Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 1 January 2023

Mini Review

Denning's Information Warfare Based Cyber Warfare Model

Hyun-A Park*

Department of Computer Engineering, Honam University, South Korea

***Corresponding Author:** Hyun-A Park, Department of Computer Engineering, Honam University, South Korea.

Received: November 16, 2022

Published: December 06, 2022

Abstract

Since the late 20's centry a computer and IT have developed, recently they supply all over the world with internet. Such as this prominent developmet, they play a very important role in our all livings. So, a government determine it as a critical policy. To activate it, we need to understand Information Warfare more clearly. Hence, we look over Denning's Information Warfare theory known for representative Information Warfare Model. To overcome generality and scalability of this model's advantage as well as defect, we propose a Cyber-Information Warfare Model for concurrent time and toward the future.

Keywords: Information Warfare; Cyber Warfare; Electronic Warfare; Information Resource; Player; Offensive Operation; Defensive Operation

Introduction

The rapid development of information and communication technology and computers in recent years has brought epochal changes in lifestyle, social systems. In particular, with the spread of the Internet, the word "global village" is becoming a reality, and computers and information and communication technologies are becoming an important part not only in economy and society, but also in the daily life of the people and the military. In particular, in order to revitalize information technology, which is being promoted as an important policy area of the government, we need to have a clearer understanding of information warfare [4].

To this end, we first look at the concept of information warfare. In the most general definition of the U.S. Department of Defense and Reto Haeni, "Information warfare means defending one's own information, information-based networks, while defending the other's information, information-based processes, information systems, and computer-based networks. It is defined as behavior that seeks to gain an information advantage by influencing others".

Next, looking at Dorothy E. Denning's information warfare model, Denning explained four major categories of information warfare: information resource, player, offensive operation, and defensive operation [1]. And the small details within that large category are very general as they contain all possible situations in information warfare, and indeed, any aspect of information warfare that is currently taking place will be difficult to deviate from Denning's model. Not only the civilian sector, but also the military aspect, as well as modern cyber warfare, the classical information warfare of the past, economic and corporate, state, and individual aspects are not covered. But if there's one downside behind this comprehensive and universal advantage, it's that not all of these situations are created equal.

Therefore, we propose a model for cyber warfare, a modern information warfare, based on Denning's model, in line with the development of computers and information and communication technologies. Currently, the concept of cyber warfare is used interchangeably in several papers. However, we focus on cyber warfare, that is, electronic warfare, which is generally used as a concept of modern information warfare [3].

Cyber warfare (electronic warfare) model

The proposed model is based on Denning's model, and its composition is the same as Denning's.

Information resource

Elements of information assets are divided into information, which is the subject of information, and weapons necessary to conduct cyber warfare [3].

Information is the target and ultimate goal of attacks and defenses carried out in cyber warfare in the everyday sense.

Weapons include information systems, network environments, computers (both hardware and software components), electrical wiring networks, security equipment, and electronic devices such as airplane guidance programs.

Player

We can classify information performers into two aspects. First, according to Denning's theory, from a functional point of view, it can be thought of as an offensive player, a defensive player, and a player with dual roles. And in another aspect, it can be divided by the performing entity, and it can be considered by individuals, companies or organizations, and countries [1,3].

Due to the nature of cyber warfare, one hacker out of curiosity of a general high school student can become an attacker, and when considering the sufficient possibility of de-massive destruction [5], individuals are also a factor that cannot be ignored in cyber warfare. In addition, companies or groups competing for other interests are engaged in fierce intelligence operations to gain an edge over each other, and even at the national level, there is a trend that all efforts are being made to cyber warfare for their own interests in terms of military security and economic activities.

Offensive operation

Denning looked at the gains and losses of offensive operations in three aspects: increasing the availability of information assets on the attacker side, increasing the availability of information assets on the defensive side, and lowering the integrity of information assets. However, this degradation of completeness has a proportional relationship where the availability of the attacker will increase depending on the success of the attacker's attack and the availability of the defender will decrease, so there is no need to think differently. Therefore, in the proposed model, we will only think about the availability of the attacker and the defender.

The attacker's availability may be an attacker's advantage using a hacker or virus penetration, physical attack, software attack, and the like. This can be divided into two main categories. First, the theft and destruction of computers, machines, and storage media are caused by physical manipulation. The following are intellectual manipulations, which include paralysis and malfunction of mechanical facilities such as systems and networks, change of information flow (damage of distribution path), damage to information storage media (damage of DB, management system, file, smart card, etc. and malfunction), stealing, destroying, and tampering with information itself, and deception and psychological warfare in terms of cognitive management as defensive attacks.

As for the defender's availability, there may be a decrease in the availability of the defender caused by theft and destruction, and malfunction due to intellectual manipulation, and a decrease in availability due to tampering and loss of information.

Defensive operation

The defensive information warfare is also largely divided into two categories, first in terms of preparation and prevention, and second, in terms of detection and response.

During the preparation and prevention phase, the following are implemented; Identification of protection targets and interdependencies, vulnerability assessment, recognizing the possibility before or early in the attack to avoid or reduce the impact of the attack, collecting information on the type of attack/hacker site attack method /technologies, marking or warning to share information on attack site, fostering professional manpower, fostering the information protection industry, establishing a legal/institutional basis for countering cyber warfare and promoting public awareness.

Detection and response include system access control, intrusion prevention and detection when connecting to the Internet, hacking prevention and virus blocking system, authentication, firewall, etc. in terms of security system construction and management.

Building a response system refers to forming a dedicated organization that can counterattack immediately after being

attacked, establishes backup and accident response capabilities, recovers from damage, and establishes and implements consistent policies by integrating the duties and functions of each ministry, etc. [4].

Conclusion

Our society has undergone changes at a fairly rapid pace in many ways compared to the past as all social systems through computer networks. In the future, information warfare is expected to have such a pattern, and accordingly, a standardized model of cyber warfare (electronic warfare) is required. Also, in this cyber warfare, the models required by the private sector and the military sector will be different, and the private sector will also have different needs depending on the objectives of various interest groups such as finance and corporations. However, if a detailed model is established based on a model that can integrate all information warfare into one, such as Denning's model, the country or organization will be able to gain an edge in information warfare more efficiently.

Bibliography

She received the B.S. degree from the Department of Mathematics at Korea University, Seoul, in 2003, and the M.S. and Ph.D. degrees in Information Security from the Korea University, Seoul, in 2005 and 2010, respectively. Currently, she is with Honam University in South Korea as an Assistant Professor. She has around 50 publications, several patent registrations and awards. Additionally, she has been a member of over 10 communities and editors. Her main research interests include Medical (Health) Information Security,Practical Retrieval System on Encrypted Database Systems. She is interested in Database Security, Access Control, Privacy Preserving in Data Mining (PPDM), Anonymous Communication Channel, Privacy Enhancing Technology (PET), and Cryptographic Protocols.

Bibliography

1. Dorothy E. "Denning, Information Warfare and Security". Addison-Wesley Publishing, USA, (1999).
2. Heejin Jang., *et al*. "Next-generation offensive information security technology". *Korea Information Processing Society Review* 7.2 (2000): 49-54.
3. Bruce D Berkowitz. "Warfare in the Information Age". *Science and Technology* 12.1 (1995): 59-66.
4. Gilhyun Nam. "Suggestions for Information Warfare (Cyber War)". *KIISC Review* 12.6 (2002): 54-57.
5. Taewon Kang and Jeongseop Hwang. "Consideration of future warfare centered on cyber warfare". *KIISC Review* 12.6 (2002): 41-53.