Array Publishers
Mini Review
Open Journal of Case Reports

The Need to Create a New Model for Predicting Future Cyber Threats and its Parameters

Christos P. Beretas*
Information Technology and Cyber Security, Innovative Knowledge Institute, Paris, France

Corresponding author: Christos P. Beretas, MSc, Ph.D, Information Technology and Cyber Security, Innovative Knowledge Institute, Paris, France. E-mail: cberetas@ikinstitute.org

Received Date: 01 December, 2020; **Accepted Date:** 09 December, 2020; **Published Date:** 15 December, 2020

Abstract

It is well known in computer science that a quantitative analysis can reveal information about a future cyber attacks, combining and analyzing elements that are necessary to carry out the analysis and on the other hand are elements that substantiate the conclusions and the implementation of the appropriate cyber security methods and policies. Quantitative analysis is necessary in critical areas such as "defence" to deal with threats of cyber attacks on critical infrastructure to predict future situations, intruders, while greatly reducing the degree of uncertainty.

Keywords: Quantitative; Threats; Security; Privacy; MAPFCA; Model; Networks

Introduction

Critical strategic infrastructures undoubtedly need to be evaluated at regular intervals against cyber threats, many of them cannot be predicted, there are no easy solutions, all forecasting models have a failure rate as they remain an important tool for assessing asymmetric threats, however this negative point can be bypassed using combinatorial prediction methods, thus compensating for the weaknesses of one method with the other. This article summarizes the reasons why the use of quantitative forecast analysis models are necessary.

Analysis

The prediction of cyber-attacks mainly on critical infrastructures as well as the implementation of the respective security and safety policies presupposes the creation of a model that is able to analyze an existing situation and prevent future cyber-attacks, this article presents the MAPFCA model (Model for Analyzing and Predicting Future Cyber Attacks). The MAPFCA model is a new model presented for the first time in this article. The MAPFCA model uses as an initial source of information that those information are available on the Internet, such as research studies by universities and special purpose organizations located in countries with predominantly aggressive activities. Then the information is analyzed regarding the possibility of operational application of the collected information. Then investigate the effect of the information gathered on the target organization's systems concerned. If the organization interested in implementing the MAPFCA model uses lower technology than the technological information that has been collected and analyzed, then hypothetical scenarios are created for future actions. Finally, according to the exported results, simulations are created so that the stakeholder understands the level of security as well as the level of deterrence. The 5 key points of the MAPFCA model are summarized below

1. Import of information from open sources (Open Source Intelligence, reports, research publications).
2. Analysis of information regarding the possibility of operational application.
3. Investigate the effect of the information collected on the systems concerned.
4. Hypothetical scenarios are created for future actions (under conditions).
5. Simulations so that the stakeholder understands the level of security as well as the level of deterrence.

General forecasting models in the past have shown that general and vague data for analysis have presented problems with ambiguity and erroneous decisions. Choosing a random model for predicting future cyber-attacks may not be able to pinpoint the true size of the problem while reducing inefficiency. Instead, the MAPFCA model was designed exclusively for cyber security, which acts as information in order to reduce uncertainty through decision making not only for the present but also for the future. The MAPFCA model is not a scientific product, it is a piece for predicting and making the right decisions, a complex process that involves both the human factor in the process of collecting information and information systems. It is mainly applied for the making of long-term decisions without excluding direct decisions. It is worth noting at this point that no prediction model is infallible, and the reason is the human factor, the human factor increases both the degree of uncertainty and the degree of inaccuracy [1]. The MAPFCA model uses a method of synthesizing predictions to achieve a common prediction, it is based on an interactive communication between the people involved collecting data while reporting their personal proposals and suggestions to the team coordinator who oversees the whole process. After the data collection and analysis, each collection and analysis team delivers the analysis result to the coordinator, the same continues until all the participating groups present their unchanged data to the coordinator. Then the data are analyzed and the implementation proposal is presented. The whole process is presented as follows.

- Individuals involved in research and analysis.
- Group coordinator.
- Analysis of data from the data of the coordinator.
- Implementation proposal.

The success of the MAPFCA model is based on the following characteristics:

- Selection of an experienced group of people.
- Confidentiality.
- Reliable team of people and coordinator.
- Personal experience regarding cyber security.
- Direct and secure communication of stakeholders.
- The coordinator oversees the whole process, insufficient completion of one-stage leads to a return to the previous one.
- Complete the whole process remotely without a trace.

As it is understood, several of the above processes can be completed electronically and automatically, the collection and analysis of data can be done in real time. As an advantage of the MAPFCA model can be added the ability of people involved in gathering information is made up of people who have the relevant experience, so there is a wealth of personal opinion on what might happen in the future. The evaluation of the information exported from the MAPFCA model focuses on the following:

- Presentation of results regarding the implementation proposals both in short and long term.
- Identifying trends and how existing and future infrastructures are affected.
- Classification of results and processes according to their importance.
- Scenario design and infrastructure simulation in it.
- Impact assessment.
- Evaluation of specificities of the organization concerned.

The choice to be made depends solely on the people involved in the whole process. From the moment that the human factor is involved in the whole process, it signals at the same time that the possible failure of the proposed action plan does not automatically mean the failure of the MAPFCA model. A safe plan of action may seem better but something that may not be the case.

Conclusion

In general, forecasting methods have their advantages and disadvantages, the human factor plays an important role both in the process of gathering and analyzing information and in the process of implementing decisions. The use of artificial intelligence in combination with the reduction of the human factor can bring about valuable predictions while minimizing failure. The MAPFCA model is intended to be used to draw conclusions and make decisions as it presents detailed information, design proposals, implementation proposals, simulation, special proposals, and finally several of the procedures can be applied using artificial intelligence.

What is missing in the current process of risk collection, analysis and assessment and should be explored for the future is the full use of artificial intelligence, preventing entirely human factor which will include the following characteristics.

- Evaluation of similar situations of the past.
- Unlimited search for open information where accessible on the internet.
- Detect and isolate invalid entities (information).
- Search online discussions about specific posts.
- Automatic selection for use of the most optimal application framework.
- Possibility to choose between mild and aggressive actions.
- Presentation of models with the least loss of information in case of cyber-attack.
- Occurrence of failure rate per applicable model of actions.
- Alternative proposals and methods.
- Criteria for alternative actions and methods.
- Balancing security and efficiency.
- Lost in changing environments.
- Transparency of information.
- Elimination of the human factor.
- Long-term reliable strategic planning.
- Overwhelming speed of calculation and waste.

References

1. John W Creswell (2013) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th Edition.