Section 2 Trends Concerning Cyberspace

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. But the other side of the coin is that 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 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 armed forces on such information and communication networks, cyber attacks are being regarded as an asymmetrical strategy capable of mitigating the strengths of enemies by exploiting weak points in enemy armed forces, and it is said that many militaries are developing offensive capabilities in cyberspace[1]. It has also been pointed out that intrusions are carried out into information and communication networks of other countries for the purpose of gathering intelligence[2].

2 Threats in Cyberspace

Under such circumstances, cyber attacks are rampant against the information and communication networks of the governmental organizations and armed forces of various countries[1].

In 2008, removable memory devices were used to insert a computer virus into networks that handled classified and other information for the U.S. Central Command, the unit commanding the U.S. military's operations in Iraq and Afghanistan. This spawned a grave situation where there was the possibility that information had been transferred externally[2]. What is more, cyber attacks also occurred in July 2009 against the websites of government agencies in the United States and the ROK including the U.S. Department of Defense and the

1-1 Paper by then Deputy Secretary of Defense William J. Lynn, "Defending a New Domain: The Pentagon's Cyber Strategy", Foreign Affairs (Sep-Oct 2010). In addition, an annual report by the U.S.-China Economic and Security Review Commission (November 2011), a bipartisan consultative body of the U.S. Congress, indicated that the Chinese military engages in computer network attacks and assessed that China's military strategy envisions the use of computer network exploitation and attack against adversaries, including the United States.

2 In a February 2011 speech, then Deputy Secretary of Defense William J. Lynn pointed out cases of intrusion by foreign intelligence agencies, including the extraction of military plans and weapons systems designs from governmental networks. Moreover, the United States Department of Defense report "Military and Security Developments Involving the People's Republic of China" (May 2012) indicated that computer networks and systems around the world, including those owned by the U.S. Government, continued to be targets of intrusions and data theft, many of which originated within China.

2-1 An annual report released by the U.S.-China Economic and Security Review Commission (November 2011) indicated that during 2010 there were a total of 55,812 counts of malicious cyber activity carried out on the United States Department of Defense.

2 Aforementioned paper by then Deputy Secretary of Defense William J. Lynn. An infected removable memory device was inserted into a computer at a U.S. base in the Middle East, and the virus, placed there by a foreign intelligence agency, was uploaded to the network of the Central Command. This virus was undetected and spread over systems that handle both classified and unclassified information, and data could have been transferred to servers under foreign control.

ROK's Ministry of National Defense, and in March 2011 against the websites of the ROK's governmental agencies, including the Ministry of National Defense[3]. These attacks disrupted the access to those websites and caused other problems.

Stuxnet, an advanced computer virus with a complex structure discovered in July 2010, was the first virus program to target the control system incorporated in specific software and hardware. It has been pointed out that Stuxnet has the ability to access targeted systems without detection and to steal information and alter the system[4]. In October 2011, a new virus was discovered, which appeared to be very similar to Stuxnet in terms of its structure[5].

In September 2011, computers of Japanese private companies producing defense equipment were found infected with malware and legislative and administrative organs were also attacked in the same year.

Cyber attacks on the information and communications networks of governments and militaries as well as on critical infrastructure significantly affect national security. Japan must continue to pay close attention to developments in threats in cyberspace.

3 Efforts against Cyber Attacks

Given these growing threats in cyberspace, various efforts are under way on the overall government level and the ministerial level, including by defense ministries.

As per cyber security policy that is being employed by countries on the governmental level, there seem to be some trends, including: 1) organizations related to cyber security that are spread over multiple departments and agencies are being integrated, and their operational units are centralized; 2) policy and research units are being enhanced by establishing specialized posts, and creating new research divisions and enhancing such functions; 3) the roles of intelligence agencies in responding to cyber attacks are being expanded; and 4) more emphasis is being allotted to international cooperation.

Also, on the defense ministry level, response to cyber attacks and ensuring safety for activities conducted in cyberspace have become vital issues for the militaries of various countries. There are various undertakings being carried out against cyber attacks in different countries, including establishing new organizations to head military operations in cyberspace and placing response to cyber attacks as an important strategic objective in national defense strategies[1].

Furthermore, attention has been drawn to issues that must be debated in order to allow for an effective response to cyber attacks, which have become a new security challenge in recent years. For instance, there is still no wide consensus on the norms covering conduct of states and international cooperation in cyberspace. In consideration of these problems, debate has been taking place[2] with the aim of promoting new efforts, such as formulating certain norms of conduct within cyberspace based on international consensus[3].

In November 2011, the U.K. government hosted an international conference on cyberspace. Issues discussed at the conference include economic growth and development in cyberspace, social benefits, safe and reliable access,

2-3 Speeches by Chairman of the then Joint Chiefs of Staff Admiral Mike Mullen (July 8, 2009) and then Deputy Secretary of Defense William J. Lynn (October 1, 2009). In April 2011, the Korean National Police Agency (ROK) reported that the cyber attack on the ROK's Government that occurred in March 2011 was carried out by the same source as the cyber attack of July 2009.

4 March 2011 testimony of Department of Homeland Security, then Deputy Under Secretary Reitinger before the U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

5 ICS-CERT (a U.S. government organization in charge of cybersecurity of industrial control systems) released an alert on a computer virus called Duqu (W32.DUQU) in October 2011. According to analysis by a private research lab, the program of the virus has many similar characteristics to Stuxnet.

3-1 Countries other than those outlined in the main text have also been making efforts within the defense structures. For example, the spokesperson of the Ministry of National Defense of the People's Republic of China announced at the regular press conference held on May 25, 2011, that the "Online Blue Army" has been established within the People's Liberation Army in order to better safeguard the network security of armed forces.

2 Besides the mentioned discussions, it is difficult to identify the attacker in the case of cyber attack, and, as in many instances the attacker has nothing to protect, deterrence is said to be difficult. In addition, the international community has yet to form a consensus of the definition and status of cyber attacks under international law including the recognition of cyber attacks as armed attacks, making it difficult to apply the existing rules of engagement (ROE) of armed forces in response to cyber attacks.

3 For example, British Foreign Secretary Hague delivered a policy speech at the annual Munich Security Conference (MSC) held in February 2011, in which he set out the following seven principles: (1) the need for governments to act proportionately in cyberspace and in accordance with national and international law; (2) the need for everyone to have the ability—in terms of skills, technology, confidence, and opportunity—to access cyberspace; (3) the need for users of cyberspace to show tolerance and respect for diversity of language, culture, and ideas; (4) ensuring that cyberspace remains open to innovation and the free flow of ideas, information, and expression; (5) the need to respect individual rights of privacy and to provide proper protection to intellectual property; (6) the need to work collectively to tackle the threat from criminals acting online; and (7) the promotion of a competitive environment which ensures a fair return on investment in network, services, and content. In the International Strategy for Cyberspace released in May 2011, the United States outlined the following principles and norms in cyberspace: (1) upholding fundamental freedoms; (2) respect for property; (3) valuing privacy; (4) protection from crime; (5) right of self-defense; (6) global interoperability; (7) network stability; (8) reliable access; (9) multi-stakeholder Internet governance; and (10) cybersecurity due diligence.

international security, and cybercrimes. Discussions will be further explored at the follow-up meetings to be held in the future[4].

1 The United States

The International Strategy for Cyberspace released in May 2011 outlines the U.S. vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize this vision. The Strategy also points out seven policy priorities. These priorities are economy, protecting national networks, law enforcement, military, internet governance, international development, and internet freedom.

In the United States, the Department of Homeland Security is in charge of protecting networks of the Federal government and critical infrastructure, and the National Cyber Security Division (NCSD) of the Department is in charge of overall coordination[5].

As measures of the Department of Defense, the Quadrennial Defense Review (QDR) released in February 2010 lists cyberspace as one of the global commons along with land, sea, air, and space, stating the necessity to assure access to global commons. Moreover, the QDR lists effective operations in cyberspace as one of the six key mission areas for which the U.S. military is to enhance its capability. The International Strategy for Cyberspace stipulates that the United States will respond to hostile acts in cyberspace as they would to any other threat to the country, and that it reserves the right to use all necessary means, including military, as appropriate and consistent with applicable international law[6]. Furthermore, the Strategy states that the United States will: (1) recognize and adapt to the military's increasing need for reliable and secure networks; (2) build and enhance existing military alliances to confront potential threats in cyberspace[7]; and (3) expand cyberspace cooperation with allies and partners to increase collective security.

The Department of Defense Strategy for Operating in Cyberspace released in July 2011 indicates that cybersecurity threats include internal threats imposed by insiders, in addition to external threats such as cyber attacks from foreign countries and that potential U.S. adversaries may seek to disrupt the networks and systems that the Department of Defense depends on. Then, the report advocates the following five strategic initiatives to respond to cyber threats: (1) taking full advantage of cyberspace's potential by treating cyberspace as an operational domain just as domains of land, sea, air and space; (2) employing new defense operating concepts to protect the Department's networks and systems[8]; (3) partnering with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity; (4) building robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; and (5) leveraging the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

In terms of the Department's organization, then Defense Secretary Robert M. Gates directed to establish a new Cyber Command in June 2009, which supervises operations in cyberspace. The Cyber Command achieved the initial operational capability in May 2010 and the full operational capability in November 2010.

4 At the conference held in 2011, more than 700 participants from governmental organizations, private sectors, and NGO representatives across 60 countries took part in. Follow-up conferences are scheduled to be held in Hungary in 2012 and in the Republic of Korea in 2013.

5 The National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security integrates the operations of the governmental agencies related to cybersecurity and functions as a 24-hour warning and surveillance center.

6 The similar view is contained in the Department of Defense Cyberspace Policy Report submitted by the Department of Defense to the Congress in November 2011. The report further indicates that DoD will conduct offensive cyber operations if directed by the President, that the U.S. Government collects foreign intelligence via cyberspace, and that international legal norms, such as those found in the UN Charter and the law of armed conflict, apply to the cyberspace domain.

7 Specifically, the International Strategy for Cyberspace states that the United States will continue to work with the militaries and civilian counterparts of their allies and partners to expand situational awareness and shared warning systems, enhance the ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace.

8 The Department of Defense is enhancing its cyber hygiene best practices to improve its cybersecurity, will strengthen internal monitoring to deter and mitigate insider threats, and will employ an active cyber defense capability, along with developing new defense operating concept. Regarding the active cyber defense capability, on February 15, 2011, then Deputy Secretary of Defense William J. Lynn explained that, "It is not adequate to rely on passive defenses that employ only after-the-fact detection and notification. Active defenses operate at network speed, using sensors, software, and signatures derived from intelligence to detect and stop malicious code before it succeeds."

2 NATO

The North Atlantic Treaty Organization (NATO) Defence Ministers Meeting in June 2011 adopted the new NATO Policy on Cyber Defence and its action plan. The policy clarifies political and operational mechanism of NATO's response to cyber attacks, and the framework for NATO assistance to member states in their own cyber defense efforts and provision of assistance in event of cyber attack against one of its member states, as well as sets out principles on cooperation with partners.

As for organization, the North Atlantic Council (NAC), which is the supreme decision making body within NATO, provides political oversight on policies and operations concerned with NATO's cyber defense. In addition, the Defence Policy and Planning Committee (DPPC), which is a consultative body to NAC on defense issues, provides oversight and advice at the expert level. The Cyber Defence Management Board (CDMB)[9], which comprises the leaders of political, military, operational and technical staff with responsibilities for cyber defense, coordinates cyber defense throughout NATO headquarters and its associated agencies. The Emerging Security Challenges Division of the International Staff formulates policies and action plans concerning cyber defense. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), which was established in 2008, conducts research and development on cyber defense. Since 2008 NATO has been conducting cyber defense exercises on an annual basis with the aim of boosting cyber defense capabilities.

3 The United Kingdom

In the United Kingdom, based on the June 2009 Cyber Security Strategy, the Office of Cyber Security (OCS) (later integrated with information assurance functions to form the Office of Cyber Security and Information Assurance (OCSIA)) was established within the Cabinet Office to form and coordinate cybersecurity strategy for the overall government, as well as the Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) to monitor cyberspace[10]. The National Security Strategy (NSS) and the Strategic Defense and Security Review (SDSR) released in October 2010 assessed cyber attacks as one of the highest priority risks and made the decision to newly establish the Defense Cyber Operations Group (DCOG), unifying cyber activities within the Ministry of Defense. In November 2011, the U.K. government unveiled the new UK Cyber Security Strategy which stipulates that an interim DCOG will be in place by April 2012 and will achieve full operational capability by April 2014.

4 Australia

In November 2009, Australia released its Cyber Security Strategy, indicating that the Cyber Security Policy and Coordination (CSPC) committee, which is an inter-departmental committee chaired by the Attorney General, shall coordinate and oversee overall government cybersecurity policy including crisis management and international collaborations[11]. Australia's Defense White Paper released in May 2009 points out the possibility for cyber attack threats to increase at a rate far above forecasted levels and highlights enhancing the military's cyber warfare capability as a priority area. Based on the concepts outlined in the White Paper, the Cyber Security Operations Centre (CSOC) was launched under the Defense Signals Directorate (DSD) in the Department of Defense in January 2010. CSOC provides the government with analyses on advanced threats in cyberspace, and coordinates and supports response to major cybersecurity issues on governmental agencies and important infrastructures.

5 Republic of Korea

The Republic of Korea (ROK) formulated the National Cyber Security Master Plan in August 2011.The plan includes such elements as institutional developments, division of roles among concerned departments, and priorities by sector. It also clarifies the supervisory functions of the National Intelligence Service[12]in responsive actions against cyber attacks and places particular emphasis on strengthening the following five areas: prevention, detection, response, systems, and security base.

9 CDMB receives support from ESCD, established within the International Staff in August 2010, for its management.

10 OCS and CSOC comprise temporary transferred staff from related ministries and agencies and are inter-governmental organizations.

11 Also, CERT Australia, which was newly established within the Department of Justice based on the Cyber Security Strategy, provides private sector businesses with information on threats and assists in handling attacks.

12 Under the Director of the National Intelligence Service, the National Cybersecurity Strategy Council has been established to deliberate on important issues, including: 1) establishing and improving a national cybersecurity structure; 2) coordinating related policies and roles among institutions; and 3) deliberating measures and policies related to presidential orders. Moreover, the Defense Information Warfare Response Center of the Defense Security Command is in charge of protecting military networks, while the National Cybersecurity Center (NCSC) of the National Intelligence Service oversees networks of the government and public institutions, and the Korea Internet Security Center (KISC/KrCERT) of the Korea Communications Commission oversees private sector networks.

In the national defense sector, the Cyberspace Command was established in January 2010 to carry out planning, implementation, training, and research and development for its cyberspace operations and it currently serves as the division under the direct control of the Ministry of National Defense. At the U.S.-Korea Security Consultative Meeting held in October 2011, the two nations agreed to strengthen their cooperation in cyberspace.

See Part II, Chapter 3, Section 6; Part III, Chapter 1, Section 2-3