Section 3. Trends Concerning Cyber Warfare Capabilities

1. Cyberspace and Security

Owing to the information technology (IT) revolution in recent years, information and communication networks such as the Internet are becoming essential components across all facets of people's lives. Cyber attacks against these information and communication networks, especially those which are the infrastructure for daily life, have the potential to seriously impact people's lives. As such, cyber security constitutes an important challenge in terms of security for each country.

Types of cyber attacks include data falsification or theft of information via unauthorized access to information and communication networks, the functional impairment of information and communication networks through the simultaneous transmission of large quantities of data, and so on. Internet related technologies are constantly evolving, with cyber attacks growing more sophisticated and complex day by day. The following points could be listed as characteristics of cyber attacks.

1) Attacks can be carried out that do not injure people or objects physically, and without actually coming into contact with them.
2) If they are able to generate hindrances for important information and communication networks then they can inflict enormous damage.
3) Since there are no geographical or temporal limitations, attacks can be carried out at any time and from anywhere.
4) They adopt a variety of different means, such as going through a countless number of computers that have been under control of computer viruses so that the involvement of the attackers themselves cannot be identified. Because of this, it is difficult to identify the attackers based on direct evidence.

For the armed forces, information and communications forms the foundation for command and control which extends all the way from central command to ground-level forces, with the dependence of units on information and communication networks expanding still further due to the IT revolution. Given this dependence of the armed forces on such information and communication networks, cyber attacks are being regarded as an asymmetrical strategy capable of mitigating the strengths of enemies while also exploiting weak points in enemy armed forces. It has also been pointed out that intrusions are carried out into enemy information and communication networks for the purpose of gathering intelligence[53].

Under such circumstances, cyber attacks are rampant against the information and communications networks of the armed forces of various countries[54]. In recent years, an exchange of cyber attacks was deemed to have occurred in the military conflict between Israel and Hezbollah in 2006 and in the one between Israel and Hamas in 2008. Additionally, when the Georgia conflict broke out in August 2008, the Georgian Presidential Office, Ministry of Defence, media, banks, and others suffered large-scale cyber attacks. These cyber attacks did not have a major effect on the activities of the Georgian Armed Forces. However, they made it impossible to view websites that expressed the official views of the Georgian government, and are thought to have interfered with some government functions[55]. What is more, cyber attacks also occurred in July of last year against information and communication networks in the United States and South Korea, including those of government agencies such as the U.S. Department of Defense and South Korea's Ministry of National Defense[56].

2. Efforts on Cyber Warfare

Given this magnification of threats in cyberspace, dealing with cyber attacks and ensuring the safety of activities in cyberspace are matters of critical importance for the armed forces of each country, and so efforts on cyber warfare are being emphasized within defense policies. For example, various countries are taking measures, as exemplified by the new establishment of agencies that oversee military operations in cyberspace, and by regarding efforts on cyber warfare as important strategic objectives within defense strategies.

Based on the Cyberspace Policy Review released in May 2009, the United States newly established the post of Cyber Security Coordinator within the White House to carry out coordination among the relevant government agencies with regard to cyber security policy. In the Department of Defense, Secretary of Defense Gates decided to establish the U.S. Cyber Command (USCYBERCOM) to oversee operations in cyberspace in June 2009. USCYBERCOM attained Initial Operational Capability (IOC) in May of this year and its full capability is set for October of this year. What is more, the Quadrennial Defense Review (QDR) released in February of this year listed land, sea, air, space, and cyberspace as "global commons," stating that it is essential to secure access to these global commons. Furthermore, it also defines effective operations in cyberspace as one of six key mission areas for enhancing the capabilities of the U.S. armed forces.

The North Atlantic Council (NAC), which is the supreme decision making body within the North Atlantic Treaty Organization (NATO), oversees policies and operations concerned with NATO's cyber defense, and has its own cyber defense policy. In 2008 the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE) was newly established to conduct research on cyber warfare.

Within the Defense White Paper released last year, Australia stated that it must improve its cyber warfare capabilities. In January of this year the Cyber Security Operations Centre (CSOC) was launched under the Defence Signals Directorate (DSD) in the Department of Defence.

South Korea established a Cyber Command to carry out planning, implementation, training, and research and development for its cyber warfare capabilities under the Defense Intelligence Agency in January of this year.