Cyber Military Strategy for Cyberspace Superiority in Cyber warfare

Jung-Ho Eom
Dept. of Military Studies
Daejeon University
Daejeon, Republic of Korea
eomhun@gmail.com

Nam-Uk Kim
Department of Electrical
and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea
nukim47@imtl.skku.ac.kr

Sung-Hwan Kim
Department of Electrical
and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea
shkim47@imtl.skku.ac.kr

Tai-Myoung Chung
School of Information
Communication Engineering
Sungkyunkwan University
Suwon, Republic of Korea
tmchung@ece.skku.ac.kr

***Abstract*—In this paper, we proposed robust and operational cyber military strategy for cyberspace superiority in cyber warfare. We considered cyber forces manpower, cyber intelligence capability, and an organization of cyber forces for improving cyber military strategy. In cyber forces power field, we should cultivated personals that can perform network computer operations and hold cyber security technology such as cyber intelligence collection, cyber-attack, cyber defence, and cyber forensics. Cyber intelligence capability includes cyber surveillance/reconnaissance, cyber order of battle, pre-CTO, and cyber damage assessment. An organization of cyber forces has to change tree structure to network structure and has to organize task or functional centric organizations. Our proposed cyber military strategy provides prior decision of action to operate desired effects in cyberspace.**

Keywords*— *cyberspace superiority, cyber military strategy, security

I. INTRODUCTION

Recently, as targeted attacks have significantly increased in cyberspace, there has been increased awareness and information about targeted attacks. Targets of all targeted attacks can be divided into a specific organization and specific software or IT infrastructure. The type of attack on the former is directed at a specific organization and the aim of an attacker is unauthorized access to confidential intelligence such as operational secrets. The type of attack on the latter is not directed at a specific organization and his/her target is the data associated with a certain kind of software such as SCADA systems [1]. The typical example of targeted attack is stuxnet

Stuxnet has raised the concern of security experts for as following reasons: target choice, sophistication, and implications for future malware. The stuxnet is highly selective about its targets and specific condition. Security experts have estimated that stuxnet requires manpower to develop stuxnet to have been five to ten people working for six months to access to SCADA systems. They also have believed that stuxnet is the first real cyber weapon because it is aimed at a physical and military target [2].

Some security experts agree that cyber warfare is now happening among nations. It is the time to prepare for battle in cyberspace. Many nations found cyber warfare policies and increase the budget for cyber warfare, and are accelerating to develop cyber weapons. Cyberspace superiority should be firstly achieved to win in cyber warfare. We will propose cyber military strategy for cyberspace superiority in term of national defense strategy.

In section 2, we describe definition of cyber warfare, and present cyber military strategy for cyberspace superiority in section 3. We conclude in section 4.

II. DEFINITION OF CYBER WARFARE

A. Cyberspace, Cyberspace Operation, and Superiority

The incident estimated as the first cyber warfare was a distributed denial of service (DDoS) attacks on Estonian important web sites starting on April 2007. Suspicions about the attacker of the DDoS attacks immediately fell on Russia [2]. Recently, a foreign intelligence service swiped 24,000 computer files from a US defense contractor in 2011, which was one of the largest cyber-attacks on a Pentagon supplier. Deputy Defense Secretary William Lynn said “It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies”. The cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs and the Joint Strike Fighter," he said. Cyber-attack on the military network and systems is rapidly increasing, and the damage is becoming serious day by day [3,4].

Cyber-attack is broken out in cyberspace located within the information environment composed of users, organizations, networks and systems that collect, process, disseminated or execute on information. In other words, Cyberspace is a global domain within the information environment consisting of the internet, communications networks, computer systems, and embedded processors and users. The military works are increasingly dependent on computer network systems in cyberspace. Cyberspace is a source of both strength and vulnerability for modern/future war. While cyberspace operations plays important role in a modern/future war, they also create critical vulnerabilities to attack or exploit for our

enemies. Enemies may attempt to deny, manipulate, disrupt, or destroy critical infrastructures and sensitive data through cyber-attack, thus affecting C4I systems and the nation. In case of the U.S air force, they depend upon critical infrastructure and key resources for many of their military activities. They also is thinking that physical security is no longer sufficient as most critical infrastructure is under cyberspace like as following figure 1 [5,6].

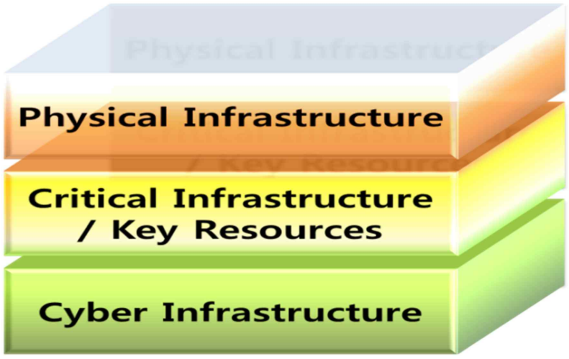

Figure 1. Cyberspace Infrastructure [7]

To achieve war objectives in the modern/future warfare, it is very important to keep the superiority in cyberspace. Cyberspace superiority defined as the operational advantage in, through, and from cyberspace to conduct military operations at a given time and area without interruption. The concept of cyberspace superiority is dependent on the idea of preventing interruption to joint our forces from enemies, which would block joint our forces from creating their final goal. Cyberspace superiority may provide sufficient freedom of operations to create the final goal [6]. To keep the cyberspace superiority, military operation conducted in cyberspace is called cyberspace operations. Cyberspace operations include computer network operations and actions to operate and defend the global information system [8].

B. The definition of Cyber Warfare

Cyber warfare can be a war between nations through cyberspace operations in cyberspace. But cyber warfare could also occurred by non-state actors in various ways [9]. Cyber warfare occurs by cyberspace operations that extend cyber power beyond the defensive boundaries of the GIG (Global Information Grid) to detect, deter, deny, and defeat enemies. Cyber warfare uses cyber exploitation, cyber-attack, and cyber defense in a cyberspace [10].

- Cyber exploitation: computer network exploitation with enabling capabilities such as vulnerabilities exploit, password cracking, and others for intelligence collection and other efforts
- Cyber-attack: computer network attack with other enabling capabilities such as hacking, malicious code, physical attack, and others to deny, destroy or manipulate data and/or infrastructure
- Cyber defense: policy, strategy, sensors, and automated processes to identify, detect and analyze malicious behaviors, simultaneously execute prepared response activities to defeat cyber-attacks before they can do threat

The characteristics of cyber warfare are as followings [9].

- Cyber warfare can enable cyber-attackers to achieve their military and strategic goals without the need for physical armed conflict.
- Cyberspace gives asymmetrical war power to small and relatively insignificant cyber-attackers.
- Using false IP addresses, foreign servers and false names, cyber-attackers can conduct with almost complete anonymity and relative impunity, at least in a given time.
- The boundaries of cyberspace are difficult to divide between the military and the civilian and between the physical and the logical; and cyber power resources are such as states or non-state actors, or proxy.
- Cyberspace defined as fifth battle space with the more traditional arenas of land, air, sea and space. Cyber warfare is viewed as a new but not entirely separate component of many-sided war field.
- Operations in cyberspace are more likely to occur in corporate with other forms of compulsion and confrontation. However, the ways and means of cyber warfare remain undeniably distinct from these other modes of war.

It is very important to formulate cyber military strategies for ensuring cyberspace superiority in cyber warfare. In next chapter, we proposed robust and operational cyber military strategies in three ways.

III. CYBER MILITARY STRATEGIES

A. Cyber forces manpower

Suppose that cyber operations strategy, tactics, cyber infrastructure, and cyber weapons are fully equipped. But if cyber warriors who can apply cyber strategy and tactics to cyber operations with cyber weapons in cyberspace are not, what will happen? In cyber warfare, cyber force's growing reliance on cyberspace requires well-educated and trained cyber warriors. They are composed of cyberspace operators and leaders who are ready to provide the required capability and capacity for operational goal accomplishment. Cyber warrior or professional with technical and tactical expertise are operational mission based individuals. Cyber warriors should possess high levels of technical knowledge, robust analytical skills, and an eminent understanding of cyber warfare. Cyber forces has to develop and manage them in the most effective education and training way [6,10].

So, cyber warriors should have three kinds of knowledge. First, they must understand military policy, cyber strategies and tactics. They should be able to work out strategies and tactics according to national defense policy for achieve the warfare objectives. Especially, cyber commander has leadership to lead cyber warriors and should be placed cyber warriors in the right place at the right time.

Second, they should be fluent in cyberspace operations. They should possess capacity and capability related to cyber exploitation, cyber-attack, and cyber defense. They also should be applied cyberspace operations to cyber war according to the change of enemy's cyberspace environment. Even though they have robust cyber-attack and security technology, even if they don't know cyberspace operations, cyberspace superiority could be not achieved.

Finally, they should be well informed cyber intelligence collection, cyber-attack and defense technology. Cyber intelligence collection enumerates system specification and exploits vulnerabilities of enemy's network and system by scanning tools. Cyber-attack technologies include such as hacking, sniffing, spoofing, hijacking, and DDoS, etc. Cyber defense technologies have intrusion detection system, firewall, intrusion prevention system, and honey system, etc. Cyber warriors must know how to appropriately implement cyber-attack and defense technologies in accordance with cyberspace operations.

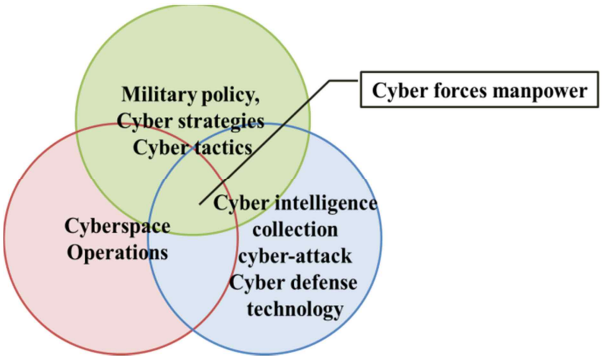

Figure 2. Requirements for cyber forces manpower

B. Cyber intelligence capability

Cyber intelligence capability should be prerequisites for keeping cyberspace superiority. In a physical warfare, the first priority is to acquire intelligence like as follows figure 3.

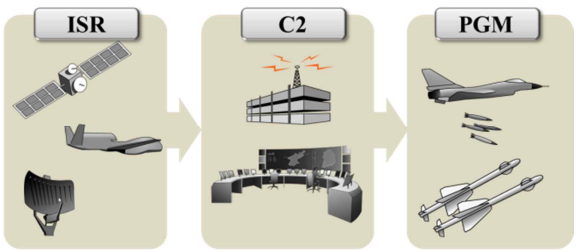

Figure 3. C4ISR+PGM Process [11]

The ISR (Intelligence, Surveillance, and Reconnaissance) was underway prior to the outbreak of warfare, and means the beginning of the battle. It is no exception in cyber warfare. It is very important to conduct surveillance cyber-attacks and collect information of cyber-attack aspects. So, we proposed a layered surveillance system for effectively monitoring cyber-attack like figure 4 [12]. Global cyber defense system means early global response system, national cyber defense system monitors intrusion to critical government infrastructure and SCADA, and military cyber defense system conducts surveillance about DoD, Army, Navy, and Air. Finally, personnel cyber defense system watches systems of officers, sergeants, soldiers, and civilian war workers.

Figure 4. Layered cyber surveillance system

Second, we have to make up the cyber order of battle. This includes detailed information of target systems or our systems such as network, server, and database, etc. It is useful to cyber response attacks if we are identifying information about the target systems. If we know precisely the information about our system, we can establish robust security measure in terms of response. Table I describes the example of the cyber order of battle [13].

TABLE 1. AN EXAMPLE OF THE CYBER ORDER OF BATTLE

Sys. name: Intel Pent4
CPU: 2.4GHz
RAM: 1GB
IP Address: 10.1.1.65
Gateway: 10.1.1.1
OS: Microsoft Window 7
Location: General Affairs
ID&P/W: tomwash&not34qaz
User: Mike
Position: manager
Duty: programming
Rights in the DCD: r, w, e
Sensitive data: /user, /user/affair, /etc.
TaskFile : /user/affair/manager/schedule/*.c

Third, we have to develop pre-CTO (Prepositional-Cyber Task Order). The pre-CTO is made up as Air Force's pre-ATO(Prepositional-Air Tasking Order). The pre-ATO defines as a method 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 to include fighter call signs, targets, weapons, and controlling agencies, etc., as well as general instructions [8]. The pre-CTO includes target system, vulnerabilities, hacking tool, master/zombie serve, and attack

time, etc. We also have to concern about real time exploit and attack. Of course, we already know zero-day attack, but we are necessary to establish the robust attack process on target system. An attack process is as follows figure 5; target identification – MPI (Main Point of Impact) exploit - hacking plan - hacking shooter - damage assessment.

Figure 5. Cyber attack process

- Target identification: decides most vulnerable target system that can wreak havoc.
- MPI exploit: selects one of the most vulnerable weak points of the identified vulnerabilities.
- Hacking plan: determines attack goal, method, time, and so on.
- Hacking shooter: actually conducts hacking on target system.
- Damage assessment: estimates the extent of damage after the attack.

Fourth, we should developed CDA(Cyber Damage Assessment) method for an accurate damage assessment by cyber-attacks. BDA(Battle Damage Assessment) is the estimate of damage resulting from the application of fatal or non-fatal military force in physical warfare. The BDA is composed of physical and functional damage assessment, and target system assessment [8]. The CDA is the estimate of damage resulting from cyber-attacks by the enemy, but includes assessing the extent of damage after we conduct cyber respond attack to the enemy. The CDA is consisted of operational, functional, and component damage assessment on target system.

Finally, we should improve the capability of cyber psychological operation. Cyber psychological operation defined as the propaganda and other planned all activities affecting opinions, feelings, attitudes of all countries and groups for effectively achieve the purpose of national defence policy in cyberspace [14]. In Iraq war, the allies have ever conducted elaborate cyber psychological operation that persuades asylum or surrender to high-ranking personals using e-mail and cell phones in cyberspace. Cyber psychological operation is more effective to perform with the public affair operation.

C. Organizations of cyber forces

Organizations of cyber forces are mission or functional centric organizations unlike any other organizations. For example, the department which continuously monitors cyber-attacks has to work for 24 hours, but the cyber-attacks response department has to solve in a few minutes or seconds as soon as cyber-attack occurs. The cyber-attacks analysis department researches attack pattern after finishing cyber-attack. Organizations of cyber forces should be organized in networked structures for sharing cyber-attacks information in real-time.

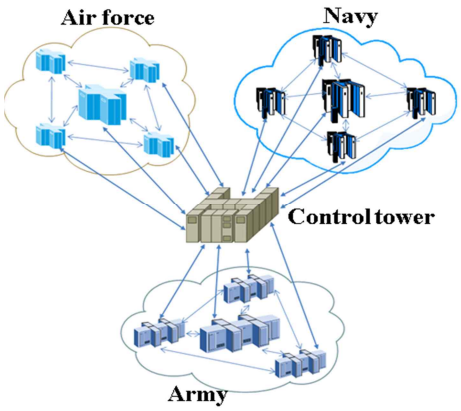

Figure 6. Networked structure of orgnization of cyber forces

Control tower is also required for control and manages consistently the scattered organizations of cyber forces as above figure 6.

IV. CONCLUSION

This paper proposed robust and operational cyber military strategies for cyberspace superiority in cyber warfare. We presented cyber military strategies in three ways.

First, we should strengthen cyber forces manpower. We need well-educated and trained cyber warriors. They should have at least three kinds of knowledge. First, they must understand military policy, cyber strategies and tactics. Second, they should be fluent in cyberspace operations. Finally, they should be well informed cyber intelligence collection, cyber-attack and defense technology.

Second, cyber intelligence capability should be prerequisites for keeping cyberspace superiority. We proposed a layered surveillance system for effectively monitoring cyber-attack. Second, we have to make up the cyber order of battle. This includes detailed information on target systems or our systems such as network, server, and database, etc. Third, we have to develop pre-CTO. The pre-CTO includes target system, vulnerabilities, hacking tool, master/zombie server, and attack time, etc. Fourth, we should developed CDA method for an accurate damage assessment by cyber-attacks. Finally, we should improve the capability of cyber psychological operation. Cyber psychological operation defined as the propaganda and other planned all activities affecting opinions, feelings, attitudes of all countries and groups for effectively achieve the purpose of national policy in cyberspace.

Finally, organizations of cyber forces are mission or functional centric organizations unlike any other organizations.

978-1-4673-1677-4

Organizations of cyber forces should be organized in networked structures for sharing cyber-attacks information in real-time.

REFERENCES

[1] Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, “Stuxnet uder the microscope”, www.eset.com, 2011.

[2] Thomas M. Chen, “Stuxnet, the Real Start of Cyber Warfare?”, the magazine of global internetworking, 2010.

[3] http://www.zdnet.com.

[4] Jung ho Eom, Nam uk Kim, Sung hwan Kim and Tai Myoung Chung, “An Architecture of Document Control System for Blocking Information Leakage in Military Information System” International Journal of Security and Its Applications, Vol.6 No.2, pp.109-114, 2012.

[5] William Tl Lord, “Cyberspace Operations; Air Force Space Command Takes the Lead”, High Frontier, Vol.5 No.3, pp.3-5, 2009.

[6] “Cyberspace operations”, Air Force Doctrine Document 3-12, Air force U.S, 2010.

[7] Patrick Beggs, “Securing the Nation’s Critical Cyber Infrastructure”, Department of Homeland Security, 2010.

[8] “Department of Defense Dictionary of Military and Associated Terms”, Joint Publication 1-02, Joint chiefs of staff, 2010.

[9] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, “On Cyber Warfare”, A Cahtham House Report, 2010.

[10] “Cyberspace Operations Concept Capability Plan 2016-2028”, TRADOC Pamphlet 525-7-8, 2010

[11] Jungho Eom, et al, “An introduction of Cyber Warfare-Attack and Security Techniques”, hongpub, 2012.

[12] Hong seob Lee, “cyber attack prevention and the advancement of response system for IT839 infrastructure protection”, Information Security Review, Vol.1 No.3, 2004.

[13] Jung-hoEom, Min-woo Park, Seon-ho Park and Tai-myoung Chung, "A Framework of Defense System for prevention of Insider's Malicious Behaviors", ICACT2011, 2011.

[14] Ki joong Lee, “A study on Alternatives of Cyber Psychological Warfare of republic of Kore”, Journal on KIAS, Vol.8 No.1, 2008.