Advanced Science and Technology Letters
Vol.51 (ITCS 2014), pp.305-308
http://dx.doi.org/10.14257/astl.2014.51.68

The Role and Responsibility of Cyber Intelligence in Cyber Warfare

Jae-Hyun Shin[1], Sang-Pil Cheon[1], and Jung-ho Eom[2]

[1] The Headquarter of Airforce,
Sindoan-myun Geryongdae-ro 663,
Geryoung-si, Choongcheongnam-do, Republic of Korea
{sjh22301, skyfeel69202}@naver.com
[2] Department of Military Studies, Daejeon University,
62 Daehakro, Dong-Gu, Daejeon-si, 300-716, Republic of Korea
eomhun@gmail.com

Abstract. In this paper, we proposed roles and responsibilities of cyber intelligence in cyber warfare. Especially, we drew support's elements of cyber intelligence in Pre-CTO procedure. In here, cyber intelligence is a cyber-discipline that exploits a number of information collection and analysis approaches to provide direction and decision to cyber commander and cyber combat units. The cyber intelligence should be prerequisites for assuring intelligence superiority in cyber warfare. This performs a key role in both cyber-attack and cyber defense. We know that the branch of information and communications performs cyber operations in cyber warfare. But the intelligence branch is more in charge of the policy, strategic, and statics in cyber warfare. They collect information requested from the operation branch and disseminate information to department related to cyber operation. They also perform critical role on each step in Pre-CTO procedure. So, the cyber intelligence is key element in to perform cyber operation.

Keywords: Cyber Intelligence, Cyber Warfare, Pre-CTO.

1 Introduction

In August 2008, when Russian troops invaded the Republic of Georgia, They just fought with troops and tanks. It was possible to attack because in advance, they performed DDoS attacks to government web sites and nation's primary web site. At that time, cyber warfare was highlighted new challenge of war. Cyber warfare is no longer a conflict in cyberspace but recognized as an aspect of warfare [1,2].

When cyber warfare is performed, there are necessarily needed cyber policies, strategies, and statics like physical warfare. For establishing them, we need cyber intelligence. This should correspond to the needs of the cyber commander, and is based on the cyber operation objective and the procedure of cyber operation plans. Especially, cyber intelligence has charge of very important role when Prepositional-

[2] He is a correspondent-author of this paper.

ISSN: 2287-1233 ASTL

cyber task oder(Pre-CTO) is processing. Pre-CTO procedure has six phases such as target recommendation, the selection of attack method, the decision of attack technique, attack launch, the remove of attack traces, and damage assessment. The role of intelligence is different for each phase in Pre-CTO. We will limit to Pre-CTO of cyber warfare for explain roles and responsibilities of cyber intelligence [2].

In this paper, we will describe the concept of cyber intelligence in section 2 and roles and responsibilities of cyber intelligence in section 3. We conclude in section 4.

2 The Concept of Cyber Intelligence

In physical warfare, intelligence provides the commander to various data for assessments and estimates that facilitate understanding the operational environment. This includes the organizations, capabilities, and processes involved in the collection, processing, analysis, dissemination, and assessment of information [3]. With reference to the definition of military intelligence, cyber intelligence refers the product resulting from the collection, processing, analysis, integration, evaluation, and interpretation of available data concerning hostile cyber organization, cyber forces capabilities, network system, and so on [4]. Cyber intelligence includes strategic, operational, and tactical cyber intelligence. Strategic cyber intelligence defines as intelligence that could destroy and breakdown a national level cyber asset. Operational cyber intelligence is intelligence that is required for planning and executing major cyber operations to accomplish cyber strategic objectives within cyberspace. These include target recommendation, the selection of attack method, damage assessment, etc. Tactical cyber intelligence defines as intelligence that is required for engagement and conduct of tactical operations. These include vulnerabilities, the main point of attack, the decision of attack techniques, etc [5].

The primary role of cyber intelligence is also to provide data and information to facilitate mission accomplishment in the cyberspace. It provides the necessary data and information to cyber commander and cyber units to accomplish strategic objectives when planning cyber operation and attacking hostile cyber infrastructure. Responsibilities of cyber intelligence are as follows. Firstly, it informs priority intelligence related to cyber operations to the cyber commander. The priority intelligence directly supports the highest priority needs of collected information related to enemy and cyberspace environment to the cyber commander for accomplishing the mission. Secondly, it is to describe the cyberspace environment that is composed of network, system, operation system, software, data, security system, and so on. Thirdly, it is to identify, define, and nominate objectives whether is system shutdown or network breakdown or information leakage or etc. Fourthly, it is to support the planning and maneuver of cyber operations. These responsibilities are very important to Pre-CTO procedure because there are objectives determination, target recommendation, the selection of attack method, the decision of attack technique, etc. There are additionally various responsibilities.

In this paper, we describe the role and responsibilities of intelligence in the Pre-CTO. And we will present the duty of intelligence must be performed at each phase in the Pre-CTO.

3 Roles and Responsibilities of Cyber Intelligence

The pre-CTO is a cyber-attack process made up as Air Force's pre-ATO (Prepositional-Air Tasking Order). The pre-ATO defines as a procedure used to task and disseminate to components, subordinate units, and command and control agencies projected sorties, capabilities and/or forces to targets and specific missions for three days from the outbreak of war. It normally provides specific instructions including fighter call signs, targets, weapons, and controlling agencies, etc., as well as general instructions. Pre-CTO guides cyber-attack according to the assigned procedure at each phase in real-time. The process of Pre-CTO has six phases such as following figure.

Fig 1 Process of Pre-CTO

Roles and responsibilities of cyber intelligence are as follows.

- Target Recommendation: Recommend the main point of attack that has the most vulnerability in target. Cyber intelligence collects information of hostile network system, identifies target had vulnerabilities, and recommends target could impacted critical damage to accomplish objectives.
- The Selection of Attack Method: Select attack method appropriate to the vulnerability of target. For example, if the objective of cyber-attack is to breakdown network, cyber intelligence provides DDoS attack.
- The Decision of Attack Technique: Decide attack technique suitable for the main point of attack after selected attack method. Cyber intelligence has to draw appropriate attack techniques and provide the priority of attack techniques among SYN, UDP, and HTTP flooding attack to cyber command.
- Attack Launch: Perform cyber-attack on target by the selected attack technique. If DDoS attack is performed, cyber intelligence must be continuously monitored zombie PC, master server, and management server that can be updated continuously. And if cyber operation environment is changed, it must provide needed information to cyber commander in real-time.
- The Remove of Attack Traces: Remove all traces of the cyber-attack by deleting log file, router access record, backdoor, and so on. Cyber intelligence must monitor backtracking from enemy.

- Damage Assessment: Assess effects of cyber-attack on target. If the expected effects did not get by the cyber-attack, cyber intelligence must provide new information to cyber command depending on his decision. If cyber command decides to attack other target, cyber intelligence has to perform duties by the process of Pre-CTO. If cyber command decides to re-launch the target again, cyber intelligence recommends other attack method and techniques to accomplish the objective of cyber operations.

Cyber intelligence announces the outbreak and termination of cyber warfare. So, roles and responsibilities of cyber intelligence are very important. In particular, when cyber operation plan is set up, and cyber-attack is performed at each phase of Pre-CTO, the duty of intelligence is a key of cyber operation.

4 Conclusion

We proposed roles and responsibilities of cyber intelligence at each phase in Pre-CTO. Pre-CTO guides cyber-attack according to the assigned procedure at each phase in real-time. The cyber intelligence should be prerequisites for assuring intelligence superiority in cyber warfare. This performs a key role in cyber operations. By presenting concrete roles and responsibilities of cyber intelligence, an effective cyber operation is able to perform. Cyber intelligence performs duties before the outbreak of cyber operation and it continues duties such as cyber operation of assessment, improvements derivation, etc after the cyber war.

Acknowledgement. This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2013S1A5A8023478)

References

1. Greengard, S.: The New Face of War, Communications of the ACM, Vol.53 No.12, pp.20-22 (2010)
2. Eom, J. H., Kim, N. U., Chung, T. M.: Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare, Proccedings of the 2012 International conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec2012), pp.295-299 (2012)
3. Dempsey, M.: Joint Intelligence, Joint Publication 2-0 (2013)
4. An introduction to cyber intelligence, http://www.Tripwire.com (2014)
5. Gortney, W.: Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (2014)

