International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

The Cyber Warfare and Cyber Security Dynamics

Bhavna Arora
Department of Computer Science & IT, Central University of Jammu, India

***Abstract*—**The contemporary era of digital world has brought about a new category of clear and present danger: the cyber warfare. Since information technology and the internet have developed to such an extent that they have become a major element of national power, cyber war has become the challenge of the day. Cyber security and cyber war are affecting all areas which include academics, politics, business, the military or law and even day to day life. Cyber issues have not only dominated recent headlines, but they have more broadly evolved from a technology matter into an area that needs immediate and special attention. This paper focuses initially on cyber warfare and later discusses the security dynamics of cyber security that encompass the cyber warfare. The dynamics are characterized by the use of information and communication technologies. The paper is of importance in understanding the critical and very important area of cyber security and cyber warfare. The requirements of cyber and information security, the critical area of cyber security and cyber warfare, types of cyber warfare and dynamics of cyber security and cyber warfare are discussed in this paper.

***Keywords*—**Cyber security dynamics; cyber warfare.

I. INTRODUCTION

Computer security, also known as cyber security or IT security, is the security applied to computers, computer networks, and the data stored and transmitted over them [1]. The most crucial and imperative valuable asset of an organization is information. Information is also the key and the critical success dynamic of an organization. So it is imperative to understand that without information security the organization as a whole cannot survive. In fact, all information security controls and safeguards, and all threats, vulnerabilities, and security process are subject to this tenets yardstick [3]. In order to maximize the business opportunities and mitigate potential risks to loss or damage , there is a compulsive need for protection of information. The fundamental requirements of information security are [3]:

1. *Confidentiality*- assurance that information is not disclosed to unauthorized individuals or processes.
2. *Integrity*- ensuring that information retains its original level of accuracy. Information must be accurate and complete, and requires protection from unauthorized, unanticipated or unintentional modification.
3. *Availability*- the timely, reliable access to data and information services to authorized users.
4. *Authentication*-the process of recognizing and verifying valid users or processes and what system resources a user or process is allowed to access.
5. *Non-repudiation*- Non-repudiation is the assurance that the senders or receivers that exchange between the two cannot subsequently be denied by either.

The threats to information are threats to quality, threat to effectiveness and a threat to organizational existence. The Information security tenet is the response to the risks that organizations and nations are facing.

II. THE CRITICAL AREA OF CYBER WARFARE AND CYBER SECURITY

More than guns, bombs or missiles the Internet are the most important tactical tool for terrorist groups today [6]. Technically defined, the cyber warfare is internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems - among many other possibilities [2].

The contemporary times are witnessing a battle ground of computer networks for economic warfare. The role of the computer as a weapon in and of itself magnifies the potential for cyber security that results in the cyber warfare. It can also be defined as "attacking and defending information and computer networks in cyberspace, as well as denying an adversary's ability to do the same" [3].

The key challenges in cyber warfare are :-

1. How the stealing from the devices would be initiated and what defense can be provided?
2. How the information based processes that deal with collection, analysis, and dissemination of information be protected from being attacked and protect the network?
3. How to protect and provide defense to the information and communication systems that collect process, store, transmit, display and disseminate information?

III. TYPES OF CYBER WARFARE

Cyber warfare is of two types - the offensive cyber warfare and the defensive warfare[3].

- *The Offensive Cyber Warfare*

In cyber warfare, the challenge is not only the individuals who may attack our computer systems, but more than 30 nations who have sponsored programs to disrupt information systems worldwide [3]. There are many sources of threats to computer security. Each of the group has different motivations and poses a different type of threat. To effectively resist attacks against its information and information systems, an organization needs to characterize its adversaries, their potential motivations, and their classes of attack [3]. It is a challenge now to really determine the cyber space potential attackers as it is quite difficult to identify them.

Dr. Bhavna Arora, "The cyber warfare and cyber security dynamics ", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 249-251, 2015.

The various identified potential adversaries are national intelligence agencies, competitors, cyber warrior, cyber terrorists, corporate competitors leading to industrial espionage, organized criminal element, insider attackers i.e employees and special case –the hackers. Each of these groups has a special way of working. They have a focused target group and are capable of attacking the organization system in their own way thus achieving their target goal of attacking the network.

- *The Defensive Cyber Warfare*

The key challenge in defensive cyber warfare is that how secure is the perimeter defense i.e what are the steps that can be taken up in order to make the system secure, reliable, scalable and manageable. A defender must be capable of securing and must always succeed in protecting systems. In an initial attack if the attackers do not succeed, it is possible that it may try again later or move on to another target that may be more vulnerable to attack. In all cases a strong defender must continually succeed in order to keep systems up and running, to protect vital information, to maintain their jobs, or to comply with the terms of a security contract.

There are some factors that favor the attackers in the network. Scalability of the network is an important concern that favors the attacker. There are many systems connected in the network through the internet and other ways that it has become almost unworkable to track the number of systems that are connected. Another factor that favors attackers is that they can easily have access to all the systems of the same technology the defender has, as well as technical system information, including weaknesses in hardware and software. However the IT companies today protect their systems and conceal their weaknesses but it is very difficult to defend against any attack as the attacker is quiet clear about the access is known to the vulnerabilities of the system. The release reports and user manuals of the products usually present the kinds of weakness are present in the products. In another scenario the attackers may also join some of the clubs, chat rooms, bulletin boards, and e-mail lists that defenders use to help them obtain information about products or confer with their peers. Individuals can easily assume identities and remain anonymous as they wander the Web seeking out information that helps them develop information warfare attack tactics [3].

IV. THE SECURITY DYNAMICS

In reality the defense of the enterprise against cyber adversaries goes much more beyond the traditional techniques i.e passwords and firewalls. Implacable the cyber threats require continuous monitoring, robust defense and 360° awareness of network activities [5].

The cyber security dynamics emerged based on the dynamics of the nodes of the networks. These dynamics include the security states that change over due course of time that is based on the attacks and defenses of nodes in the network. Based on the dynamics of the nodes in live environment, various models can be build that analyze the security state of the node. A node may be secured at one instance and be unsecured in another instance. The change of state of node may be due to the cyber attack and cyber security thereafter.

The cyber security dynamics deal with the probability of nodes of being compromised at any instance in a network. However this statistics can be used to define security risks in a network and can be used later for implementing the defense mechanism in the network.

Based on the power and potential of the attacks, the cyber security dynamics leads to the variation of defense mechanisms i.e at what level the cyber security defense needs to be planned. It could be done at the management level or design level.

The general dynamics of the cyber security can be categorized as- defense, exploit, integrate and operate. Each of the parameter is briefly described in Fig.1.

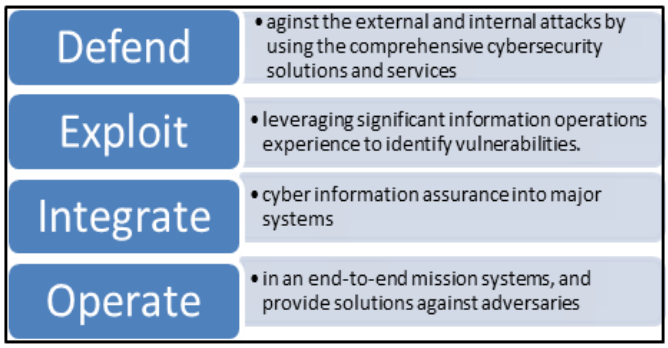

Fig. 1. General dynamics of cyber security.

These dynamics are applicable to trends and solutions that can be provided at various layers and levels in networks. Enabling these would help the organizations protect themselves against any cyber warfare or cyber security attack.

The cyber security is influenced by various concepts and parameters. As the network is quite vast, the evolution of security state is caused by the interaction between the cyber attacks and the cyber defenses [4]. Fig. 2 briefly identifies the parameters of the dynamics of cyber security in a network. These are effective at various levels of the nodes and network architecture. The first parameter –Principles, is based on dynamic and statistical systems that influence the dynamics of the nodes from time to time. These principles are based on mathematical models. The second parameter-Techniques and designs focus on setting up various architectures and policies that can be designed and implemented at various layers and networks. The third parameter –Mechanisms and Operations work on operations like cryptography, algorithms and access control. They affect the confidentiality and authentication of the nodes in the network. Further, the information on network setup and types of attacks play a vital role in understanding the dynamics of the cyber security of the network. Based on the data compiled, a statistical analysis can be performed and system can be trained using machine learning techniques to prepare the nodes in the network and prevent any cyber attack.

Dr. Bhavna Arora, "The cyber warfare and cyber security dynamics ", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 249-251, 2015.

ISSN: 2454-1532

Efficient design of the system can prevent cyber attacks thus preventing the cyber warfare.

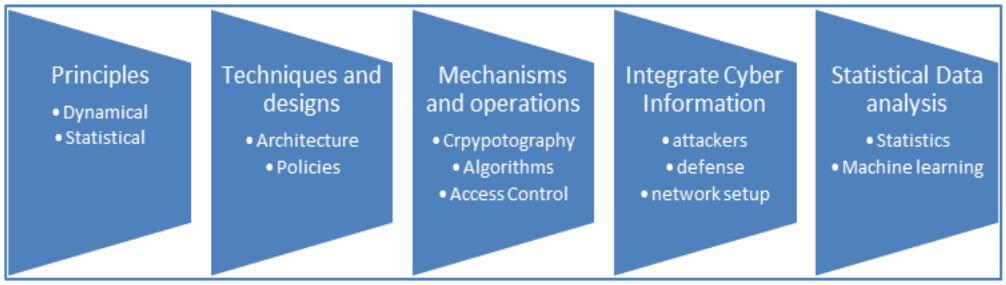

Fig. 2. Parameters for cyber security dynamics.

V. CONCLUSION

Today, the computers carry huge amount of data and databases related to medical, business, transport, crime and other areas. The ever-increasing over dependency of the economy and infrastructures on IT system has created quite high levels of security risks. Vulnerabilities arise as no systems are completely secure. The threats and risks that result from inexpensive cyber attacks are of great concern to nations these days. All the sectors like the public, private and military sectors are affected. In order to fulfill the aim of achieving cyber security, there is a large range of challenging theoretical and practical problems that must be adequately addressed. These issues and problems cannot be bypassed or overlooked as they are inherent, and therefore must be confronted and tackled - regardless of the specific technical approach that is taken. In order to achieve the desired outcomes, multi discipline research is required. The dynamics mentioned in this paper are not achievable in just one area. A coordinated research among various disciplines is the need of the hour.

REFERENCES

[1] https://en.wikipedia.org/wiki/Computer_security
[2] http://searchsecurity.techtarget.com/definition/cyberwarfare
[3] "Information Warfare: Cyber Warfare is the future warfare" Global Information Assurance Certification Paper, SANS Institute, 2004.
[4] S. Xu, "Cybersecurity Dynamics," Department of Computer Science, University of Texas at San Antonio.
[5] http://www.gdc4s.com/cyber
[6] B. Arora, "Information warfare: the emerging threat to digital economy," *8th International Conference on Advanced Computing & Communication Technologies ICACCT*, 2014.

Dr. Bhavna Arora, "The cyber warfare and cyber security dynamics ", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 249-251, 2015.

ISSN: 2454-1532

Dr. Bhavna Arora, "The cyber warfare and cyber security dynamics ", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 249-251, 2015.