A Leverage Strategy of the Cyber Warfare Security Policy Based on Systems Thinking

Ho-Kyung Yang [1], Jin-Mook Kim [2], Hwang-Bin Ryou [3]

[1.] Department of Defense Acquisition Program, Kwangwoon University
[2.] Division of IT Education, Sunmoon University
[3.] Department of Computer Science, Kwangwoon University
porori2000@kw.ac.kr, calf0425@sunmoon.ac.kr, ryou@kw.ac.kr

Abstract: As the network composed of numerous sensor nodes, sensor network conducts the function of sensing the surrounding information by sensor and of the sensed information. The concept of the battlefield is also changing to one that includes not only physical spaces but all areas including the networks of the nation's key industries and military facilities, energy facilities, transportation, and communication networks. In light of the changing warfare in terms of how it is conducted and what form it takes, the Korea military has to seek ways to effectively respond to threats of cyber warfare. In the past, although partial strategies on cyber warfare were studied, no research was done through the overall system flow. In this paper, key variables related to cyber warfare security are classified into personnel, management, and technology. A simple model and an extended model are suggested for each area, and based on the technology area of the extended model, formal methods are used to verify the validity and a detailed response strategy is suggested according to the identified leverage.
[Ho-Kyung Yang, Jin-Mook Kim, Hwang-Bin Ryou. **A Leverage Strategy of the Cyber Warfare Security Policy Based on Systems Thinking.** *Life Sci J* 2014;11(10s):175-179]. (ISSN:1097-8135). http://www.lifesciencesite.com. 28

Keywords: Systems Thinking, Cyber warfare, Leverage strategy, simulation, Cyber attack

1. Introduction

It is essential that the advancements in new information and communication technology are applied to the military when it comes to the area of information and communication in order to conduct the changed form of warfare in the 21st century. Efforts are being made in order to share the effects such as tactical monitoring and tracking, as well as real-time gathering of battlefield information.

But with such advancements in the network, security threats are increasing as well. Furthermore, as the network expands, the number of routes via which to attack increases and as the amount of data being moved increases, so does the amount of those data which would be dangerous if leaked out.

In this paper, using the systems thinking methodology, primary variables that comprise the overall security system of cyber warfare are selected and classified under the areas of personnel, operation, and technology. Furthermore, simple and extended models are suggested which show, for each area, the causal relationships that exist between different variables. In addition, formal methods are used to verify the validity of those variables in the area of technology in the extended model in particular and a specific response strategy is suggested according to the identified leverage.

2. Related researches

2.1 Systems thinking

The system thinking is a way of thinking for finding strategies for making a system more effective, by gaining an intuitive understanding of the underlying mechanisms of the system.

The primary goal of systems thinking is coming up with a fundamental diagnosis and solution for the problem, and suggesting a model for connectivity [1][2][3].

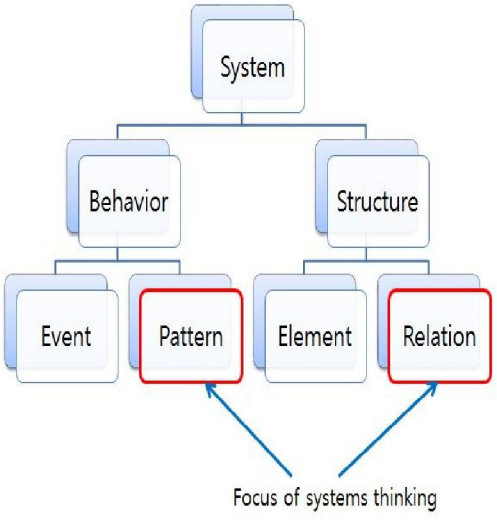

Figure 1. Focus of systems thinking

2.2 Cyber warfare

Cyber warfare refers not only to the simple act of destroying computer systems but also activities that affect the physical systems and infrastructures which depend on them.

Cyber defense is sub-classified into information protection and physical protection. The more well-equipped a country is with information infrastructure and the more the information processing systems and the key systems of the society depend on computers, the more likely that it becomes a target for cyber-attacks and the higher the degree of consequent damages sustained.

In contrast to the form of warfare of the past, in cyber warfare the opponent's belief and information systems are attacked, and because of that it is difficult to imagine how the battles will unfold in stage-by-stage detail or accurately predict the outcome[4][5].

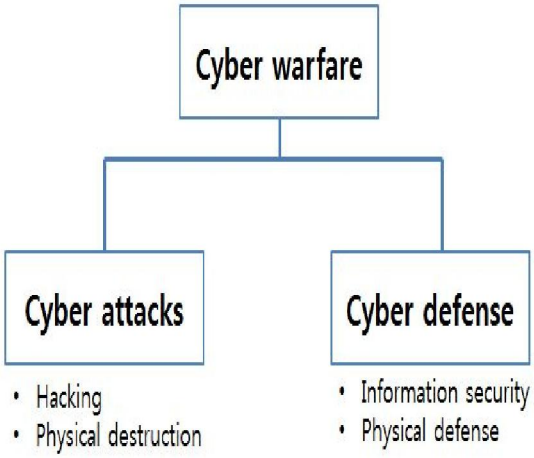

Figure 2. Details from of cyber warfare

2.3 Formal methods

Formal methods are specifications of software and hardware, and mathematics-based methods for development and verification, which are used in computer science and software engineering.

Using formal methods, inconsistences, ambiguities, and incompleteness that a system may have can be found, improving the level of understanding of the system.

With formal methods, problems that may occur due to wrong interpretations of defects in the requirements can be corrected at the beginning, so that correct requirements can be written up[6][7].

3. Cyber Warfare Based on Systems Thinking

3.1 Problem definition

Looking at the global trends of late, it is already a widely-known fact that warfare is conducted in the form of terrorism rather than a full-scale war.

Hacking and viruses in cyberspace have also been taking the form of cyber terrorism since the 2000s. The world is already engaged in the unseen warfare in cyberspace for national security.

While cyber warfare in cyberspace may be an unlikely event, there is potential for the use of computer viruses as a consequence of existing weapons of war, and also the potential for their use as a means of cyber terrorism is ever increasing.

Therefore, domestically as well, a plan is needed to deal with cyber warfare. Specifically, tools with which to train countermeasures need to be developed, which would work by predicting actual cyber warfare situations such as attacks on key information infrastructures that are on the Internet. Furthermore, different types of hacking attacks by hackers, their countermeasures, and potential targets of attack need to be stored and managed in a database. In addition, there needs to be a system in place that can predict new movements in hacking attacks and give warnings as necessary.

Formal methods are specifications of software and hardware, and mathematics-based methods for development and verification, which are used in computer science and software engineering.

3.2 Selecting key variables

Because systems thinking aims to gain an understanding of the overall structure, a casual map has to be drawn up in order for such understanding allowing the recognition of the forms in specific detail; and in order to draw up the casual map, key variables that comprise the system have to be found.

The key variables are found through related papers or research reports, in-depth interviews with pertinent persons, and surveys.

The primary variables for selecting key variables are first identified, and in the defense-in-depth strategy, in order to achieve information assurance, classification is done into three areas - personnel, operation, and technology - and among the primary variables those which are redundant or less important are removed to obtain the key variables. Formal methods are specifications of software and hardware, and mathematics-based methods for development and verification, which are used in computer science and software engineering.

3.3 Drawing up a causal map

3.3.1 Simple model for the area of personnel

Figure 3 shows the simple model for the personnel area. As shown in past research, the contents relating to the personnel have a lot of influence when it comes to cyber warfare.

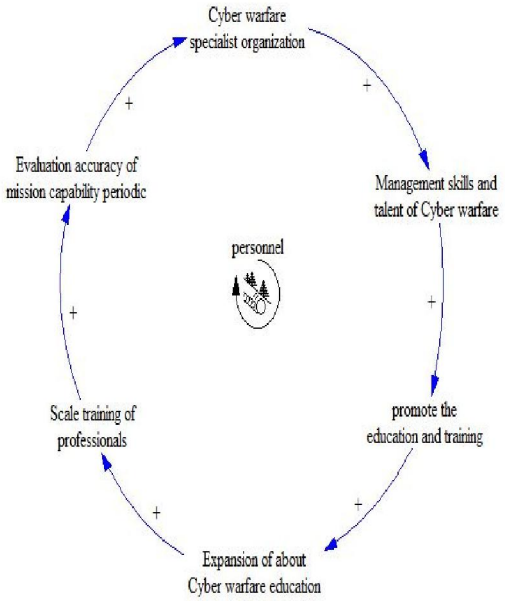

Figure 3. Simple model of people field

In cyber warfare, it's not a matter of simply how much expensive equipment or weapons one has amassed but rather how effectively those are utilized. As that is crucial, the area concerning personnel becomes important.

The loop for the personnel area has an overall positive (+) effect as a self-reinforcing loop. Formal methods are specifications of software and hardware, and mathematics-based methods for development and verification, which are used in computer science and software engineering.

.

3.3.2 Simple model for the area of operation

Figure 4 shows the simple model for the area of operation. There have been many suggestions in past research on the ways in which cyber warfare should be conducted. The loop for the operation area has an overall positive (+) effect as a self-reinforcing loop

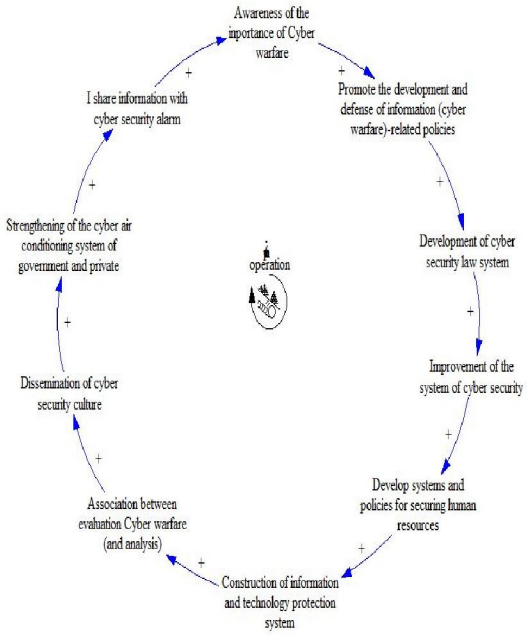

Figure 4. Simple model of operation field

3.3.3 Simple model for the area of technology

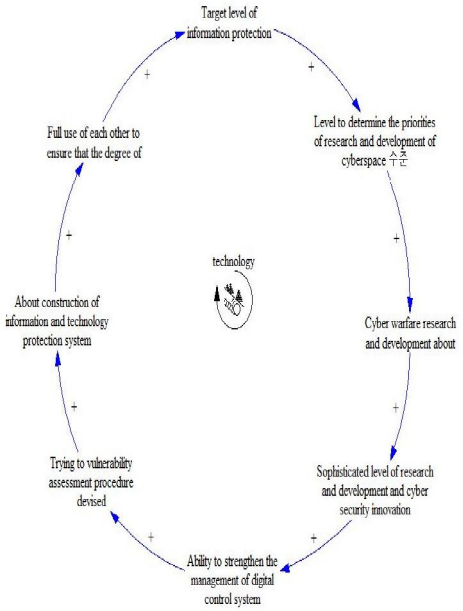

Figure 5. Simple model of technology field

Figure 5 shows the simple model for the area of technology. The loop for the technology area has an overall positive (+) effect as a self-reinforcing loop.

Level of information protection aimed for should be decided.

Based on this, the priorities of cyberspace R&D are decided, according to which R&D takes place, as well as technological innovations and sophistication in R&D.

Also, management of the digital control system is strengthened, assessments of vulnerabilities are performed, and information protection systems and technologies are constructed. When subsequently interoperability is secured as well, overall cyber warfare protection is realized. Formal methods are specifications of software and hardware, and mathematics-based methods for development and verification, which are used in computer science and software engineering.

4. Cyber Warfare Model Assessment

4.1 Assessment of validity of the extended model

As for the verification standard, based on CC, which is the international assessment standard for information protection systems, redundant assessment activities are removed.

The potential for misunderstandings is reduced by clearly defining key variables. Assessment activities regarding actual technology aspects are reorganized and standard requirements of new common criteria are added as necessary.

The assessment criteria are specified in a technical specification, which defines the terminology for each variable and classifies the criteria in stages. The formula for establishing the standards of the technology area in cyber warfare is as shown in Formula 1[8][9].

$$x = \sum_{k=1}^{n} M_{k1} + M_{k2} + \cdots + M_{kn}$$

Description of each symbol of the formula

x : The elements of the current development technology score

n : The number of elements

$k1, k2, \cdots, kn$: nTh element

M : Each element in the development of the score

4.2 Leverage Strategy

The said results of examination of the variables in the art loops, points of strategies appropriate initial art, and improve the encryption level. Protection target level of information, which is to be improved to continuous, it is intended to improve the encryption level on the basis thereof, so that they can maintain a high target levels.

I said that the point of the strategy of the proper second of the art, secure and appropriate research personnel. It is necessary to work with a lot of research and development in order to improve the research and development of precision version between. To achieve the research and development of these essentially first, it is necessary to ensure proper research personnel.

5. Conclusion

Looking at the operational concepts of warfare and growth trends, the South Korean military has to come up with a plan to effectively respond to the threats of cyber warfare.

While strategies of cyber warfare have been studied in part in the past, no research has been done based on the overall system flow. .

In this paper, in order to gain an understanding of cyber warfare security, systems thinking methodology, which is one of the research methodologies, is used to identify the key variables that comprise the overall security system for cyber warfare. These key variables are then classified into the areas of personnel, operation, and technology.

The causal relationships between the variables are used to create simple and extended models for each key variable, in order to visualize the overall constitution of cyber warfare. .

The overall structure of cyber warfare security suggested in this paper and the leverage strategies which are applicable for the area of technology would not only be able to be used as basic data when establishing laws and regulations as part of preparing for cyber warfare but also when establishing pertinent policies as well.Please, follow our instructions faithfully, otherwise you have to resubmit your full paper. This will enable us to maintain uniformity in the conference proceedings as well as in the post-conference luxurious books by WSES Press. The better you look, the better we all look. Thank you for your cooperation and contribution. We are looking forward to seeing you at the Conference.

Corresponding Author:
Prof. Jin-Mook Kim
Division of IT Education
Sunmoon University
Asan-si, ChungNam, 336-708, Korea
E-mail: calf0425@sunmoon.ac.kr

References

1. John d.Sterman, BUSSINESS DYNAMICE, McGraw-Hill, 2000
2. Richmind B., System Thinking: Critical Thinking Skills for the 1990s and Beyond, Systems Dynamics Riview, 1993
3. Richmond.B, System Thinking, Crotical Thinking Science and Systems Theory, Philadelphia, The University of pennsylvania press, 1991
4. Hak-kwon Kim, A study on cyber warrior training scheme for cyber war of military, KyungHee University, 2008
5. Hyun-su Jung, Research on proactive Response Measures against Cyber Warfare, Korea University, 2001
6. Hyuk Lee, Kum-Taek Jeong, Jin-Young Choi, applying formal methods to Earthquake crisis manual, Korea Computer congress 2011, Vol 38, No 1, pp302-305, 2011
7. Kum-Raek Jeong, Jin-Ho Lee, Suk Seo, Jin-Young Choi, Specification and Verification of Crisis response Manual using Formal Methods, Korea Computer Congress 2010, Vol 37, No1, pp.116-119, 2010
8. CCRA Management Committee, CC(Common Criteria for Information Techonlogy Security Evaluation) v3.1 Revision 4
9. Ho-Kyung Yang, A Study on Technological Security Policy Leverage strategy foe Cyber warfare, Kwangwoon University, 2013