International Journal of Software Engineering and Its Applications
Vol.8, No.9 (2014), pp.137-146
http://dx.doi.org/10.14257/ijseia.2014.8.9.11

Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace

Jung ho Eom

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

Abstract

In this paper, we proposed roles and responsibilities of cyber intelligence in cyber operations. In particular, we focused on the roles and responsibilities of cyber intelligence on each phase of cyber operations. Cyber operations are activities related to defense, assurance, and attack to achieve objectives in or through cyberspace. While cyber operation is conducting, cyber intelligence must properly support cyber commander and units for ensuring cyberspace intelligence superiority. 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 operation units. This is a key role in both cyber-attack and cyber defense. We know that the branch of information and communications conducts cyber operations in cyberspace. But we don't know well that the cyber intelligence is more in charge of the policy, strategic, and tactics in cyber operations. It is collected information requested from cyber command and units, and is disseminated information to department related to cyber operations. The cyber intelligence is a key factor in cyber operation cycle.

Keywords: *Cyber Intelligence, Cyber Operations, Cyber Warfare*

1. Introduction

According to security professionals, Unite 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 in advance, they conducted DDoS attacks to Georgia government homepage and nation's primary web site. At that time, cyber-attacks were highlighted new challenge of war. Cyber-attacks are no longer a conflict in cyberspace but recognized as an aspect of war. In Republic of Korea, over 10 government agencies, political parties, and media press have damaged website defacement and access block by DDoS attack originated from North Korea(estimated) in June 2013 [1-4].

Cyber-attacks should not be overlooked the level of threat or conflict in cyberspace. Cyber-attacks are maneuvers or actions performed in cyberspace as a war takes place in the physical space. So, organized cyber defense system should be established to prevent cyber-attacks. When cyber-attack or defense is performed, operation plan should be established, and 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 that facilitate understanding the operational environment. This includes the organizations, capabilities, and processes involved in the collection, processing, analysis,

ISSN: 1738-9984 IJSEIA

dissemination, and assessment of information. Without intelligence, operations can't be performed, and the superiority of war also can't secure. In cyber warfare, intelligence is very important factor to secure the superiority in cyberspace. 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 [5, 6].

In this paper, we proposed the roles and responsibilities of cyber intelligence in the cyber operations. The primary roles and responsibilities of cyber intelligence are to provide data and information to cyber commander and units to facilitate mission accomplishment for performing cyber operations. Cyber intelligence supports to planning, executing, and assessing cyber operations. It is very important key in the outbreak and termination of cyber operations. So, it should be precisely specified roles and responsibilities of cyber intelligence [5,6].

This paper organized as follows. We will describe cyber intelligence in section 2 and roles and responsibilities of cyber intelligence in section 3. In the section 4, we explain case study of roles and responsibilities of cyber intelligence in cyber operations, and conclude in the last section.

2. Cyber Intelligence

In kinetic warfare, intelligence defines as the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information such as foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. Information means the useful form of the data by filtering and processing raw data collected from intelligence, Surveillance, and Reconnaissance (ISR) system. It is a valuable data when it contributes to the commander's decision-making process by providing reasonable perception into future battle conditions or situations. The relationship among data, information, and intelligence is as following figure [5, 7].

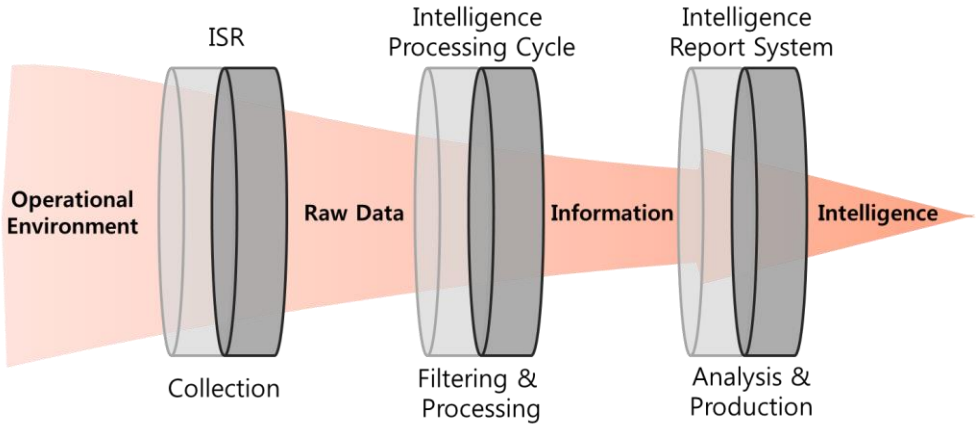

Figure 1. The Relationship among Data, Information, and Intelligence [5]

As above mention it, 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, hardware, software, data, threats, vulnerabilities, and so on. It is mainly to collect

information for or from cyberspace that is a global domain within the information environment consisting of the interdependent information communication infrastructures. Cyber intelligence for cyber operations ensures the ability to provide collaborative intelligence analysis, fused and integrated intelligence, and automated surveillance and reconnaissance capabilities to enable cyber operations. Surveillance and reconnaissance capabilities include including operation plan, information collection, processing and vulnerability exploitation, analysis and production, and dissemination. Cyber intelligence from cyberspace is any valuable information that we can collect from cyber operations environment. The flow of cyber intelligence occurs across the strategic, operational, and tactical level of cyber warfare. Strategic cyber intelligence defines as intelligence that provides all information related to make decisions and take action to cyber commander to achieve the goal of war, supports cyber operations across the range of military operations, assesses the current cyberspace environment, and estimates future cyber capabilities and intentions of adversaries that could affect the national cyber security. 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, impacts assessment, etc. Tactical cyber intelligence means intelligence that is required for engagement and maneuver of tactical operations. These include vulnerabilities, the main point of impacts, the decision of attack techniques, *etc.*, [8, 9]. Figure 2 shows the flow of cyber intelligence.

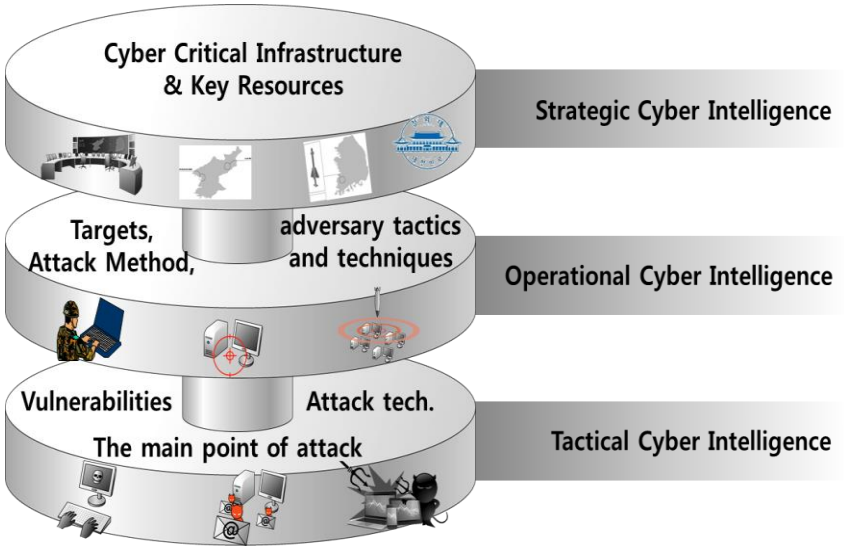

Figure 2. The Flow of Cyber Intelligence

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 cyber strategic objectives when planning cyber operations and attacking the hostile cyber infrastructure. Responsibilities of cyber intelligence are as follows. Firstly, it directly informs priority intelligence related to cyber operations to the cyber commander. The priority cyber intelligence directly supports the highest priority needs of collected information related to hostile cyber capabilities, cyber assets 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, hardware, operation system, software, data, security system, and so on. And it should be known influences that affect the maneuver of friendly and hostile cyber forces. Thirdly, it is to identify, define, and nominate objectives whether is system shutdown or network breakdown or information leakage or etc. So, cyber command has to decide objectives as considering hostile's probable intentions, last situation, objectives, strengths, critical capabilities, and so on. Fourthly, it is to support the planning and maneuver of cyber operations. These responsibilities are very important to cyber operations procedure because there are objectives determination, target recommendation, the selection of attack method, the decision of attack technique, etc. Fifthly, cyber intelligence assesses the effectiveness of cyber operation's attack on the hostile cyber assets with respect to objectives. There are additionally various responsibilities [5].

3. Roles and Responsibilities of Cyber Intelligence on Cyber Operations

Cyber operations are the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. They include computer network operation and activities to operate and defend the friendly cyber infrastructure. Computer network operation is the component of cyber operations that establishes operates, manages, and defends friendly cyber critical infrastructure and key resources, and attacks hostile cyber critical assets in cyberspace [8]. In this paper, we proposed roles and responsibilities of cyber intelligence on the process of cyber operations.

The process of cyber operations is a sequence of tactical maneuver with cyber strategic objectives in cyberspace. This process includes a portion of Pre-CTO (Cyber Task Order) that is a cyber-attack process made up like 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 [7]. Pre-CTO guides cyber-attack according to the assigned procedure at each phase in real-time. The process of cyber operations has seven phases including Pre-CTO like Figure 3.

• Information Collection: Collect data or information required to satisfy the intelligence requirements specified by the cyber commander. It should be collected priority intelligence requirement in the intelligence requirements. Priority intelligence requirement (PIR) is an intelligence requirement that expressed as a priority for intelligence support, which the cyber commander and units need to understand the situation of adversary and operational conditions in the cyberspace [5, 7]. Cyber intelligence for cyber operations includes as following according to information and national security alliance's 'Operational Levels of Cyber Intelligence' [11].

- Trend analysis of cyber warfare indicating the technical direction in which cyber capabilities of hostile forces are evolving

- Indications that hostile cyber forces have selected a technical approach for targeting your organization

- Indications that hostile cyber forces are building cyber capability to exploit a particular way of approach

- The revelation of hostile cyber force's tactics, techniques, skill, and procedures

- Understanding of the hostile cyber force's cyber operational cycle such as decision making, acquisitions, command and control method, etc.

- Technical, social, legal, economic, environmental other vulnerabilities of the hostile cyber forces

- Information that enables the defender to impact a hostile cyber forces as they move through the kill chain

• Target Recommendation: Detect and identify a target that has vulnerabilities and satisfies cyber command's intents. And cyber intelligence selects and prioritizes targets considering collected information, cyber operational requirements, and capabilities. Lastly, cyber intelligence recommends the main point of impacts that has the most vulnerability in target could impact critical damage to accomplish objectives. Most of target in cyber operations are time-sensitive target.

• The Selection of Attack Method: Select attack method enough to satisfy cyber commander's objectives, effective impact on the hostile forces, and appropriate to vulnerability of target considering friendly cyber capabilities, cyber weapons, techniques and skills. For example, if the objective of cyber-attack is to breakdown network, cyber intelligence provides DDoS attack.

• The Decision of Attack Technique: Recommend the most effective attack technique could be satisfied cyber operational objectives and suitable for the main point of impact. Cyber intelligence has to candidate the optimal attack techniques and provides the priority of attack techniques. For example, if he decides DDoS attack as attack method, cyber intelligence has to recommend the most optimal attack technique among SYN, UDP, and HTTP get flooding attack to cyber command.

• Cyber Maneuver: Perform cyber-attack on the main point of impact with the selected attack technique. Cyber maneuver is the application of cyber forces to disrupt, deny, degrade, destroy or manipulate network computing and data resources for achieving cyberspace superiority in respect to the adversary [12]. If HTTP get flooding is decide on above phase, cyber intelligence must be continuously monitored HTTP transaction, the change of web service, and the adversary's response. And if cyber operation environment is changed, it must provide PIR to cyber commander in real-time.

• The Removal of Attack Traces: Remove all traces of the cyber-attack by deleting log file, router access record, backdoor, and so on. In particular, when target or cyber maneuver is changed, the existing action record must be cleared. And cyber intelligence must monitor backtracking from enemy.

• The Assessment of Attack Impacts: estimate impacts on target system resulting from cyber maneuver. In cyber operations, functional damage assessment is mostly performed. If the expected effects did not get by the cyber maneuver, cyber intelligence must provide new PIR 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 operations. If cyber command decides to re-launch on the same target again, cyber intelligence recommends other attack method and techniques to accomplish the objectives of cyber operations.

Figure 3. The Process of Cyber Operations

4. The Case Study

In this chapter, we explain how cyber intelligence supports cyber operations according to the process of cyber operations. In information collection phase, it collects the information needed for cyber operations, using information collection tool such as scanning tools, vulnerability analysis tools and so on. Recently, malware like Stuxnet and Duqu is included information collection function, and provides the necessary information. U.S's National Security Agency works on program named PRISM which is a clandestine mass electronic surveillance data mining program launched in 2007. It collects stored Internet communications based on demands made to Internet companies such as Google [13]. Cyber intelligence collects information related to server as following table.

Table 1. The Example of Information Collection

Type	Server
Name	Solaris 11
Information	UNIX based Operation System developed by Sun Microsystems Supports architecture such as SPARC, x86, AMD64, IA-32, etc. Use Common Code Base Cloud security on all layers Software package, network and server virtualization, storage security File system, kernel, VM, system call vulnerabilities

In target recommendation phase, cyber intelligence must determine target appropriated to attack for achieving cyber command's objectives, not determines the target had the most vulnerability. If cyber commander decide Solaris 11 server as attack target and system paralysis as his objectives, cyber intelligence recommends vulnerabilities as following table to cyber commander. This table is including CVE(Common Vulnerabilities Exposure) list related to Solaris 11 server. All vulnerabilities in the table are related to the availability. But the main points of impact related to vulnerabilities are different. So, cyber intelligence should recommend the main point of impact could achieved cyber command's objectives

Table 2. The Example of Vulnerability [14]

ID	Description
CVE-2013-3799	Unspecified vulnerability in Oracle Solaris 10 and 11, when running on AMD64, allows local users to affect availability via unknown vectors related to Kernel
CVE-2013-3797	Unspecified vulnerability in Oracle Solaris 11 allows local users to affect availability via unknown vectors related to File system/DevFS.
CVE-2013-3787	Unspecified vulnerability in Oracle Solaris 10 and 11 allows remote attackers to affect availability via unknown vectors related to Kernel.
CVE-2013-3765	Unspecified vulnerability in Oracle Solaris 11 allows local users to affect availability via unknown vectors related to Kernel/VM
CVE-2013-3765	Unspecified vulnerability in Oracle Sun Solaris 11 allows local users to affect availability via unknown vectors related to Network Configuration

In the selection of attack method phase, cyber intelligence must recommend attack method appropriated to MPI(Main Point of Impact) for accomplishing system paralysis. MPI is one of Kernel, File system, VM including in the CVE list. If cyber commander decide File system as MPI, cyber intelligence recommends attack method considering MPI and system paralysis. DDoS attack is generally used to be disabling to network or system. 6.25 cyber terrors happened at Korea in 2013 also include DDoS attack method. However, DDoS attack may the final objectives to paralyze system, and it is also used as one means for achieving another attack aims.

In the decision of attack technique phase, cyber intelligence must recommend attack technique in the SYN flooding, UDP flooding, ICMP flooding and HTTP get flooding. Recently, DDoS attack does not use only one attack technique because it evolves into a form of APT(Advanced Persistent Threat). Customized malware is often programmed to more sophisticated and powerful attacks considering attack target and cyberspace conditions. In here, supposed to recommend HTTP get flooding attack. It is good that cyber intelligence describes attack progress, results, effects, etc. for cyber commander through the cyber war simulation. Cyber intelligence should inform several attack techniques applied simulation results to cyber command for choosing the most effective technique.

In the cyber maneuver phase, HTTP get flooding is conducting. It is a DDoS attack technique that HTTP transaction is processed after processing normal TCP connection. It continuously requests HTTP Get to the server, and then server performs HTTP request process as well as normal TCP session. Then, HTTP process module is overloaded. Before cyber maneuver is launched, cyber intelligence should check the threshold value set of the

TCP connection requests and HTTP Get request as collecting security system of the hostile cyber forces. And cyber intelligence should continuously monitor the activities of the hostile security system.

The removal of attack trace is necessary to hide the attack source or avoid the hostile cyber force's backtracking. Cyber intelligence supports removal methods such as delete log file, router access record, backdoor, etc. to cyber operation teams. The more sound removal method is to destroy the Master Boot Record(MBR) or delete all the existing records as forcing shut down the system. In addition, attack trace could be hidden as deleting the program file after overwriting a string at program files. Cyber intelligence supports the information of the most optimal and effective removal method and process to cyber operation teams.

In the assessment of attack impact phase, cyber intelligence must estimate impacts of target system resulting from cyber maneuver. Cyber intelligence performs physical, functional, and component impact assessment on target system. Cyber intelligence evaluates the degree of physical impact such as hard disk's MBR destruction, the degree of functional impact such as HTTP process overload, and the degree of component impact such as packet transmission delay. Moreover, cyber intelligence has to collect recovery time that target system is capable of performing the normal function, and the alternative system. We continuously should research the method of impact assessment because there is no method for estimating an accurate impact.

5. Conclusion

We proposed roles and responsibilities of cyber intelligence in cyber operations. In this paper, we focused on the roles and responsibilities of cyber intelligence on each phase of cyber operations. Cyber operations are activities related to defense, assurance, and attack to achieve objectives in or through cyberspace.

Cyber intelligence defines the product resulting from the collection, processing, analysis, integration, evaluation, and interpretation of available data concerning hostile cyber organization, cyber forces capabilities, network system, hardware, software, data, threats, vulnerabilities, and so on. It is mainly to collect & disseminate information for or from cyberspace that is a global domain within the information environment consisting of the interdependent information communication infrastructures. The primary role of cyber intelligence is to provide data and information to facilitate mission accomplishment in the cyberspace. It also provides the necessary data and information to cyber commander and cyber units to accomplish cyber strategic objectives when planning cyber operations and attacking hostile cyber infrastructure. Responsibilities of cyber intelligence are different according to each the phase of cyber operations. Cyber intelligence collects data or information required to satisfy the intelligence requirements specified by the cyber commander in the information collection phase. It detects and identifies a target that has vulnerabilities and satisfies cyber command's intents in the target recommendation phase. It recommends attack method enough to satisfy cyber commander's objectives in the selection of attack method phase. It has to candidate appropriate attack techniques and provides the priority of attack technique in the decision of attack technique. It should continuously monitor our attack action and the activities of the hostile security system in the cyber maneuver phase. It supports removal methods such as delete log file, router access record, backdoor, etc. to cyber operation branch in the removal of attack traces phase. It estimates impacts on target system resulting from cyber maneuver in the assessment of attack impacts phase.

In future, we will develop cyber intelligence action cycle system systematically as integrating roles and responsibilities on cyber operation and military information cycle.

Acknowledgements

"This paper is a revised and expanded version of a paper entitled [The Role and Responsibility of Cyber Intelligence in Cyber Warfare] presented at [ITCS2014, Saipan and 17~20 July]."

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

References

[1] N. Kshetri, "Cyberwarfare: Western and Chinese Allegations", ITProfessional, **(2014)** January-February, pp. 16-19.
[2] J.-H. Shin, S.-P. Cheon, and J.-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, Saipan USA, **(2014)** July 17-20.
[3] T.-M. Chung, J.-H. Eom, S.-H. Kim and N.-U. Kim, "Information Security: Ask and Answer", Hongneung Publishers, Seoul, **(2014)**.
[4] J. 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.
[5] M. E. Dempsey, Joint Intelligence, Joint Publication 2-0, **(2013)**.
[6] An introduction to cyber intelligence, http://www.Tripwire.com, **(2014)**.
[7] W. E. Gortney, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, **(2014)**.
[8] M. A. Vane, "Cyberspace Operations Concept Capability Plan 2016-2018", TRADOC Pamphlet 525-7-8, **(2010)**.
[9] M. M. Hurley, "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance", Air & Space Power Journal, **(2012)**, pp. 12-33.
[10] J.-ho Eom, N.-uk Kim and T.-M. Chung, "Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare", The Proceedings of the 2012 International conference on Cyber Security, Cyber Warfare and Digital Forensic, Kuala Lumpur Malaysia, **(2012)** June 26-28.
[11] G. Bamford, J. Felker and T. Mattern, "Operational Levels of Cyber Intelligence", Intelligence and National Security Alliance, **(2013)**.
[12] S. D. Applegate, "The Principle of Maneuver in Cyber Operations", The proceedings of The 4th International Conference on Cyber Conflict, Tallinn Estonia, **(2012)** June 5-8.
[13] PRISM (surveillance program), http://en.wikipedia.org/wiki/PRISM_(surveillance_program).
[14] CVE List, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=solaris.

Authors

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. His research interests are information security, cyber warfare, network security.