Chapter 2

Issues in the International Community

Section 1 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 have become essential components across all facets of people's lives. On the other hand, cyber attacks, especially against information and communication networks, which are critical infrastructures, have the potential to seriously impact people's lives. As such, cyber security constitutes one of the important challenges in terms of security for each country.

Types of cyber attacks include the functional obstruction of information and communication networks, data falsification or theft of information via unauthorized access to information and communication networks or through the insertion of viruses via email as well as functional impairment of the networks through simultaneous transmission of large quantities of data, and so on. Internet-related technologies are constantly evolving, with cyber attacks growing more sophisticated and complicated day by day. The characteristics of cyber attacks[1] are listed as follows.

(1) Diversity: Diversity of attackers, methods, purposes and circumstances of attacks

(2) Anonymity: Easiness for attackers to hide or disguise their identity.

(3) Stealth: Difficulty of detecting the presence of attacks or even recognizing the occurrence of damage

(4) Advantage for attackers: Easiness to obtain means of attack and difficulty of completely eliminating software vulnerabilities

(5) Difficulty of deterrence: Limited deterrence effects gained through the threat of retaliatory attacks and defense measures

For armed forces, information and communications form the foundation for command and control which extends all the way from central command to ground-level forces, and the IT revolution is further enhancing the dependence of units on information and communication networks. Given this dependence of armed forces on 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 of foreign militaries are developing offensive capabilities in cyberspace[2]. It has also been pointed out that intrusions into information and communication networks by other countries are carried out for the purpose of gathering intelligence[3].

2 Threats in Cyberspace

Under such circumstances, cyber attacks have frequently been carried out against the information and communication networks of the governmental organizations and armed forces of various countries[1].

With regard to some of those attacks, it has been pointed out that Chinese organizations including the People's Liberation

[1-1] "Toward Stable and Effective Use of Cyberspace," published in September 2012 by the MOD and SDF.

[1-2] A paper by then Deputy Secretary of Defense William J. Lynn, "Defending a New Domain: The Pentagon's Cyber Strategy," Foreign Affairs (Sep-Oct 2010).

[1-3] 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.

[2-1] In its Annual Report of November 2012, the U.S.-China Economic and Security Review Commission (a bi-partisan advisory body created by the Congress with the aim of monitoring, investigating and submitting reports on the national security implications of the bilateral trade and economic relationship with China) indicated that during 2011, there was a total of 50,097 counts of malicious cyber activities carried out on the United States Department of Defense.

Army (PLA), intelligence and security agencies and private hackers' groups have been involved[2]. China is presumed to be strongly interested in cyberspace[3], and it has been pointed out that the PLA has organized a cyber unit and is conducting training and that the PLA and the security agency are hiring employees of IT companies and hackers[4]. For example, a report published in February 2013 by a U.S. information security company concluded that a unit belonging to the PLA had been carrying out cyber attacks on companies in the United States and other countries since 2006[5].

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. This spawned a grave situation where there was a possibility that information could be transferred externally. Regarding this incident, there have been allegations of Russian involvement[6]. It has been pointed out that the Russian military, intelligence and security agencies and other organizations are involved in cyber attacks[7], and the Russian military is presumed to be considering creation of cyber command and job offers to hackers[8].

Cyber attacks also occurred in July 2009 against the websites of governmental agencies in the United States and the ROK including the U.S. Department of Defense and the ROK's Ministry of National Defense, and in March 2011 against the websites of the ROK's governmental agencies. Regarding these incidents, the Korean National Police Agency concluded that the attack originated at an IP address located in China that was owned by the North Korean Ministry of Post and Telecommunications[9]. It has been pointed out that North Korean government organizations are involved in cyber attacks and that North Korea is training personnel on a national scale[10].

Stuxnet, an advanced computer virus with a complex structure was discovered in June 2010[11]. In October 2011, another new virus was discovered, which appeared to be very similar to Stuxnet in terms of its structure, and also in May, June and August 2012, advanced viruses were discovered[12].

Moreover, supply chain risks, such as the risk that products in which deliberately and illegally altered programs are embedded may be supplied by companies[13], have been pointed out.

Cyber attacks on the information and communications net-

[2] An annual report released in November 2012 by the U.S.-China Economic and Security Review Commission stated that the PLA and the Chinese intelligence and security agencies were involved in cyber attacks originating in China.

[3] In a report at the 18th National Congress of the Chinese Communist Party, then President Hu Jintao remarked that China would pay serious consideration to maritime, outer space and cyber space security.

[4] An annual report released in November 2011 by the U.S.-China Economic and Security Review Commission stated that the Chinese government or military appeared to be supporting activities to intrude into computer networks and that the military itself was presumably involved in computer network attacks. An annual report released in 2009 by the same commission stated that the PLA was hiring personnel with expert skills concerning computers from among private companies and the academic circle and established an information warfare militia and was conducting exercises using cyberspace. The report also pointed out the possibility that the PLA was hiring personnel from the hacker community.

[5] "APT 1: Exposing One of China's Cyber Espionage Units," released in February 2013 by Mandiant, a U.S. information security company, concluded that the most active cyber attack group targeting the United States and other countries is Unit 61398 under the PLA General Staff Department Third Department. Moreover, in a speech at the Asia Society in February 2013, Thomas Donilon, National Security Advisor to the U.S. President, remarked that the United States was urging China to (1) share the recognition of the risk of cyber problems, (2) put a stop to illegal cyber activities and (3) establish common norms of behavior.

[6] An article carried by the Los Angeles Times (online version) in November 2008 reported that a senior military U.S. official said an extraordinary report had been submitted to the President regarding cyber attacks on the Department of Defense that appeared to be originating in Russia. News agency Reuters reported in June 2011 that although the Department of Defense refused to make any comment concerning the origin of those attacks, experts inside and outside the U.S. government were suspecting involvement by the Russian intelligence agency.

[7] "Cyberwarfare: An Analysis Of the Means and Motivations of Selected Nation States," released in November 2004 by Dartmouth College's Institute for Security, Technology, and Society, pointed out possible involvement of the Russian military and intelligence and security agencies in cyber attacks.

[8] "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace," a report released in November 2011 by the Office of the National Counterintelligence Executive, included a paragraph to the effect that the Russian intelligence agency was using cyber operations to gather economic and technology information to support economic development and national security. In 2013, the online version of the Russian newspaper Izvestia quoted a senior Russian military official as saying that the Minister of Defense had issued an order for preparation to establish a cyber command. In October 2012, the Voice of Russia reported that the Russian Ministry of Defense had started offering jobs to hackers.

[9] The ROK government announced a result of investigation that North Korea had also been involved in the breakdown of the computer network of South Korean agricultural cooperatives in April 2011 and cyber attacks on South Korean news organizations in June 2012.

[10] For example, a release titled "North Korea's Cyber Terrorism Capability" and issued at an emergency seminar related to North Korea's cyber terrorism held in June 2011 by the NK Intellectuals Solidarity, a group of defectors from that country, pointed out the involvement of government agencies in North Korean cyber-related organizations and stated that the country was looking for superior talents nationwide and providing expert training to develop a cyber force.

[11] Stuxnet was the first recognized 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 being detected steal information and alter the system.

[12] 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 organization, the program of the virus has many similar characteristics to Stuxnet. Kaspersky Lab, a major information security company, announced that it had discovered a high-capacity, complex computer virus called Flame in May 2012, and a computer virus called Gauss in June 2012. In August in the same year, it was reported that the computer system of Saudi Aramco, Saudi Arabia's state-run oil refining company, was attacked with a computer virus called Shamoon and received massive damage.

[13] "Cyber Supply Chain Risk Management," released in July 2011 by Microsoft.

works of governments and militaries as well as on critical infrastructure significantly affect national security. As there have been allegations of involvement of government organizations, Japan must continue to pay close attention to developments in threats in cyberspace.

In September 2011, computers of Japanese private companies producing defense equipment were found to be infected with malware. According to the National Police Agency, after the Japanese government made a cabinet decision concerning the acquisition of ownership of the three Senkaku islands in September 2012, cyber attacks took place and caused damage to at least 19 websites of Japanese courts, administrative organizations and university hospitals for several days.

3 Efforts against Cyber Attacks

Given these growing threats in cyberspace, various efforts are under way on the overall government level and the ministry level, including defense ministries[1].

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 with the aim of promoting new efforts, such as formulating certain norms of conduct within cyberspace based on international consensus[2].

An international conference on cyberspace was held in London in November 2011 and in Budapest in November 2012. Issues discussed at the conferences included economic growth and development in cyberspace, social benefits, safe and reliable access, international security, and cybercrimes. Discussions will be further explored at the follow-up meetings to be held in the future[3].

Participants deliberating on various issues and proposals concerning cyberspace at an international conference held in Budapest (November 2012) [Official Website for the Prime Minister of Hungary]

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, protection of 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.

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 sea, air, and space, stating the necessity to assure access to the global commons. Moreover, the QDR lists cyberspace as one of the six key mission areas for which the U.S. military is to enhance its capability.

The Department of Defense Strategy for Operating in Cyberspace released in July 2011 indicates that cybersecurity

[1] Generally speaking, at 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. At the level of defence department, various measures have been taken, such as establishing a new agency to supervise cyberspace military operations and positioning the effort to deal with cyber attacks as an important strategic objective.

[2] It is difficult to identify the attacker in the case of a cyber attack, and, as in many instances the attacker has nothing to protect, deterrence of attack is considered to be difficult. In addition, the international community has yet to form a consensus on 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] A follow-up conference is scheduled to be held in the Republic of Korea in 2013.

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 one of the operational domains as well as domains of land, sea, air and space; (2) employing new defense operating concepts to protect the Department's networks and systems; (3) partnering with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy; (4) building robust relationships with U.S. allies and international partners to strengthen cybersecurity; and (5) leveraging the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

In terms of organization, the Department of Defense decided to establish a new Cyber Command in June 2009, which supervises operations in cyberspace. The Cyber Command became fully operational in November 2010.

2 NATO

The new NATO (North Atlantic Treaty Organization) Policy on Cyber Defence, and its action plan, which were adopted in June 2011, clarifies the 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 the event of a 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) provides political oversight on policies and operations concerned with NATO's cyber defense. In addition, the Emerging Security Challenges Division of the International Staff, which formulates policy and action plans concerning cyber defence, and the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), which aims to become NATO's cyber defence-related research institution, were established.

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 November 2011, the United Kingdom announced a new Cyber Security Strategy[4], which set goals for the period until 2015 and specified actions plans for capability enhancement, establishment of norms, cooperation with other countries and personnel training.

In terms of organization, the Office of Cyber Security and Information Assurance (OCSIA) was established within the Cabinet Office to form and coordinate cyber security strategy for the overall government, as well as the Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) to monitor cyberspace.

The Defense Cyber Operations Group (DCOG), unifying cyber activities within the Ministry of Defense, was established by April 2012 as a provisional measure, and it is scheduled to acquire full operational capability by April 2014.

4 Australia

In January 2013, Australia published its first National Security Strategy, which positions the integrated cyber policy and operations as one of the top priority matters concerning national security[5].

In terms of organization, the Cyber Policy Group (CPG), which coordinates and supervises cyber security policy for the overall government, was established under the Cyber Policy Coordinator (CPC). The Cyber Security Operations Centre (CSOC) of the Australian Signals Directorate (ASD) provides the government with analyses on advanced threats in cyberspace, and coordinates and supports response to major cybersecurity issues on governmental agencies and critical infrastructures[6].

[4] In the Cyber Security Strategy, which was published in June 2009, the United Kingdom indicated the policy of ensuring its interests by reducing cyberspace risks, taking advantage of cyber opportunities and improving knowledge, capabilities and decision-making. In the National Security Strategy (NSS) and the Strategic Defense and Security Review, the United Kingdom specified cyber attacks as one of the top priority risks.

[5] In the Defence White Paper, published in May 2009, Australia proposed cyber warfare capability as one of the capabilities that should be strengthened by the Australian military as a priority matter while pointing out the possibility that the threat from cyber attacks could grow more than expected. In November in the same year, Australia adopted the Cyber Security Strategy, the objective of which was to maintain a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy.

[6] In January 2013, Australia announced the establishment of the Australian Cyber Security Center (ACSC), in which cyber security officers from various government agencies are concentrated in order to strengthen the national capability to deal with cyber attacks.

5 Republic of Korea

The Republic of Korea (ROK) formulated the National Cyber Security Master Plan in August 2011, which clarifies the supervisory functions of the National Intelligence Service[7] in responsive actions against cyber attacks and places particular emphasis on strengthening the following five areas: prevention, detection, response, systems, and security base. 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[8]. In addition, at the meeting of the U.S. and ROK foreign and defense ministers (2+2) in June 2012, a plan to establish a consultative body concerning cyber security was adopted for the purpose of coordination between the two countries in the cyber field. Based on the plan, the first U.S.-ROK Cyber Policy Consultations meeting was held in September 2012 with the participation of foreign and defense authorities and other relevant organizations. In the meeting, they discussed cooperation in cyberspace among relevant organizations of both countries and cyber crime countermeasures.

See▶ Part II, Chapter 2, Section 5;
Part III, Chapter 1, Section 1-3

[7] 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.

[8] The basic plan for national defense reform (2012-2030) that was submitted to the president in August 2012 by the Ministry of National Defense proposed significant enhancement of cyber warfare capability as a future military reform.