ARTIFICIAL INTELLIGENCE: ROLE & IMPORTANCE IN CYBER SECURITY THREATS

Razauddin* & Dr. Leena Bhatia**

** Ph. D. Scholar, Himalayan University, Itanagar, Arunachal Pradesh, India.*

***Research Supervisor, Himalayan University, Itanagar, Arunachal Pradesh, India.*

ABSTRACT:

Usage of machines did not only ensure growth. Still machines are used. In comparison to man machines are easier to handle. One such attempt of man is artificial intelligence. Artificial intelligence thinks and works like a man. It is capable of producing results better than a man. With the use of computers, the problems of cyber security have also increased manifolds. To combat this problem man had started using artificial intelligence. This is how, started the role of artificial intelligence in cyber security threats. This instigated the current research. Here, an effort was made to explore if and to what extent artificial intelligence has played a role in controlling cyber security threats. Based on the conclusions of this research further applied research can be pursued. So the type of research approach adopted in this study is exploratory. In this research the dependence was mainly on secondary data. The conclusion reached was that advanced nations are reaping the effectiveness of using artificial intelligence in controlling cyber security threats. Unfortunately the economically poorer nations are unable to do so.

Key Words: Artificial intelligence, cyber security, threats, computers, cyber terrorism etc.

INTRODUCTION:

There was a time in the history of the human civilization when the world was dependent on manual labor. But gradually the situation started to change with the progress of civilization. It was the introduction of machines that changed the course of time. But usage of machines did not only ensure growth. They also brought with them many complications. Still machines are used and one of the main reasons behind that is that machines do not get tired. Moreover, in comparison to man machines are easier to handle. One such attempt of man is artificial intelligence. Artificial intelligence thinks and works like a man. It is capable of producing results better than a man can produce. Another attempt of mankind to ensure 100% accuracy and save time is the usage of computers. But with the use of computers, the problems of cyber security have also increased manifolds. In order to combat this problem man had the option of using artificial intelligence. It enabled man to use a technology that thinks like man and tries to produce results like man. This is how, started the role of artificial intelligence in cyber security threats.

LITERATURE REVIEW:

Marvin Minsky of Department of Mathematics and Computation Centre, University of Cambridge wrote an article titled "A Selected Descriptor- Indexed Bibliography to the Literature on Artificial Intelligence". It was published in IEEE on March, 1961.

In this article the author wrote that the listing done in this article has been done with the objective of producing an introduction to the literature on the study of artificial intelligence. The author divided this area into categories and cross indexed accordingly. While writing this article the author kept in mind that large biographies without any systematic arrangement are next to useless. The author mentioned specifically that the field of artificial intelligence is relatively young. Not much has been done in this field, yet a lot of time has been wasted in doing the same thing and in rediscovering the same things. That prompted the author to produce a bibliography of literature regarding artificial intelligence.

This article is an absorbing one as it is one of the first research articles written on artificial intelligence. But to make this article even more interesting the author could have written at least a little bit about the expected future of artificial intelligence.

J. McCarthy and P.J. Hayes wrote an article in 1981 on the problems associated with artificial intelligence. This article was titled "Some Philosophical Problems from the Standpoint of Artificial Intelligence".

The authors wrote, "A computer program capable of acting intelligently in the world must have a general representation of the world in terms of which its inputs are interpreted. Designing such a program requires commitments about what knowledge is and how it is obtained. Thus, some of the major traditional problems of philosophy arise in artificial intelligence."

The first part of the paper begins with a philosophical point of view that seems to arise naturally once idea of actually making an intelligent machine is taken seriously. We go on to the notions of metaphysically and epistemo-logically adequate representations of the world and then to an explanation of *can, causes*, and *knows* in terms of a

representation of the world by a system of interacting automata. A proposed resolution of the problem of freewill in a deterministic universe and of counterfactual conditional sentences is presented.

The authors commented, "The second part is mainly concerned with formalisms within which it can be proved that a strategy will achieve a goal. Concepts of situation, fluent, future operator, action, strategy, result of a strategy and knowledge are formalized. A method is given of constructing a sentence of first-order logic which will be true in all models of certain axioms if and only if a certain strategy will achieve a certain goal."

The formalism of this paper represents an advance over McCarthy (1963) and Green (1969) in that it permits proof of the correctness of strategies that contain loops and strategies that involve the acquisition of knowledge; and it is also somewhat more concise.

The third part discusses open problems in extending the formalism of part 2.

This paper would have been very interesting if effort was made from the authors to study the philosophical problems related to artificial intelligence and incorporate them with the real life problems.

James A. Lewis of Centre for Strategic and International Studies wrote an article titled "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". This article was published on December, 2002.

In this article wrote that the internet is a new thing and sometimes new things appear to be more frightening than they actually are. He was of the opinion that cyber weapons were of less value in attacking national power. The author wrote, "To understand the vulnerability of critical infrastructures to cyber-attack, we would need for each target infrastructure a much more detailed assessment of redundancy, normal rates of failure and response, the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. This initial assessment suggests that infrastructures in large industrial countries are resistant to cyber-attack.18 CSIS, 2002 10 Terrorists or foreign militaries may well launch cyber-attacks, but they are likely to be disappointed in the effect. Nations are more robust than the early analysts of cyber terrorism and cyber-warfare give them credit for, and cyber-attacks are less damaging than physical attacks. Digital Pearl Harbors are unlikely. Infrastructure systems, because they have to deal with failure on a routine basis, are also more flexible and responsive in restoring service than early analysts realized. Cyber-attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective. However, if the risks of cyber-terrorism and cyber-war are overstated, the risk of espionage and cybercrime may be not be fully appreciated by many observers."

This article acts as a piece of solace for those who are worried seriously about cyber threats. It is because this article tells us that cyber threats are less dangerous than they are being projected. But nothing has been specifically mentioned here about why the author thinks so. Donation of time and energy to explain the reasons for so would have made this article even more useful and worth reading.

The current U.S. electrical power grid is an out-of-date infrastructure, and the Smart Grid is an upgrade that will add much new functionality to meet customers' new power requirements. Updating a system as complex as the electrical power grid has the potential of introducing new security vulnerabilities into the system. This document

presents a review of the work related to Smart Grid cyber security. The work reviewed is separated into five categories that make up different components of the Smart Grid: Process Control System (PCS) Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis. The Smart Grid is a large complex system, and it still requires a lot of cyber security design work.

A research artilcle titled "Artificial Intelligence Techniques for Cyber Security" was written by Arockia Panimalar, Giri Pai and Salman Khan. It was published in International Research Journal of Engineering and Technology (IRJET). In this digital world, the outburst of IOT and linked devices, cyber security experts face a lot of encounters. The authors wrote that the experts require all necessary arms and ammunitions in the form of technology and training to combat the cyber security threats. The number of attached workplaces lead to heavy traffic, more security attack vectors, security breaches and lot more that the cyber area cannot be handled by humans. Be that as it may, it is hard to create software system with standard mounted algorithms (hard-wired logic on deciding level) for successfully cautious against the powerfully developing attacks in networks. It has turned out to be evident that numerous cyber security issues are additionally settled with progress only procedures of Artificial Intelligence area unit acquiring utilized.

RESEARCH METHODOLOGY:

This research is not based on any previous research. It is a first of its kind. Here, an effort is being made to explore if and to what extent artificial intelligence has played a role in controlling cyber security threats. Based on the conclusions of this research further applied research can be pursued. So the type of research approach adopted in this study is exploratory.

CONCLUSIONS & RECOMMENDATIONS:

In this research the dependence is on secondary data i.e. the data collected from books, research articles, features, opinions expressed by eminent scholars, writers and thinkers on the topic or related topics.

The inner meaning of the secondary data was excavated through analysis and interpretation. While analyzing and interpreting the data, it had to be remembered that the analyzed and interpreted materials must have accuracy and relevance for reaching the research objectives of this particular study. It is only then that proper conclusions can be reached and the research questions can be answered.

In this research the conclusion reached was that usage of artificial intelligence in managing cyber security threats has reduced costs and increased the accuracy manifolds. It has been a big success particularly in technologically advanced nations. However developing countries are yet to reap the effectiveness of artificial intelligence. That is why developing and poor economies are entering a vicious circle. They are unable to afford artificial intelligence in controlling cyber security threats. So cyber security threats are increasing in these countries which are having an adverse impact on their economies. So their economies are not developing. And because their economies are not developing, they are unable to employ artificial intelligence for the said purpose.

REFERENCES:

1. https://ieeexplore.ieee.org/abstract/document/4503297/authors#authors.
2. https://www.sciencedirect.com/science/article/pii/B9780934613033500337.
3. Lewis, James A. (December, 2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: Centre for Strategic and International Studies. P. 1 -12.
4. Green, Paul E., Tull, Donald S. & Alabaum, Gerald (2004). Research for Marketing Decisions, 5th edition, United States, Prentice-Hall.
5. Baumeister, Todd (2010). Literature Review on Smart Grid Cyber Security, P. 23 -30.
6. Panimalar, Arockia, U., Giri Pai & Khan, Salman (March, 2018), Artificial Intelligence Techniques for Cyber Security, International Research Journal for Engineering and Technology, Volume 5, Issue 3, Pg. 122-124.
7. Bhutada, Sunil & Bhutada, Preeti (2018), Applications of Artificial Intelligence in Cyber Security, International Journal of Engineering Research in Computer Science and Engineering, Volume 5, Issue 4, Pg. 214-219.