International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.293-302
http://dx.doi.org/10.14257/ijsia.2016.10.11.24

Modeling of Cyber Target Selection for Effective Acquisition of Cyber Weapon Systems

Ki Hoon Kim and Jung ho Eom *

Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon,
kkh2368@dju.kr, eomhun@gmail.com

Abstract

In this paper, we propose a model that can effectively select cyber targets when acquiring cyber weapons systems. Cyber target selection is the process of deriving the most vulnerable part of the target system. Cyber target selection is carried out with 3 components such as 'center of gravity', 'target attribute and control characteristics', and 'type and characteristics of information communication system'. Gravity refers to the weakest part of the enemy (security holes), and the security holes that cause the most decisive effects when cyber-attacks are happening. The target attributes are classified into the geographical attributes where the target is, the functional attributes which tasks are performed, and the human attributes who uses and who owns them. Control characteristics are the factors that determine how an attack effect on a potential target system occurs by cyber weapons systems or operations. When a cyber-attack target is selected, the final attack target is selected by the form, characteristic, and function by distinguishing the target of the center, the target of the layer, and the list of the information communication system. And then, the main attack points that are targets of actual cyber operations are selected based on the selected cyber targets.

Keywords*: Cyber Target, Cyber Weapons, Target Selection, Main Attack Points*

1. Introduction

A lawmaker issued that 'South Korea's cyber command was found to have been hacked on October 2016'. A malicious code has been identified and it seems to use of the vulnerability of the vaccine routing server which is tasked with security on military computers for Internet-connection purpose, and it has connected to around 20,000 military computers. According to some security professionals, United States have experienced cyber-attacks such as secret data thefts originating from China in the last decade. In August 2008, when Russian troops invaded the Republic of Georgia, They just fought with troops and tanks. It was possible to attack because, they conducted DDoS attacks to Georgia government homepage and nation's primary web site in advance. At that time, cyber-attacks were highlighted as the new challenge of war. Cyber-attacks are no longer a conflict in cyberspace but recognized as an aspect of war [1-5].

Cyber-attacks should not be overlooked as a level of trivial threat in cyberspace. Cyber-attacks are maneuvers or actions performed in cyberspace when a kinetic war takes place in the physical space. So, the systematic cyber defense system should be established to prevent, detect, analyze and trace cyber-attacks. When cyber-attack or defense is performed, an operation plan should be established, and cyber intelligence is required accordingly. The cyber intelligence should be prerequisites for assuring intelligence superiority in cyber operation. In kinetic warfare, intelligence provides the commander to various data for assessments and estimates

* Corresponding Author : Jung Ho Eom

ISSN: 1738-9976 IJSIA

that facilitate understanding the operational environment. This includes the organizations, capabilities, and processes involved in the collection, processing, analysis, dissemination, and assessment of information. Especially, without cyber target intelligence, the operational superiority also can't secure and can never win the cyber warfare. Cyber target intelligence is intelligence that portrays and locates the components of a cyber target or target complex and indicates its vulnerability and relative importance [6]. Cyber target intelligence is very important factor to secure the operational superiority in cyber operation. When cyber response attack is conducted, we can't make a proper retaliatory attack if we have no exact hostile target intelligence [7]. When we select a cyber target for cyber response attack, we use cyber target intelligence. Cyber operations are addressed at a target in order to attain a desired effect. Cyber operations are conducted against hostile cyber identities and objects, resulting in a predefined effect. So, it is very important to select cyber target (cyber identities and objects, etc.) for achieving the predefined effects. Cyber-attack cycle is consisted of 7 steps; reconnaissance, weaponized, deliver, exploit, install, command and control, and action on the objective. An exploit step in the cyber-attack cycle means to exploit a cyber targets such as an application or operation system vulnerability. In this step, the attacker seeks known or previously unknown software application or operation system vulnerability on a targeted network and system [8-9].

So, we propose a cyber target selection model for achieving predefined cyber-attack effect. Cyber target is selected with such 3 components as 'center of gravity', 'target attribute and control characteristics', and 'type and characteristics of information communication system'. The proposed model carefully selects cyber target because effects are achieved by engaging targets. This paper is organized as follows. We will describe cyber target and its effects in section 2 and cyber target selection model in section 3. We demonstrate the proposed model's procedure in section 4, and conclude in the last section.

2. Cyber Target and Effects

Cyber operations are addressed at a cyber target for getting a desired effect. In other words, cyber operations mean the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace. The objective of cyber operations is to reach predefined effects by conducting a cyber-attack on adversary target. Effects can be achieved in cyberspace by attack adversary targets on the physical or non-physical dimension of cyberspace, using cyber weapons. Cyber operations can achieve these effects stand-alone or in parallel with other operations. The effects achievable through cyber operations are diverse such as the constructive and the disruptive effects. Constructive effects can be achieved by using such cyber targets as cyber identities and cyber objects. Constructive effects can be achieved by influencing and supporting friendly actors, armed forces attempt to generate disruptive effects against an adversary [8]. In other study, effects by cyber operations are categorized by the severity and persistence of effects. The three categories of severity are primary, secondary, and indirect effects. The first effect is Primary effect that has the potential of directly affecting physical information assets and human life. The second effect is the secondary effect that degrades or disrupts physical information assets as a second-order consequence of effects in the cyberspace. The last effect is the indirect effect that remains within the cyberspace, having only an electrical and informational impact. Three categories of persistence degrees are permanent, temporary, and transient effect. The permanent effect includes effect that requires replacing information communication system or

extensive and time-consuming repairs. Temporary effect persists after finish cyber operation. However, it means to recover entails actions of lesser cost in resources and time unlike permanent effects. The transient effect abates quickly after finished cyber-attack, with little effort on the part of the targeted asset [10].

Effects are addressed at a target against which the constructive or disruptive activity is addressed. Effects can be achieved by engaging targets selected from an actor's physical, moral, and conceptual component. In the physical dimension, objects and humans can be addressed targets constructively or disruptively. Objects are tangible elements such as systems and supplies. Human varies from one to groups and may be adversary, neutral, or coordinated. In the non-physical dimension, the psyche of human can be addressed target with the purpose of influencing the moral and conceptual components. Especially, in the cyberspace, targets are divided into cyber objects and cyber identities. Cyber objects are the logical elements enabling interoperability and communication between physical objects such as protocols, applications, DNS, OS, S/W, and data etc. Cyber identities are the digital and virtual identities (ID) of people, individuals, groups, and organizations such as e-mail accounts, SNS accounts, etc [8].

Targeting means action of a military cyber force engaging, or preparing to engage, adversary targets as describe above. It also describes the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities [11].

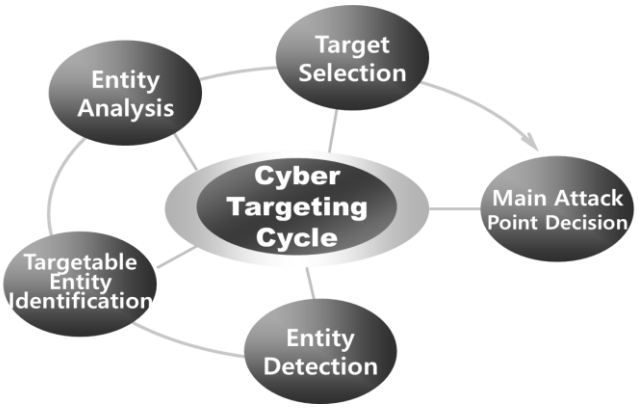

Figure 1. Cyber Targeting Cycle

Once a cyber target is determined, the vulnerability of the target must be identified. The attack entity is the target system, but the main attack point is the weakest component of the target. For example, if a web server has been selected as a target, it should identify the vulnerability of the web server. There are vulnerabilities such as 'Perl CGI' script related to CGI script processing and 'DOS .bat' files in case of Windows NT Netscape Communications Server. Perl CGI scripts can delete all files in the current directory on the server. A CGI script implemented as a '.bat' file has a vulnerability that executes arbitrary commands. Cyber targeting cycle is performed as shown in the figure above.

① Entity Detection: Collect data, using scanning tools and vulnerability analysis tools to collect information, on entities that can be targeted, such as equipment type, operating system, application program, IP address, port number, and provided services.

② Targetable Entity Identification: Identify entities that meet the attack objectives and that the attacker achieves the desired effects, using data processing techniques.

③ Entity Analysis: Analyze the characteristics, functions, importance, and damage effects of targetable entities to select potential military targets.

④ Target Selection: Select the appropriate target that can minimize the physical damage while also threatening the enemy.

⑤ Main Attack Point Decision: Determine the components that are the most vulnerable of the selected target, which can only cause the target's functional damage and maximize the attack effect

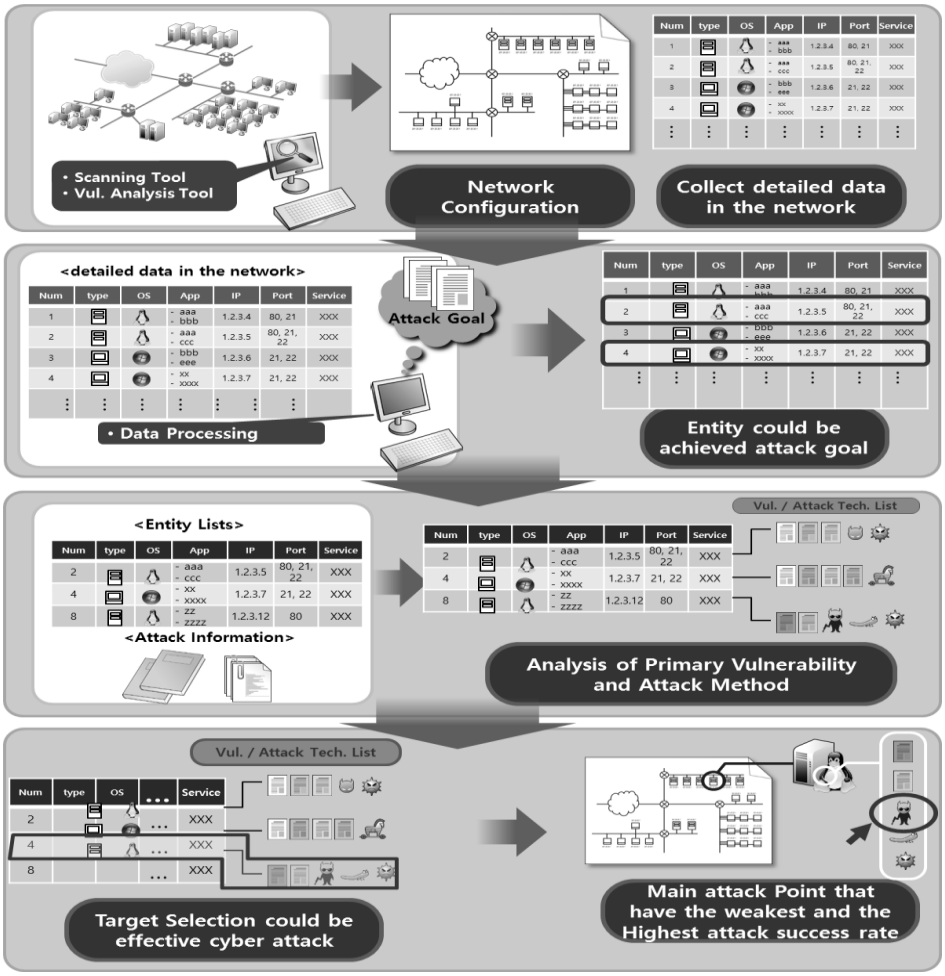

Figure 2. Cyber Targeting Processing

3. Cyber Target Selection Model

Our proposed model includes the process of determining from attack target system identification to the main attack point. The cyber target is selected as the most vulnerable point of the enemy chosen to execute the cyber commander's intent or policy in order to achieve the purpose of the cyber operation.

First, the cyber commander selects one of the strategic, tactical, and operational targets to achieve operational objectives. Our model can be selected according to the Center of Gravity (CoG) as applying the notion of targeting and attacking effect-based operations

for strategic paralysis, which was used in the Iraq war. EBO(Effectiveness Based Operations) is an operational concept that neutralize enemy combat forces and achieve operational objectives faster without generating casualties rather than removing and destroying enemies in order to end war [12,13]. Effectiveness based operations and cyber operations can have the concept of a center of gravity in selecting military cyber targets because they have commonalities in terms of achieving the goal by disabling the enemy's combat power and paralyzing the enemy rather than destroying the enemy. A center of gravity means the weakest part of the enemy, and the security hole that causes the most decisive effects when cyber-attack is conducted. The center of gravity is divided into strategic, operational and tactical center. Strategic center means national core infrastructure system that can cause social confusion and paralysis, such as power grid, transportation network, financial network, military information communication network, etc. Operational center refers to the core information system of cyber operations such as air control system, air defense control system, and combat command communication system operated by each army, etc. Tactical center means such as the operating equipment, software of each weapon system or unit, etc. This classification should identify the vulnerabilities of each system. The following figure shows the type of target along the center of gravity for paralysis.

Figure 3. Classification of Center of Gravity

Second, Robert Fenelli of the US Cyber Command can select the target by target attributes and control features in his paper [10] 'A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict'. The target attributes are classified 3 attributes into the geographical attributes where the target is located, the functional attributes of which tasks are performed, and the human attributes of who uses and who owns them. Control features mean that a cyber weapon or operation can be used to determine if effects should be happened to a potential target. Control features are divided into physical layer, logical layer, cyber user layer, and command control layer as shown below [10].

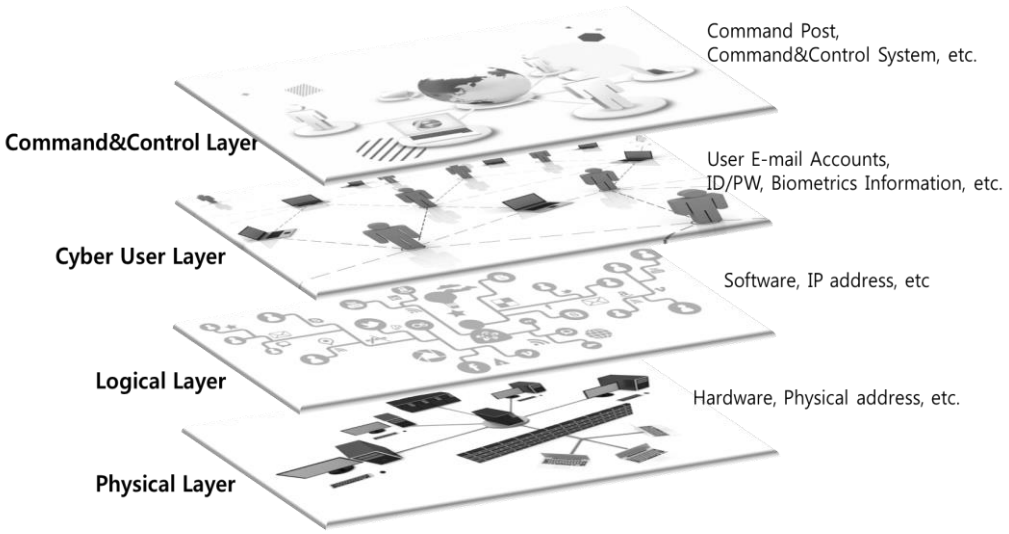

Figure 4. Control Features Layer [10]

The physical layer includes features of a device's hardware, its operating system, and its physical environment. Information of hardware could be identified as general type, manufacturer or specific model, or device's unique identification by embedded serial numbers. 'For example, in the case of smart phones', it may provide direct information about geographic locations through GPS or mobile network location services.

The logical layer has features of the software, configuration, and the software's state on a device. For example, those are logical network addresses, such as IP addresses. Although an IP address does not contain location information, the nature of IP networks and knowledge of address range assignments could be seek geographic location or ownership [14]. It may also facilitate identifying the function of a device in the logical layer.

Cyber user layer has identities in the cyberspace. These features are useful in determining the ownership, affiliation and users of information assets. Both user in the physical layer and user in the logical layer often exist in one to many or many to many forms. A user may have many cyber users while a single cyber user may exist. For example, they are the user account, accounts for local and remote systems such as electronic mail.

Command and control layer contains the command and control functions available to launch, finish and redirect a cyber weapon or operation. This also includes functions related to command and control of targeting and effects during the cyber operation. And this conducts predefined trigger maneuvers for launching, finishing or redirecting some aspect of a cyber operation and controls on the capability of cyber weapons to propagate autonomously.

Last, our model designates cyber target's components with the cyber infrastructure list. This list is constructed by the types and characteristics of the infrastructure system. This list arranges all possible infrastructure-related components according to criteria defined in the infrastructure scope. It is generally classified according to types and characteristics of infrastructure. And then, it can be divided into seven major categories based on the type and characteristics of the infrastructure, which can be classified in detail.

Table 1. Cyber Infrastructure List

Classification	Explanation	Type
Hardware	Information assets with physical characteristics such as mechanical, electronic, and in the infrastructure	Hard disk, Tape Cartridge, CD-ROM, System Terminal, Disk Array, Print Server, etc.
Operation System	A kind of software to operate computer hardware efficiently	UNIX, DOS, Windows, Linux, etc.
Application	Software made up for use in specific areas of the user's needs, such as document editing, payroll accounting, information processing, calculations, etc.	Word Processor, Compiler, DBMS, Web Browser, etc.
Network	Hardware and software that provide the ability to share data between different systems	Network OS, HUB, Router, Bridge, Gateway, Modem, Network Interface Card, Protocol Types, LAN Types, Access Control S/W, etc.
Data	Electronic information that can be produced, stored, and processed in the infrastructure systems	Employee Data, Financial Data, Contract Data, Project Data, System Data, etc.
User	All personnel, including operators, developers, analysts, and combatants, users, who use the infrastructure	System and security administrator, information analyst, application software developer, database administrator, cyber policy maker, cyber combatant, etc.
Environment	tangible or intangible elements indirectly associated with the infrastructure system	Security controller, Uninterruptible power supply, Fire control system, Access control system, etc.

When a cyber target is selected, it is possible to create a final attack target as shown in the following figure by distinguishing the type, characteristic, and function of the target selection by a center of gravity, the target by layer, and the infrastructure list like described above. In this time, the selected target is the infrastructure component that has the attack point, not the main attack point. The cyber-attack should determine the main attack point, even if the target system is determined, because the attack is executed using the vulnerability of the target system. That is, the main attack point must be determined based on the cyber target list and the vulnerability list of network system. Vulnerability is a security hole that can be exploited for known bugs or attacks in networks and systems. In other words, those are weaknesses of design, implementation, operation, and management. In addition, the vulnerability is also used as a cyber-attack route to down network and system to prevent normal service of network and system, or to leak, change or destroy important information in the system. In addition, the success or failure of the cyber-attack depends on the degree of vulnerability, the intensity of attack, and the effectiveness of countermeasures.

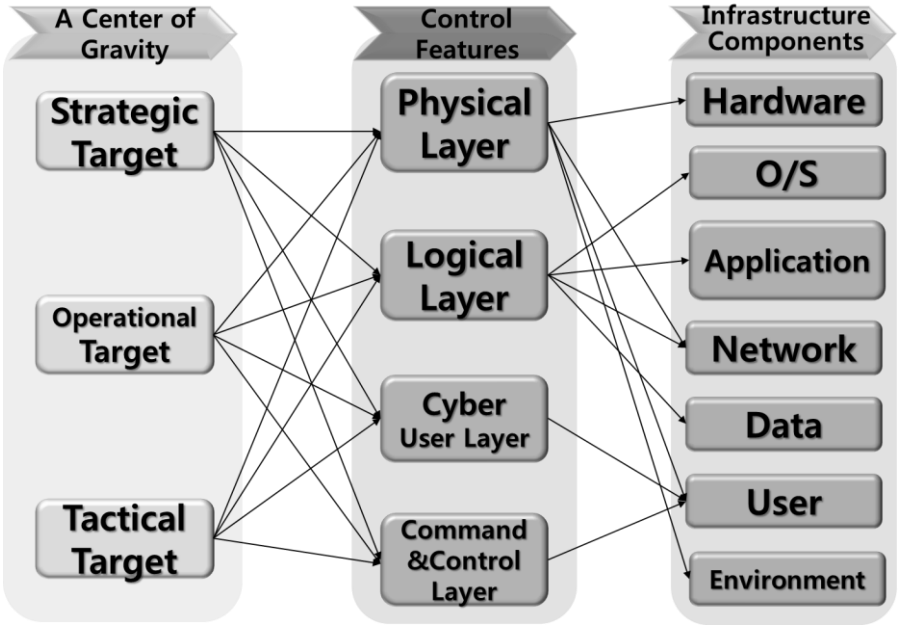

Figure 5. Cyber Target Selection Model

When the cyber target system is selected as shown above, it is necessary to identify the vulnerabilities of the system and determine the main attack point among them. The vulnerability list is always available whenever vulnerability is found, and can be found on the vulnerability site (https://cve.mitre.org/cve/, CVE list provided) [15]. However, the vulnerability to the user or the environment element may not be listed separately, but may be the target itself, that is, the user may be the operator and the administrator, etc. and the environmental element may be a UPS, a fax machine, a printer, etc. The reason is because the user or environment factor is not a direct damage factor through cyber operations, but an incidental or secondary damage factor. For example, if an enemy commander is selected as a target, he can use psychological techniques to extract information by using the weaknesses of a commander's mobile terminal, account, e-mail, etc., or to recommend surrender via text message or e-mail.

4. Application of Our Proposed Model

In the case of network, operating system, and application software network, the main attack point can be identified through the vulnerability list. For example, in order to disable an air defense system server at an enemy air defense control command, information about the server type, operating system, language, etc. used by the enemy should be obtained and the vulnerability of the server should be identified.

Suppose that an objective of cyber operation is paralyzing an enemy's strategic command and control function. If so, the center of gravity for the cyber-attack will be the strategic center of command and control. In the second stage, it is included in the physical layer because the function paralysis of system is the goal. Assuming that the server is Solaris, the main network that sends and receives information such as cyberspace information or commands, it is included in the hardware component in the infrastructure list. The figure below shows the target selection (center-feature-composition) for paralysis

strategic command and control function. The infrastructure component corresponds to hardware.

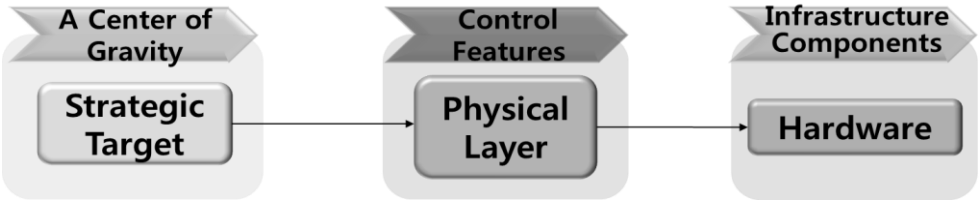

Figure 6. Target Selection for Paralysis Strategic Command and Control

The vulnerability could be the main attack point, 'CVE-2016-0693, CVE-2016-0535', where the Solaris server is vulnerable to availability. The CVE-2016-0693 is a weak point of remote control related to LDAP module of PAM. The CVE-2016-0535 is a weak point of remote control related to RPC. The figure below shows the process result for target selection and main attack point selection.

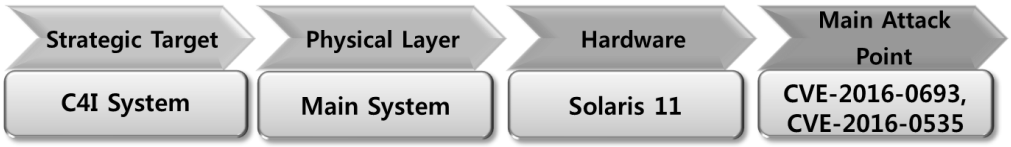

Figure 7. The Last Cyber Target Selection for Cyber Operation

5. Conclusion

We proposed cyber target selection model for effectively select cyber targets when acquiring cyber weapons systems. Cyber target selection is the process of deriving the most vulnerable point of the target system and seek cyber-attack route. It is carried out with such 3 components as ‘center of gravity’, ‘target attribute and control characteristics’, and ‘type and characteristics of information communication system’.

Targeting means action of a military cyber force engaging, or preparing to engage, adversary targets. It also describes the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Effects can be achieved in cyberspace by attacking adversary targets on the physical or non-physical dimension of cyberspace, using cyber weapons. So, cyber operations can achieve these stand-alone effects or in parallel with other operations. It is a very important process to select cyber target in cyber operations. In cyberspace, targets are divided into cyber objects and cyber identities. Cyber objects are the logical elements enabling interoperability and communication between physical objects such as protocols, applications, DNS, OS, S/W, and data etc. Cyber identities are the digital and virtual identities (ID) of people, individuals, groups, and organizations such as e-mail accounts, SNS accounts, etc.

First, the cyber commander selects one of the strategic, tactical, and operational targets to achieve operational objectives. Second, Robert Fenelli of the US Cyber Command can select the target by target attributes and control features in his paper [10]. Last, our model designates cyber target’s components with the cyber infrastructure list. We applied the proposed model to cyber-attack scenario that is an objective of cyber operation is paralyzing an enemy's strategic command and control function.

In the future, we will research the technical details and the effectiveness of the proposed model. Finally, we will configure the proposed model to run automatically.

Acknowledgements

"This paper is a revised and expanded version of a paper entitled [Architecture of Cyber Intelligence System for Cyber Attack & Defense Training] presented at [ITCS2016, Bali and 5~8 July]."

This research was supported by the Daejeon University fund (2015)

References

[1] http://english.yonhapnews.co.kr/ **(2016).**
[2] Nir Kshetri, Cyberwarfare: Western and Chinese Allegations, ITProfessional, January/February, pp.16-19 **(2014).**
[3] Jae-Hyun Shin, Sang-Pil Cheon, and Jung-ho Eom, The Role and Responsibility of Cyber Intelligence in Cyber Warfare, The proceedings of The 3rd International Conference on Information Technology and Computer Science, **(2014)** July 17-20, Saipan USA.
[4] Tai-Myoung Chung, Jung-Ho Eom, Sung-Hwan Kim, and Nam-Uk Kim, Information Security: Ask and Answer, hongneung Publishers, Seoul **(2014).**
[5] Jung ho Eom, Modeling of Document Security Checkpoint for Preventing Leakage of Military Information, Journal of Security and Its Application, Vol.6 No.4, **(2012)**, pp.175-182.
[6] William E. Gortney, "department of Defense Dictionary of Military and Associated Terms", Joint Publication 1-02, **(2014).**
[7] An introduction to cyber intelligence, http://www.Tripwire.com **(2014).**
[8] Paul Ducheine and Jelle van Haaster, "Fighting Power, Targeting and Cyber Operations", the 6th International Conference on Cyber Conflict **(2014)**, 3-6 June 2014, Tallinn, Estonia.
[9] "The Cyber Attack Cycle", U.S. Army Cyber Command, http://www.eur.army.mil
[10] Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict", the 4th International Conference on Cyber Conflict (2012), 5-8 June, Tallinn, Estonia.
[11] Smart and Steven J., "Join Targeting in Cyberspace", Air & Space Power Journal, Vol.25 Issue4, **(2011)**, pp.65-75.
[12] "Iraq War: based on Air Operations", Air Force Combat Development Group, **(2003)**.
[13] Jung ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace", International Journal of Software Engineering and Its Applications, Vol.8, No.9, pp.137-146 **(2014)**.
[14] J. Muir and P. van Oorschot. Internet Geolocation and Evasion, Technical Report TR-06-05, School of Computer Science, Carleton University, **(2006)**.
[15] CVE List, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=solaris **(2016).**

Authors

Ki Hoon Kim received his Ph.D. degrees in Military Studies from Daejeon University, Daejeon, Korea in 2016, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are Military Acquisition Management, Cyber War Power Acquisition, and Military Studies.

Jung ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. He is now the director of cyber forces development and CPO forum. His research interests are information security, cyber warfare, network security.

