A Literature Review of Cyber Security

Pallavi Murghai Goel, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

***Abstract*: The term cyber security is often employed interchangeably with the term protection of information. This paper argues that while cyber security and information protection are significantly similar, these two terms are not completely comparable. In addition, the paper argues that cyber security stretches beyond conventional information security definitions to include not only the protection of information data, but also that of other properties, including the individual himself. In information protection, reference to the human factor is generally linked to human's role(s) in the process of protection. In cyber security this aspect has a further element, namely, humans as possible targets of cyber-attacks or even engaging unknowingly in a cyber assault. This additional aspect has ethical consequences for society as a whole, as it may be seen as a social obligation to protect such marginalized groups, for example children.**

***Keywords*: *Information security, Cyber security, Cybersecurity, Cyber-Security, Computer security, Risk, Threat, Vulnerability*.**

INTRODUCTION

Cyber security has developed into a topic of global significance and value. More than 50 countries have already officially published some form of strategy paper outlining their official stance on cyberspace, cybercrime and/or cyber security. Cyber security is used, in most literature, as an all-inclusive term. Definitions of this word differ, e.g. the Merriam Webster dictionary defines it as "measures taken to protect a device or computer network from unauthorized access or attack" The International Telecommunications Union (ITU) describes the following for cyber security. Cybersecurity is the array of resources, procedures, security principles, safety protocols, rules, risk management strategies, activities, training, best practices, compliance, and technology that can be used to secure the cyber environment and the properties of the company and user. Assets of the organization and user include connected computing devices, staff, equipment, software, utilities, telecommunications networks, and the entirety of information exchanged and/or processed in the cyber world.

Cybersecurity seeks to ensure that the security resources of the company and the assets of users are obtained and protected against specific physical threats in the cyber world. The general safety targets include the following: Availability, Integrity, which may include authenticity and nonrepudiation, Confidentiality. Those meanings are somewhat similar to information security concepts. This paper would discuss in detail the meaning of information security and then suggest that in terms of how it is traditionally defined, the limits of cyber security as a concept are broader than those of information protection. This paper will concentrate primarily on the fundamental nature of security in general and seek to illustrate, through examples that the purpose of cyber security assets is to protect an additional dimension that stretches beyond traditional information security boundaries. This paper further argues that all human beings in their personal capacity and society as a whole may be directly harmed or influenced by cyber-security attacks, although this is not generally the case for information security where harm is often indirect. This disambiguation is seen by the authors as a significant addition to the popular body of information and cyber security expertise for the field. Such a body of information in the subject field offers a "foundation for interpreting words and concepts" and thus serves as a "taxonomy of topics applicable to practitioners around the world.". According to Whitman and Mattord, the industry standard has historically been to ensure the confidentiality, honesty and availability of information, which is also known as the CIA triangle of information security. "The security of these three information characteristics is as important today as it has always been, but the CIA triangle model no longer adequately addresses the computer industry's ever-changing climate". A few terms in the descriptions above need to be explored in greater depth. Firstly, it should be clear that the protection of information is not a software or technology but a process. Safety of information according to Wood used to be a purely technical problem. However, as the use of computers and networks grew, the securing method for these computers and networks also had to change in order to expand beyond just the technological. The information protection method can involve the use of some goods, which is not something that can be bought off the shelf. The second important thing to note about the above meanings is that the protection of information is generally interpreted in terms of the properties or characteristics that should

have safe information. These usually include confidentiality, honesty, and information availability but may include additional features.

INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY

Security in Information and Communication Technology (ICT) is about securing the specific technology-based systems in which information is typically stored and/or transferred. The international standard describes ICT protection as all aspects of the confidentiality, honesty, availability, non-repudiation, transparency, accuracy and reliability of information resources. Because information security requires the defense of the information resources underlying it, it can be argued that ICT security is a sub-component of information security.

Consequently, the concept of ICT security is somewhat close to that of information security. However, additional characteristics are added to the description, which could be best defined in this context as services which should be provided by secure information resources. Including non-repudiation, transparency, honesty and reliability, the principle of data security is often referred to as denoting the defense of real data in the information system. Since the definition given in Dhillon includes most of the characteristics in the definition of IT security, and since the security of the underlying data is largely dependent on the overall protection of the information system on which the data resides,, it can be argued that the term data security is in fact used in Dhillon to refer to the same concept as that which ISO/IEC TR 13335-1calls ICT security.

This should be evident from the meanings addressed that there is a distinction between securing the resources for information and securing ICT resources. A safe resource for information may include any organization from which information is obtained or to which it is sent. A secure resource for information technology is a protected repository of information that happens to reside on an IT network. It is also necessary to remember that information alone cannot be considered protected in terms of ICT-based systems unless all of the tools and processes that deal with that information are also protected.

As mentioned above, the first three attributes, confidentiality, honesty and availability, are widely referred to as the CIA triangle model, which since the introduction of the mainframe has been considered the industry standard for computer security. In today's inter-networked business setting, new elements have been added to the concept to meet the security needs of organizations. A clear understanding of the meaning of all of the above is essential for an understanding of information and ICT security, as without the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of the information. All of the above (including the precision, utility and possession of information) play an important role in the security of information and should be considered equally relevant. However, one or more of these characteristics or services may, depending on the nature of the information itself, be more applicable in specific scenarios than other. For example, the accuracy of inflationary statistics is of obvious interest to economists, although the confidentiality of the same data seems to be unimportant because it would certainly allow anyone to access such information.

However, by definition a violation of confidentiality happens only if the information is accessed by an unauthorized party. In this scenario, because everybody would be an authorized recipient of inflationary data, the confidentiality of the information would in effect be maintained. Therefore, maintaining the protection of the information of the organization in an organizational sense is not a case of determining the features or services are appropriate, but rather of correctly identifying the permitted entities and other criteria for any given piece of information. As described above, when analyzing ICT security, it is clear that various threats target related vulnerabilities, and ultimately have a negative impact on ICT infrastructure. It is obvious in this case that the technical infrastructure is considered to be the asset which requires protection. Accordingly, ICT is the asset that is protected in ICT security.

In the case of information security, ICT is the system where information is collected, stored and communicated. In this case, it is a knowledge which is considered to be the asset which requires security. In this case, information and communication technology can be defined as, inter alia, a vulnerability that is targeted by various threats in an attempt to compromise the asset, that is, information. Thus, it is important to note that

information is the asset to be secured when it comes to information security. The following sections will argue that the nature of the threats, vulnerabilities and assets in cyber security differs from that of information security

CYBER SECURITY

As mentioned above, the word cyber security is used interchangeably by several current publications concerned with cyber security with the word information security. If cyber security is synonymous with protection of information it would be fair to conclude that cyber security incidents can also be defined in terms of the characteristics used to identify security of information. Of example, a cyber-security incident may often lead to a violation of confidentiality, credibility or information availability. This is true for most threats related to cyber security that a user and/or organization can face. However, it is this paper's contention that there are cyber security risks that do not form part of the officially established information security spectrum.

LITERATURE REVIEW

Knowing and being ready is the first line of protection against cyber threats and cybercrimes, e.g. by information security training. Training can take two forms, the first is aimed at security professionals and aims to improve understanding of the latest threats and to increase skill levels in defending and mitigating against them. The aim of this paper is to research the idea of a cyber range, and to include a comprehensive analysis of literature covering unclassified cyber ranges and safety test beds [1]. In this review, we establish a taxonomy for cyber range systems and analyze existing literature that focuses on architecture and scenarios, but also capacities, functions, resources etc. In this paper the IoT-based smart grid's risks and future approaches are analysed and focus on forms of cyber threats and include an in-depth of the smart grid's cyber-security environment. In particular, we concentrate on addressing and analyzing vulnerabilities in the network, challenging countermeasures, and requiring protection. We strive to provide a deep understanding of cyber-security vulnerabilities and solutions, and provide a roadmap to future cyber-security research directions in smart grid applications [2].

A cyber security control V&V process model is built in this study to solve the problem, based on the principle of adaptive focusing testing. Additionally a quantitative approach is built to define and prioritize fault-prone information security controls. It has been verified that the model built may provide an additional and more reliable framework for expert subjective judgment [3].This article focus on the importance of different cyber defense standards, and cyber security framework architecture. We discuss security threats, assaults and cyber security measures. Then we discuss the different issues of standardization of cyber security. We also address the national information security policy to secure cyberspace, as well as various government strategies in protecting cyber security. Finally, we have some important guidelines for information security and information safety [4]. This paper discusses the requirements required for the Federal Government's evaluation of cybersecurity policies for the United States Department of Health and Human Services.

The overarching aim of cybersecurity policies and procedures is enabled by compliance with established Federal regulations and standards to protect the operational resources and goals of the United States Department of Health and Human Resources and to encourage best practices of security in the defense of information systems against unauthorized actors and cyber threats [5]. This automation reduces human errors in order processing, and increases order delivery performance. However, attacks from cyberspace, particularly from the Internet, can disrupt that. In this paper, we propose a novel attacker-defender model against an adversary of the quantum response (QR) to protect critical assets by considering the defending budget and the reliance on properties. The protection level of each asset in the solution indicates its desirability to be secured [6]. This paper present a survey of deep learning approaches for detecting cyber security attack, the datasets used, and a comparative analysis.

In particular, we provide an overview of intrusion detection systems focused on deep learning approaches. The dataset plays an important role in intrusion detection, so we define 35 well-known cyber datasets and group such datasets into seven categories: network traffic dataset, electric network dataset, internet traffic dataset,

virtual private network dataset, android device dataset, IoT traffic dataset, and internet link [7]. Machine learning techniques are commonly used in the creation of an intrusion detection system (IDS) for the timely and automated detection and classification of cyberattacks at network and host rates. However, when malicious attacks are continuously evolving and occur in very large quantities requiring a scalable solution, several problems come up. There are numerous databases of malware publicly accessible for further study by the information security community [8]. The ultimate goal of this study is to automatically and efficiently learn useful feature representations from large quantities of unlabeled raw network traffic data by using deep learning approaches. We propose a novel intrusion model for the network by stacking dilated convolutionary auto encoders and testing our approach on two new datasets for intrusion detection. Several studies have been carried out to test that our method is successful[9]. This paper develop the detection engine with multiple advanced deep learning models and performing a quantitative and comparative evaluation of these models, we research the feasibility of off-line deep learning based NIDSes. First we present the general technique of deep learning and its theoretical consequences for the issue of network intrusion detection. We then analyze several machine learning solutions for two tasks of network intrusion detection [10].

CONCLUSION

This paper examined the meanings of both the security of information and ICT. The paper then argued that cyber security is distinct from information security, despite sometimes being used as an equivalent concept for information security. Information security is information defense, which is an advantage, against potential harm resulting from various threats and vulnerabilities. At the other hand, cyber security is not only the defense of cyberspace itself, but also the safety of those operating in cyberspace, and all of their properties that can be accessed via cyberspace. This paper argues that while cyber security and information protection are significantly similar, these two terms are not exactly comparable. In addition, the paper argues that cyber security reaches beyond conventional information security boundaries to include not only the protection of information resources, but also that of other properties, including the individual himself. In information protection, reference to the human factor is generally linked to human's role(s) in the process of protection. In cyber security this aspect has a further element, namely, humans as possible targets of cyber-attacks or even engaging unknowingly in a cyber assault.

REFERENCES

[1] M. M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” *Computers and Security*. 2020.

[2] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, 2018.

[3] C. Lee, H. Bin Yim, and P. H. Seong, “Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept,” *Ann. Nucl. Energy*, 2018.

[4] J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Futur. Gener. Comput. Syst.*, 2019.

[5] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, “Cyber security education is as essential as ‘the three R’s,’” *Heliyon*, 2019.

[6] K. F. Cheung and M. G. H. Bell, “Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study,” *Eur. J. Oper. Res.*, 2019.

[7] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” *J. Inf. Secur. Appl.*, 2020.

[8] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, 2019.

[9] Y. Yu, J. Long, and Z. Cai, “Network Intrusion Detection through Stacking Dilated Convolutional

Autoencoders," *Secur. Commun. Networks*, 2017.

[10] J. Yan, D. Jin, C. W. Lee, and P. Liu, "A Comparative Study of Off-Line Deep Learning Based Network Intrusion Detection," in *International Conference on Ubiquitous and Future Networks, ICUFN*, 2018.