IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.9, September 2020 E-ISSN: 2347-2693

Cyber Threats in Artificial Intelligence

Mangoldip Saha[1*], Anirbit Sengupta[2], Abhijit Das[3]

[1]Camellia Institute of Engineering & Technology, Burdwan, India
[2]Dr. Sudhir Chandra Sur Institute of Technology & Sports Complex, India
[3]RCC Institute of Information Technology, Kolkata, India

**Corresponding Author: sahamangoldip@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v8i9.4347 | Available online at: www.ijcseonline.org

Received: 31/Aug/2020, Accepted: 12/Sept/2020, Published: 30/Sept/2020

***Abstract*—** In the state of affairs of Digital Security there has been an alternate from the vicinity of Digital Guiltiness to the part of Digital War in the route of the most present day couple of years. As indicated by the new difficulties, the master network has two principle draws near to embrace the way of thinking and techniques for Military Insight, and to utilize Man-made brainpower strategies for balance of Digital Assaults. This paper portrays a portion of the outcomes got at Specialized the American College of Sofia in the usage of undertaking identified with the use of insightful techniques for expanding the security in PC systems. The investigation of the achieve ability of different Man-made reasoning strategies has demonstrated that a technique that is similarly successful for all phases of the Digital Knowledge can't be distinguished. While for Strategic Digital Dangers Knowledge has been chosen and examined a Multi-Specialist Framework, the Repetitive Neural Systems are presented for the necessities of Operational Cyber Threats Artificial Intelligence.

***Keywords*—**Remote Network Monitoring, Artificial Intelligence, Sequential Feature Selection, Behavioral Assessment, Cyber Threats Intelligence Neural Networks.

I. INTRODUCTION

Over the previous couple of years, the inclinations of transition of the Cyber Threats from the Cyber-Crime area to the Cyber- War area has conjointly added on confederate diploma adequate transition of Cyber Defense methods to navy technological know-how [1]. 1st of all, this troubles the appreciation interior the assessment of the threats of the questionable "Cyber Kill Chain" model, in a same way due to the reality the utility of historic Military Intelligence Technology.

Furthermore, inner the stipulations anywhere well-resourced and expert adversaries habits Multi-year intrusion campaigns targeting touchy economic, proprietary, or united states good sized safety data, the local safety techniques that leverage archives regarding these adversaries will produce confederate diploma Genius electric powered circuit, sanction native defenders to determine a kingdom of facts superiority that decreases the adversary's likelihood of success with every and each and every ensuing intrusion try. That's why in holding with the overwhelming majority of consultants, the qualitative transition to New Cyber Defense tools need to include the magnificent use of computing strategies to look at information changed, community flows, sources of threats, and to set up super have an impact on measures, jointly with proactive ones.

Following these trends, the university of PC Systems and Technology at Technical University of Serbia started out evaluation on the making use of clever strategies for developing the safety in laptop computer pc networks. A critical location of this investigation is dedicated to the Cyber Threat Intelligence. This article summarizes some consequences of a quest done by way of way of the mission team.

II. BASIC FEATURES OF THE CYBER THREATS

- The Cyber Intelligence or, more precisely, Cyber Threats Intelligence (CTI) has the following definition in the draft Bulgarian National Cyber Security Strategy [2]:
- Establishment of mechanisms and technical means to preserve an updated image of feasible threats of unique scale, sources and character, trends in geopolitical Context development and applicable country wide cyber picture analysis and;
- Developments of competencies to assist discover attribution sources and take appropriate types of protection and counteraction.

According to the archives of INSA (Intelligence and National Security Alliance) [3, 4, 5] the guidance of the talent in cyber operational surroundings is a systematic and non-stop method of analyzing plausible threats to become aware of a suspicious set of activities that may also endanger systems, networks, information, employees, or customers by using presenting skill to visualize and consider a number of precise penetration sensor inputs to deliver up a precise threat. This technique helps the organization's chance management approach and decision-making in the place of records security. Its application identifies possible threats and assists protection and hazard

managers selectively put into effect and maximize Deep protection techniques via higher understanding the ease entail points in time and space in the running environment. The Cyber Threats Intelligence Cycle [6] is a systematic, non-Stop method of inspecting manageable threats to notice a suspicious set of things to do that might threaten the organization's systems, networks, information, employees, or customers through providing a capability of visualizing and assessing a number of particular intrusion sensor inputs and open source statistics to infer precise hazard guides of action. The model helps the organization's risk management strategy and the facts protection group's decision- making. The utility of the mannequin identifies conceivable risk courses of motion and helps the Security and danger management leaders selectively follow and maximize a defense in depth strategy with the aid of a higher appreciation of the organization's cyber threats at imperative points in time and house in the operational surroundings 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

The following figure is a graphical representation of the Cyber Threat Intelligence Cycle.

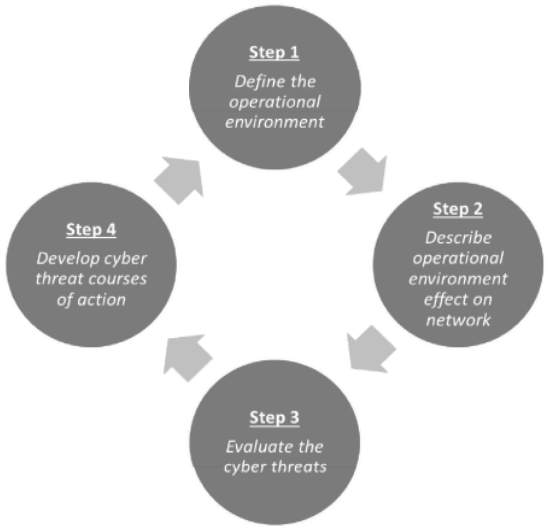

Fig. 1. Cyber Threat Intelligence Cycle

Like its army analogue, the Cyber Threats Intelligence is developed at three levels: strategic, operational, and tactical. For the functions of this study, the 2nd one is considered: INSA defines [5] the operational degree as: "The stage at which campaigns and primary operations are planned, conducted, and sustained to gain strategic targets inside theaters or different operational areas. At this level, actors construct the capabilities wanted to aid the tactical operations. They maneuver in our on-line world to position functionality where they want to in order to be tremendous in their tactical missions. At the operational level, an organization's running environment can be described in terms of physical, logical, records and social layers".

III. METHODS OF AI IN SECURITY

The essence of Artificial Intelligence (AI) is based totally on the declaration that people's brain (the achievable (inborn) capacity of a conscious character to conclude on given information) can be described so exactly that it is machine- simulated. After numerous decades of research, AI is now not only the challenge of lookup or planning of some movement, but also of more complex and interdependent solutions. Artificial Intelligence is defined as the brain displayed with the aid of machines and / or software. This is a tutorial area of learn about exploring the goal of creating intelligence. The important problems explored by using AI consist of reasoning, information presentation, computerized planning and scheduling, computer learning, natural language processing, computer vision, robotics and common intelligence.

AI permits us to enhance self-reliant laptop 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 discipline of lookup that focuses on improving cyberspace safety measures.

With rapid pace of improvement and the wish for more high quality countermeasures, Artificial Intelligence comes as a herbal answer to the hassle of coping with the ever- growing number of network attacks. Applications in the subject of AI are widely prevalent via the cutting-edge information society. This interdisciplinary endeavor has created a joint link between pc experts and community Engineers in designing, simulating and developing network penetration patterns and their characteristics.

As stated in the introduction to this article, world exercise has already noted a giant range of more than a few Artificial Intelligence applications in laptop security. Without making an attempt for a comprehensive classification, we may want to divide these techniques into two most important directions:

A. Conditionally named "distributed" methods:
A1. Multi-Agent Systems of Intelligent Agents;
A2. Neural Networks;
A3. Artificial Immune Systems and Genetic Algorithms.

B. Conveniently named "compact" methods:
B1. Machine Learning Systems, including: associative methods, inductive logic programming, Bayes classification;
B2. Pattern Recognition algorithms; B3. Expert Systems;
B4. Fuzzy Logic.

Having into account this range of methods, it is of specific importance that enough standards are selected for the assessment and determination of precise software for each precise solution. In the above mentioned project, the specification was carried out for two of the fundamental sections of CTI. It ought to be stated here that inside the

task the application of Multi- Agent structures used to be chosen and experimented as the most terrific technique for the wishes of the Tactical Cyber Intelligence.

IV. METHODS OF AI FOR OPERATIONAL THREATS

The ultimate intention of Operational Cyber Intelligence is to minimize chance to an organization's imperative mission and belongings by: defining the operating environment; describing the impact of the working environment; evaluating the adversary; and figuring out workable adversarial publications of action certificate of analysis (COA). The Operational Cyber Intelligence presents a thread that hyperlinks the probability and influence of a cyber-attack with its strategic degree implications by using making sure a coherent framework for analysis and prioritization of workable threats and vulnerabilities given the organization's risk environment. Operational Intelligence is based totally on the Doctrine of Active Defense. Instead of searching for records concerning a precise assault against the organization, it focuses on inspecting.

The opponents' fight doctrines, weapon structures and assault and operational scenarios. This method shifts the middle of gravity to the capacity to respond and block the outcome of the attack within the organizational environment or in its immediate vicinity.

Our essential concept was that the foundation for the automation of the Operational CTI can be the behavioral model of the probable adversary. It must be emphasized that the problem of the use of artificial brain techniques in the Operational CTI is a absolutely new matter, and systematized literary sources have not yet been found. Only, there are reviews regarding the use of behavioral evaluation based on computing device studying by the companies: Exabeam (USA), Darktrace (UK), CyberX (USA), Interset (Canada). The TU-Sofia crew concluded that the exercise and the outgoing traffic in the network of the supposed adversary have been to be the fundamental source of facts for constructing his behavioral model. This conjures up analogies with the Non- Invasive Brain - Computer Interface whereby the physiological signals of the human intelligence (for example, thru Electroencephalograms (EEGs)) can be used for human feelings contrast [7]. Indeed, the streams of measured parameters obtained by using n-number exclusive IP addresses of the monitored object the use of RFC 1757 Remote Network Monitoring methods [8] can be in contrast to EEG with n-number of channels.

If this analogy is utilized in practice, first of all, on the order of the classification model of feelings [9], a fundamental classification of the behavior of the possible adversary, primarily based on the desires of our research, should be constructed. Currently, in the absence of references for such studies, it is assumed that this behavior can be divided for the existing into two fundamental types: hostile and non- hostile.

In order to reap the best viable performances, it is fundamental to work with a smaller number of variables which describe some relevant properties of the records retrieved from the network. These variables are recognized as "features". Features can be aggregated into a vector regarded as "feature vector". Thus, feature extraction can be described as an operation which transforms one or several indicators into a characteristic vector. Identifying and extracting precise features from signals is a vital step, due to the fact otherwise the classification algorithm will have hassle identifying the class of these features, i.e., the behavioral state of the possible adversary. According to some researchers [10], it looks that the preference of a proper pre-processing and characteristic extraction approach have extra influence on the remaining performances than the determination of a excellent classification algorithm [16].

Therefore, following the analogy of the Brain-Computer Interface, two simple duties have to be solved:

1 To discover a suitable approach to choosing characteristics from which to derive facets suitable for behavioral interpretation and validation. In doing so, the indispensable inter-subject discrimination of the aspects for the subsequent classification need to be ensured;

2 To build and optimize an ensemble of classifiers based on skilled fashions to be used to assess behavior.

According to the researcher's scenario, layout of the system of assessing the behavior of the supposed adversary can consist of two foremost phases:

1) offline coaching section to calibrate the device and
2) online segment which uses the machine to apprehend the type of conduct states and translate them into the laptop commands. Both offline and on line phases observe a closed-loop process, normally composed of six steps:

a) Network pastime measurement- this step consists in community surveillance of broadband Internet site visitors (E-Mails, Web traffic, immediate messengers, etc.) using methods, such Packet Capture Appliances Fig. 2 in order to Acquire signals reflecting the opponent's intentions [11];
b) preprocessing - this step consists in cleaning and demising input information to beautify the relevant facts embedded in the signals;
c) Feature extraction – this extraction pursuits at describing the signals with the aid of a few relevant values knownas "features";

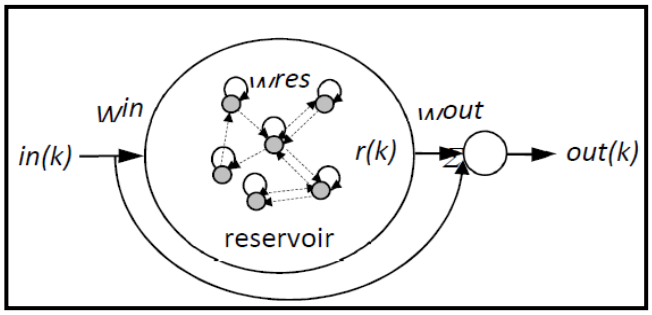

Fig. 2. Packet Capture Appliances

Classification - this step assigns a classification to a set of aspects extracted from the signals, which corresponds to the kind of behavioral country identified. This step can additionally be denoted as "feature translation". Classification algorithms are known as "classifiers" [15];
b) Translation into a command/application - once the behavioral country is identified, a command is related with this kingdom in order to manipulate a given application. Once the records have been acquired, they are pre-processed to smooth (de-noise) the alerts and to decorate applicable information embedded in these signals.

The pre-processing step objectives at increasing the signal-to-noise ratio of the enter signals. To perform this pre-processing, a range of spatial- spectro-temporal filters [10] can be used. Naturally, numerous different pre-processing methods, which are more complex and more advanced, can be proposed and used. But in our initial experiments we have been 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) technique was once proposed as a mechanism for feature determination – this is a type of Recurrent Neural Networks where the so-called "Reservoir Computing" method for coaching is formulated [12].

The basic structure of an ESN, presented in Fig. 3, consists of a reservoir of random connected dynamic neurons with sigmoid nonlinearities (usually hyperbolic tangent):
r(k) = f res(W inin(k) + W resr(k-1))
and a linear readout *f out* (usually identity function) at the output:
out (k) = f out (W out [in (k) r (k)])

Here *k* denotes discrete time instant; *in(k)* is a vector of network inputs, *r(k)* - a vector of the reservoir neurons states and *out(k)* – a vector of network outputs; *nin*, *nout* and *nr* are the dimensions of the corresponding vectors *in*, *out* and *r* respectively; *W out* is a trainable *nout* (*nin*+*nr*) matrix;

W in and *W res* are *nr nin* and *nr nr* matrices that are randomly generated and are not trainable. In some applications, direct connection from the input to the readout is omitted.

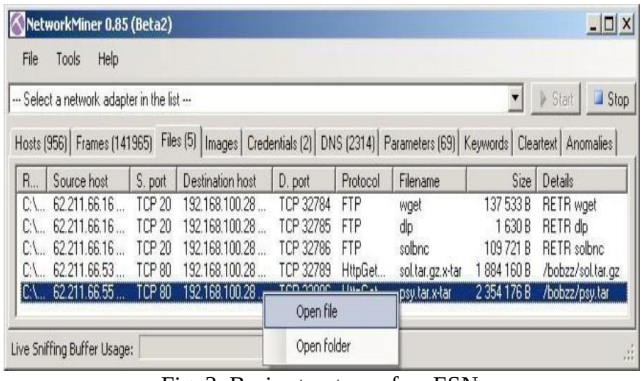

Fig. 3. Basic structure of an ESN

The important gain of the ESN is the simplified education algorithm since only weights of the connections from the reservoir to the readout neurons are concern to coaching [13]. Thus as a substitute of gradient descent getting to know an awful lot quicker least squares approach can be used.

We commenced on the presumption that the usage of reservoir computing pre-training is really useful for choosing the most relevant discriminative facets and achieving contemporary performance for issue unbiased recognition. The Reservoir Computing approach may want to be used no longer only for time sequence processing but also for excessive dimensional static records representation. Finally, the current exercise suggests that IP-trained ESNs outperform pre-trained deep auto-encoders and can sincerely attain almost 100% checking out accuracy.

Exploring the feasibility of education cross-subject classifiers, we have settled on the Sequential Feature Selection (SFS) manner [14] that reduces the inherent statistics variability and can lead to an excessive inter-subject behavior status cognizance accuracy. Starting from an empty set, SFS increments sequentially a new function that high-quality predicts the category at the present day iteration. The manner stops when there is no more improvement in the prediction. SFS is a very fantastic way to become aware of the dominant behavioral signatures across subjects.

However, it is a computational heavy and time-consuming procedure, which used to be the essential motivation to appear for a computationally less intensive alternative.
The state of the artwork of the works described in this article can be described as a transition from the development of a theoretical model to an experimental setting.

As the experiments are in their early stage, it is imperative to factor out that the consequences are encouraging, but it is still too early to declare any definitive conclusions.

V. CONCLUSION

As can be considered from the above, the system of introducing Artificial Intelligence techniques at the different stages of Cyber Threat Intelligence is at very distinctive stages: while in Tactical Intelligence, it has lengthy long past out of the section of research and experiments and is used for building actual high quality systems, In the area of Operational Intelligence, these research are in a very preliminary section and require the commitment of vast resources. Furthermore, the query arises as to the utility of feasible results of Operational Intelligence in the activity of Tactical Intelligence systems, which are intended to neutralize the immediately threats to laptop structures and networks.

REFERENCES

[1] Elike Hodo, Xavier Bellekens, Ephraim Iorkyase, Andrew Hamilton, Christos Tachtatzis and Robert Atkinson. Machine Learning Approach for Detection of nonTor Traffic. Journal of Cyber Security, Vol. **6.2**, pp **171**–**194**, November **2017**. doi: 10.13052/jcsm2245- 1439.624

[2] [RFC 1757] Remote Network Monitoring Management Information Base, Carnegie Mellon University, 1995

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

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

[5] Koprinkova-Hristova P., Bozhkov L. and Georgieva P., Echo State Networks for feature selection in affectivecomputing

[6] Republic of Bulgaria: *National Cyber Security Strategy "Cyber Resilient Bulgaria 2020",* 2016-03 NCSS Bulgaria final draft v 5 3, Bulgarian government, **2016**

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

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

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

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

[11] L. Bozhkov, P. Georgieva Classification models of emotional bio signals evoked while viewing affective pictures

[12] Erik Hjelmvik, Passive Network Security Analysis with Network Miner, (IN)SECURE Magazine, no. **18**, pp. **18**–**21**,**2008**.

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

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

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

