives the environment and responds promptly to the changes that occur in it, and
- pro-activity - not just acting in response to their environment but being able to exhibit targeted behavior (manifestation of initiative).

Additional features of the agents are:

- communicability - interfaces to users and other agents, in particular collaborative agents;
- continuity - continuous and repeated execution of functions, it does not apply to all types of agents;
- mobility - nodal migration (even in case of low code mobility), not for all – e.g. agents for extracting information from distributed document systems;
- adaptability - evolution of reactions at the same environmental parameters, does not apply to all types of agents;
- self-learning - behavioral change based on previous experience;
- target orientation – actions does not just in response to the environment, but to achieve a goal;
- flexibility - actions are not following some scenario.

For the purposes of the experimental model, agents from the Learning Agents class are used. Owing to their learning, they are capable to work independently in an originally unknown environment and become more competent than their initial knowledge.

The learning agents consist of four conceptual elements:

• learning element - responsible for making improvements and upgrades, uses feedback from criticism of how the agent manages and determines how the implementation element should be changed to better perform in the future;

• performance element - responsible for the choice of external activities;

• critic - tells the trainer how well the agent is doing in terms of a fixed standard of performance; this success factor is external to the agent, he should not change it to adjust his indications to his own behavior.

• problem generator - responsible for proposing actions that will lead to the accumulation of new and informative experiences.

For our experiment a tentative system named as Network Gateway Monitoring System (NGMS) (Fig. 4) have been built. This is a multi-agent-based software framework, which consists of two parts - Network Prevention (NP) and Host Prevention (HP). The NP component works on the transport layer of the TCP / IP model, and checks the network traffic for detecting and preventing malicious packets and infiltration traces. The HP component works on t he application layer of the TCP / IP model and the System Software layer of the operating system, and inspect the operation of the operating system and kernel activity to detect and prevent malicious code.

The experiments have been successfully conducted to verify and evaluate individual components and the entire platform. The proposed system succeeds in detecting attacks and malicious code that target the protected system with high accuracy and real-time. The NP component manages to characterize the normal behavior of the TCP \ IP protocol and to detect the attacks aiming to break the header of the packets. The HP component proved its high ability to protect against malicious code that affects Windows operating systems, no matter if the malicious code is in the kernel or focused on us er activity.

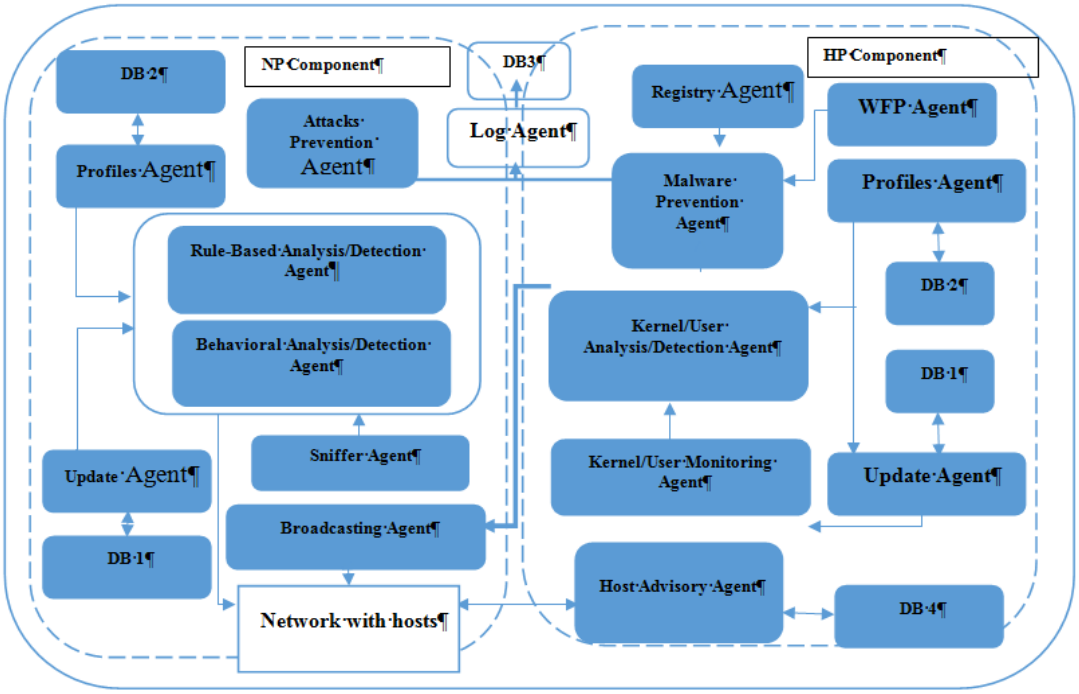

Fig. 4 *The experimental Network Gateway Monitoring System*

The system described below has the following features and capabilities as a solution for threat protection in the network:

• protection against attacks and malicious code - the interaction between NP and HP within the proposed system provides proactive protection of endpoints from attacks and malware as a requirement for e-Business needs;

• significant reduction of false positives and false negative events - the use of behavioral data analysis techniques in system basics and normal behavior profiles eliminates much of false positives and false negative alarms;

• real-time, high performance and flexibility;

• detection of threats in early stage - the implementation of an in-depth defense strategy allows the detection and blocking of threats at an early stage;

• easy profile building - the use of behavioral data analysis techniques eliminates the need to use a large amount of information for training and building normal profiles, as in case of anomaly-based techniques;

• no need for a signature database of the different types of viruses, trojans and malicious code - the NP component is able to record and update the information automatically, depending on the result of the analysis;

• registering and recording of the events in real-time so that experts at a later stage can analyze the characteristics of abnormal network traffic behavior.

5 Methods of Artificial Intelligence Suitable for Operational Cyber Threats Intelligence in Economics

The ultimate goal of Operational Cyber Intelligence is to reduce risk to an organization's critical mission in economics and assets by: defining the operating environment; describing the impact of the operating environment; evaluating the adversary; and determining potential adversarial courses of action (COA). The Operational Cyber Intelligence provides a thread that links the probability and impact of a cyber attack with its strategic level implications by ensuring a coherent framework for analysis and prioritization of potential threats and vulnerabilities given the organization's threat environment. Operational Intelligence is based on the Doctrine of Active Defense. Instead of searching for information regarding a specific attack against the organization in economics, it focuses on analyzing the opponents' combat doctrines, weapon systems and attack and operational scenarios. This approach shifts the center of gravity to the ability to respond and block the outcome of the attack within the organizational environment or in its immediate vicinity.

Our main idea is that the basis for the automation of the Operational CTI can be the behavioral model of the likely adversary. It should be emphasized that the problem of using artificial intelligence methods in the Operational CTI is a completely new matter, and systematized literary sources have not yet been found. Only, there are reports concerning the use of

behavioral analysis based on machine learning by the companies: Exabeam (USA), Darktrace (UK), CyberX (USA), Interset (Canada).

The TU-Sofia team concluded that the activity and the outgoing traffic in the network of the supposed adversary were to be the main source of information for building his behavioural model. This evokes analogies with the non-invasive brain - computer interface whereby the physiological signals of the human brain (for example, through Electroencephalograms (EEGs)) can be used for human emotions evaluation [21].

Indeed, the streams of measured parameters received by different IP addresses of the monitored object using RFC 1757 Remote Network Monitoring methods [22] can be compared to EEG with n-number of channels.

If this analogy is applied in practice, first of all, on the order of the classification model of emotions [23], a basic classification of the behavior of the possible adversary, based on the needs of our research, must be constructed,. Currently, in the absence of references for such studies, it is assumed that this behavior can be divided for the present into two basic types: hostile and non-hostile.

In order to obtain the best possible performances, it is necessary to work with a smaller number of values which describe some relevant properties of the data retrieved from the network. These values are known as “features”. Features can be aggregated into a vector known as “feature vector”. Thus, feature extraction can be defined as an operation which transforms one or several signals into a feature vector. Identifying and extracting good features from signals is a cr ucial step, because otherwise the classification algorithm will have trouble identifying the class of these features, i.e., the behavioral state of the possible adversary. According to some researchers [24], it seems that the choice of a proper pre-processing and feature extraction method have more impact on the final performances than the selection of a good classification algorithm.

Therefore, following the analogy of the brain-computer interface, two basic tasks have to be solved:

- to find a suitable approach to selecting characteristics from which to derive features suitable for behavioral interpretation and validation. In doing so, the necessary inter-subject discrimination of the features for the subsequent classification must be ensured;
- to build and optimize an ensemble of classifiers based on trained models to be used to assess behavior.

According to the researcher's scenario, design of the system of assessing the behavior of the supposed adversary can consist of two main phases: 1) offline training phase to calibrate the system and 2) online phase which uses the system to recognize the type of behavior states and translate them into the computer commands. Both offline and online phases follow a closed-loop process, generally composed of six steps:

a) network activity measurement- this step consists in network surveillance of broadband Internet traffic (e-Mails, Web traffic, instant messengers, etc.) using methods such Packet Capture Appliances in

order to obtain signals reflecting the opponent’s intentions;

b) preprocessing - this step consists in cleaning and denoising input data to enhance the relevant information embedded in the signals;

c) feature extraction – this extraction aims at describing the signals by a few relevant values called “features”;

d) classification - this step assigns a class to a set of features extracted from the signals, which corresponds to the kind of behavioral state identified. This step can also be denoted as “feature translation”. Classification algorithms are known as “classifiers”;

e) translation into a command/application - once the behavioral state is identified, a command is associated with this state in order to control a given application.

Once the data have been acquired, they are pre-processed to clean (de-noise) the signals and to enhance relevant information embedded in these signals. The pre-processing step aims at increasing the signal-to-noise ratio of the input signals.

To perform this pre-processing, various spatial-spectro-temporal filters can be used. Naturally, numerous other pre-processing methods, which are more complex and more advanced, have been proposed and used. But in our initial experiments were based on two of the most popular methods, namely, Independent Component Analysis (ICA) and Common Spatial Patterns (CSP) method.

Based on a study of literary sources, the Echo State Network (ESN) method was proposed as a mechanism for feature selection – this is a class of recurrent neural networks where the so-called “reservoir computing” approach for training is formulated [25]. The main advantage of the ESN is the simplified training algorithm since only weights of the connections from the reservoir to the readout neurons are subject to training [26]. Thus instead of

gradient descent learning much faster least squares method can be used.

We started on the presumption that using reservoir computing pre-training is beneficial for selecting the
most relevant discriminative features and reaching state-of-the-art performance for subject independent recognition. The reservoir computing approach could be used not only for time series processing but also for high dimensional static data representation. Finally, the existing practice shows that IP-trained ESNs outperform pre-trained deep auto-encoders and can actually achieve almost 100% testing accuracy.

Exploring the feasibility of training cross-subject classifiers, we have settled on the Sequential Feature Selection (SFS) procedure [27] that reduces the inherent data variability and can lead to a high inter-subject behaviour status recognition accuracy. Starting from an empty set, SFS increments sequentially a n ew feature that best predicts the class at the current iteration. The process stops when there is no more improvement in the prediction. SFS is a v ery effective way to identify the dominant behavioral signatures across subjects. However, it is a computational heavy and time-consuming procedure, which was the main motivation to look for a computationally less intensive alternative.

As experiments are in their early stages, it is necessary to point out that the results are encouraging, but it is still too early to declare any definitive conclusions.

6 Conclusion

As can be seen from the above, the process of introducing Artificial Intelligence methods at the different levels of Cyber Threat Intelligence is at very different stages: while in Tactical Intelligence, it has long gone out of the phase of research and experiments and is used for building real effective systems in business, In the field of Operational Intelligence, these studies are in a very initial phase and require the commitment of substantial resources. Furthermore, the question arises as to the application of possible outcomes of Operational Iintelligence in the activity of Tactical Intelligence systems in economics, which are intended to neutralize the immediate threats to computer systems and networks.

Further applications in business and economics of the described artificial intelligence methods for network and information security are foreseen.

Acknowledgment

This research is conducted and funded in relation to the execution of a sc ientific-research project № H07/56 “Increasing the level of network and information security using intelligent methods” under the contract with National Science Fund in Bulgaria.

References:

[1] *ENISA Threats Landscape Report* 2016: 15 Top Cyber-Threats and Trends, January 2017

[2] [2] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion* Kill Chains Lockheed Martin Corporation 2015

[3] Republic of Bulgaria: *National Cyber Security Strategy “Cyber Resilient Bulgaria 2020”* 2016-03 NCSS Bulgaria final draft v 5 3

[4] *Cyber Intelligence: Setting the Landscape for an emerging Discipline, Intelligence and National Security Alliance* (INSA), 2011

[5] *Operational Level of Cyber Intelligence*, INSA, 2013

[6] *Operational Cyber Intelligence*, INSA, 2014

[7] Brian P. Kime *Threat Intelligence: Planning and Direction*, SANS Institute, 2015

[8] *Advanced cyber-security intelligence,* Quocirca, 2012

[9] Michael Luck, Peter McBurney, Christ Preist *Agent Technology: Next Generation Computing*, AgentLink II, January 2003

[10] S. D. Chi, J.S. Park, K.C. Jung and J.S. Lee Network Security Modeling and Cyber Attack Simulation Methodology, *Lecture Notes in Computer Science*, Vol. 2119, 2001

[11] V. Gorodetski, O. Karsayev, I. Kotenko, I. Khabalov Software Development Kit for Multi-Agent System Design and Implementation, *Lecture Notes in Artifical Intelligence*, Vol. 2296, Springer Verlag, 2002

[12] Molesini, A., Omicini, A., and Viroli, M. Environment in agent-oriented software engineering methodologies, *International Journal on Multiagent and Grid Systems*, 2007

[13] G. Gai, L. Rui, H. Wu, X. Hu An Improved Collaborative Method for Recommendation and Rating Prediction, IEEE International Conference on Data Mining Workshop, 2014

[14] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez.*An Architecture for Intrusion Detection using Autonomous Agents*, Purdue University West Lafayette, 2007

[15] Taraka D. Peddireddy *Multiagent Network Security System using FIPA-OS*, University of South Carolina, 2011

[16] D. Dasgupta, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsettii CIDS: *An agent-based intrusion detection system*, The University of Memphis, 2014

[17] Trifonov R., Manolov S. Tsochev G. Application of multi-agent systems for network and information protection, 28th International Conference on Information Technologies (Info-Tech 2014), Varna, Bulgaria

[18] Tsochev G, Trifonov R., Yoshinov R. Multi-agent framework for intelligent networks, 29th International Conference on I nformation Technologies (Info-Tech 2015), Varna, Bulgaria

[19] Tsochev G, Trifonov R., Naydenov G. Agent Communication Languages Comparison, 7th International Scientific Conference COMPUTER SCIENCE'2015, Durres, Albania

[20] Tsochev G, Trifonov R., Popov G. A Security Model based on M ulti-agent systems, 30th International Conference on I nformation Technologies (Info-Tech 2016), Varna, Bulgaria

[21] Liu Y., Sourina O. and Nguyen M. K. Real-time EEG-based human emotion recognition and visualization, Proceedings of the Int. Conf. on Cyberworlds (CW '10), Singapore, 2010

[22] RFC 1757 R emote Network Monitoring Management Information Base, Carnegie Mellon University, February 1995

[23] L. Bozhkov, P. Georgieva Classification models of emotional biosignals evoked while viewing affective pictures, International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH), Vienna, 2014

[24] Hammon P.S. and Sa V.R. de Preprocessing and meta-classification for brain-computer interfaces*, IEEE Transactions on Biomedical Engineering*, 54(3), 2007.

[25] Lukosevicius M. and Jaeger H. Reservoir computing approaches to recurrent neural network training, *Computer Science Review*, vol. 3, 2009

[26] Koprinkova-Hristova P., Bozhkov L. and Georgieva P. Echo State Networks for feature selection in affective computing *13th Int. Conf. on Practical Applications of Agents and Multi-Agent Systems (PAAMS)*, Spain, 3-5 June 2015

[27] Guyon I. and Elisseeff A. An Introduction to Variable and Feature Selection*, Journal of Machine Learning Research*, vol. 3, 2003

[28] Ljubomir Lazic, Nikos Mastorakis " Cost effective software test metrics " in WSEAS Transactions on C omputers, V olume 7, I ssue 6, pp 599-619

[29] Ljubomir Lazic, Nikos Mastorakis, "Orthogonal Array application for optimal combination of s oftware defect detection techniques choices" in WSEAS Transactions on Computers, V olume 7, Issue 8, pp 1319 - 1336