International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

AI in Cyber Security- A Review

Govind Kumar[1], Dr. R. Chinnaiyan[2]

[1]PG Scholar , Department of MCA, New Horizon College Of Engineering, Bangalore, Karnataka, India
[2]Professor, Department of MCA, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

The speed of processes and the quantity of knowledge used in cyber area can not be handled by humans nor sizeable automation. It is trouble to developed software system with standard algorithm for effectively against the dynamically evolving attacks in networks. When measuring the papers obtainable regarding AI applications in cyber security, we will conclude that helpful applications exist already. Initial of all, to applications of artificial neural nets in security and a few alternative cyber security areas.

Keywords : Cyber Security, Syber Attacks, Artificial Intelligence, Cyber Kill Chain, Integrated Security Approach, Artificial Neural Network

I. INTRODUCTION

Since 1988, when the first denial-of-service (DOS) attack was launched, the sophistication, number, and impact of cyber attacks have increased significantly. As cyber attacks have become more targeted and powerful so have cyber security countermeasures. While the first security tool was limited to spotting signatures of viruses and preventing their execution, today we find solutions that are designed to provide holistic protection against a wide range. Implement resilient and continuous protection, security systems need to constantly adjust to changing environments, threats, and actors involved in the cyber play. Cyber reality, however, appears somewhat different. Security approaches are regularly tailored to known attacks, and due to a lack of flexibility and robustness, security systems typically are unable to adapt automatically to changes in their surroundings. Even with human interaction, adaption processes are likely to be slow and insufficient.

Due to their flexible and adaptable system behavior, artificial intelligence (AI) techniques can help overcome various shortcomings of today's cyber security tools. Although AI has already greatly improved cyber security, there are also serious concerns. Some view AI as an emerging existential risk for humanity. Accordingly, scientists and legal experts have expressed alarm at the increasing role that autonomous AI entities are playing in cyberspace and have raised concerns about their ethical justifiability.

The purpose of this work is to highlight the shortcomings of traditional security measures as well as the progress that has been made so far by applying AI techniques to cyber security. In addition, this work summarizes the risks and concerns linked to this development, by exploring AI's status quo, addressing present concerns, and outlining directions for the future.

II. CHALLENGES OF CYBER SECURITY

Although awareness of cyber threats has increased; large amounts of money has been invested; and efforts are being made to fight cybercrimes, the ability of organizations to sufficiently protect their own virtual assets is not yet known. The involved parties in cyberspace range from single individuals, private organizations, non-state actors to governmental organizations, all aiming to protect their cyber assets, attack those of others, or both. In addition, the sources of cyber threats are manifold: cyber threats basically arise from potential malicious acts due to financial, political, or military reasons.

However heterogeneous and dynamic the nature of cyberspace might be, certain similarities of attacks and their countermeasures can be used to describe and allow for a holistic security framework. Most cyber attacks follow certain attack phases that can be described as a **cyber kill chain**. *This* framework assumes that every attack sequence starts with a **reconnaissance** phase, in which an attacker tries to locate gaps and vulnerabilities of a target system. The **weaponizing** phase follows, during which the uncovered weaknesses are used to develop targeted malicious code. This is followed by the **delivery** phase when the malware is transferred to the potential target. After the malware is delivered successfully, the **exploit** phase occurs during which the malware triggers the installation of an intruder's code. Afterwards, the compromised host system allows the establishment of a command and control channel so that the attacker can initiate malicious actions. Counteractions can be determined depending upon where a malicious action appears in the cyber kill chain.

The **integrated security approach** (ISA) provides key ideas for a holistic view on cyber defense and a framework for such categorization. The main aim of the ISA is to generate **early warnings**, or alarms, preferably before the attack is launched (before the exploit phase).

The alarm is supposed to generate a relevant warning message that translates newly gathered threat data into actionable tasks.By this means, the message further supports the selection of countermeasures or already contains dedicated counteractions to prevent organizations from being victims of an attack. If an intrusion can not be prevented in advance, the extent of the attack must be detected, followed respectively by reaction and response. These measures should include actions to stop or counterattack the invader, in addition to defining recovery procedures to quickly rollback the system to its initial state.

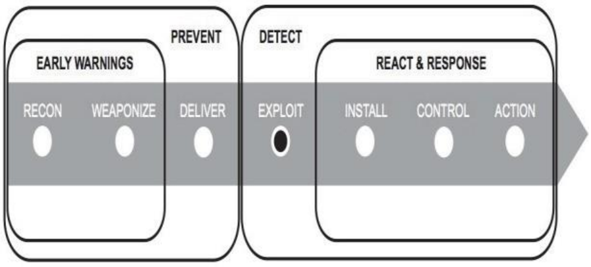

Figure 1. Cyber kill chain phases encapsulated countermeasures integrated security approach

Figure 1 above depicts the interconnection of cyber attacks, described by the cyber kill chain, with their countermeasures, covered by the ISA. The diagram depicts the cyber kill chain, here visualized as the gray arrow in the center, encapsulated by the ISA. The cyber kill chain includes the seven phases of a cyber attack, whereas the ISA consists of four counteraction phases. For detecting and blocking attacks as early as possible, all attack phases of the cyber kill chain need to be considered within the comprehensive ISA framework. As stated above, the emphasis is on preventing attack and detecting malicious activities during the first three phases of an intrusion, here visualized as recon, weaponize , and deliver on the left side of the diagram within the gray arrow.

After the attack—depicted as exploit in the center of the arrow—the ISA measures detection, reaction, and response necessary to interfere with the compromising malicious activities. The complex and dynamic nature of cyber space leads to various strategic and technological challenges that hinder and complicate an organization's ability to protect itself sufficiently in this virtual environment. These challenges comprise data acquisition, technology driven matters, as well as shortcomings in regulation and process management.

III. CHALLENGES IN GATHERING CYBER INTELLIGENCE

The fact that perpetrators leave tracks when attempting to attack a potential target system is the key to better understanding an attacker. Consequently, an ISA with its holistic view of an organization's security requires gathering and analysis of a range of information for gaining cyber intelligence. There are challenges, however, in acquiring relevant data as well as in processing, analyzing, and using it. Therefore, related efforts to effectively prevent, detect, and respond to malicious intrusions are regularly aided by security tools that aim to automate supporting security processes. The main **challenges in acquiring relevant data tracks** are- Amount of data: The amount of data has increased exponentially since electronic devices and their use has become ubiquitous in our work and daily lives. For the implementation of an ISA, data from all systems across entire organizations may need to be considered. Heterogeneity of data and their sources: The variance in data and its sources makes it difficult to identify and collect those data; moreover, both are spread across organizational and national borders. Even if the relevant heterogeneity within the cyber environment is identified, topology and behavior of systems and networks may change and, thus, require constant adaption.

Artificial Neural Networks to Prevent Malicious Intrusions

Another technique that emerged from the field of AI is the **artificial neural network** (ANN). ANNs are statistical learning models imitating the structure and the function of the human brain. They can help to learn and solve problems, especially in environments where algorithms or rules for solving a problem are difficult to express or are unknown. Since ANNs' system behavior is kind of elusive, they are considered undefined black-box models. In cyber security, ANNs have been used successfully within all stages of ISAs and, hence, can encapsulate all phases of the cyber kill chain. Integrated in cyber security, ANNs can be used for monitoring network traffic. As depicted in Figure 2 below, malicious intrusions can be detected already during the delivery phase and before an actual attack occurs. This is a desired goal of cyber security, and it is a great achievement when cyber attacks can be hindered before they take place, thus, elaborating upon the main idea of perimeter defense. ANNs can be successfully used to learn from past network activities and attacks in order to prevent future attacks from actually transpiring.

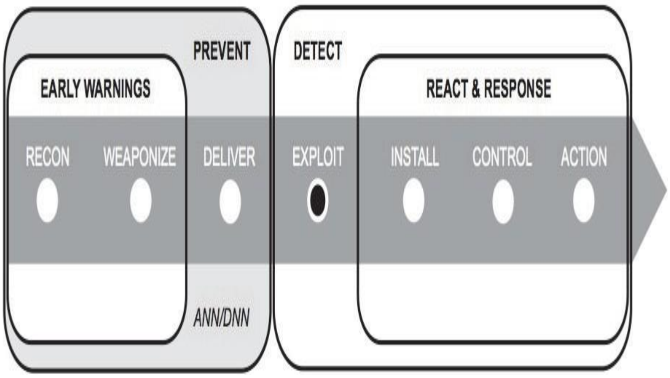

Figure 2. Artificial Neural Networks to Prevent Attacks within an Integrated Security Approach

Compared to conventional techniques used for cyber defense, the great advantage of using ANNs is their learning ability. As mentioned above, patterns that describe normal and abnormal network activities are traditionally defined manually by security professionals based on their expert knowledge.

Within an anomaly-based IDPS approach, it was shown that ANNs can be successfully utilized to evaluate header information[37] of network data packages to *learn* patterns for normal network behavior. A first preparatory step, the ANN was trained to identify and learn patterns of header attributes that belonged to normal network traffic. Every future data packet that was transferred over the monitored network was compared afterwards with these pre-learned patterns. When attributes of packet headers matched the *normal* pattern, they were transferred as usual. Irregularities in a data packet's header information that mismatched the learned pattern were classified as malicious and rejected by the IDPS. This dedicated approach has shown that the overall detection rate of attempted intrusions has improved without generating any false positive or false negative alarms. While traditional IDPSs, both signature-based and anomaly-based, work mostly against known intrusions, this ANN approach has successfully protected against instances of intrusions that were previously unknown. In summary, ANNs are said to support a viable approach to building robust, adaptable, and accurate IDPS.

IV. EXPERT SYSTEM

Expert systems are computer programs designed to provide decision support for complex problems in a domain; these are the most widely used AI application. Conceptually, an expert system consists of a knowledge base, which stores the expert knowledge, and an inference engine, which is used for reasoning about predefined knowledge as well as finding answers to given problems.

Depending on the way of reasoning, expert systems apply to different problem classes. A case-based reasoning (CBR) approach allows solving problems by recalling previous similar cases, assuming the solution of a past case can be adapted and applied to a new problem case. Subsequently, newly proposed solutions are evaluated and, if necessary, revised, thus leading to continual improvements of accuracy and ability to learn new problems over time. Rule-based systems (RBS) solve problems using rules defined by experts. Rules consist of two parts: a condition and an action. Problems are analyzed stepwise: first, the condition is evaluated and then the action that should be taken next is determined. Unlike CBR systems, RBSs are not able to learn new rules or automatically modify existing rules. This fact refers to the "knowledge acquisition problem," which is crucial in adapting to dynamic environments.

V. CONCLUSIONS

AI is considered as one of the most promising developments in the information age, and cyber security arguably is the discipline that could benefit most from it. New algorithms, techniques, tools, and enterprises offering AI- based services are constantly emerging on the global security market. Compared to conventional cyber security solutions, these systems are more flexible, adaptable, and robust, thus helping to improve security performance and better protect systems from an increasing number of sophisticated cyber threats. Currently, deep learning techniques are possibly the most promising and powerful tools in the realm of AI. DNNs can predict cyber attacks in advance, instead of solely preventing them, and might lead to a new phase of cyber security. Despite the promising nature of AI, it has emerged as a global risk for human civilization, while the risks and concerns for its use in cyberspace are justified. Here, four major issues can be identified: the lack of AI's full autonomy, concerns about data privacy, the absence of sufficient legal frameworks, in addition to ethical concerns originating from a missing moral code of autonomous decision-making systems. Until now, neither people nor AI alone have proven overall success in cyber protection. Despite the great improvements that AI has brought to the realm of cyber security, related systems are not yet able to adjust fully and automatically to changes in their environment; learn all the threats and attack types; and choose and autonomously apply dedicated countermeasures to protect against these attacks. Cyber security is not only a technological issue; it is also about regulation and the way that security risks are dealt with. It is necessary to integrate any technical solutions, relevant processes, and people into an ISA framework to achieve optimal security performance. In the end, it is still the human factor that matters—not (only) the tools.

VI. REFERENCES

[1]. Prof Enn Tyugu, "Artificial Intelligence in Cyber Defense," in Proceedings of 3rd International Conference on Cyber Conflict [ICCC], 7–lO June, 2Oll Tallinn Estonia, eds. C. Czosseck, E. Tyugu, and T. Wingfield (Tallinn, Estonia: CCD COE, 2011), pp.

[2]. www.techopedia.com

[3]. www.tutorialspoint.com

[4]. www.youtube.com

[5]. My Digital Shield, "A History of Cybersecurity: How Cybersecurity Has Changed in the Last 5 Years," October 5, 2015, http://www.mydigitalshield.com/history- cyber-security-cyber-security-changed-last-5-years/.