Section 5 Trends Concerning Cyberspace

1 Cyberspace and Security

Owing to the Information and Communications Technology (ICT) advancement in recent years, information and communication networks such as the Internet have become essential components across all facets of life. On the other hand, cyber attacks, especially against information and communication networks, which are critical infrastructures, have the potential to seriously impact lives of individuals.

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 by the 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 ICT advancement is further enhancing the dependence of units on information and communication networks. Given the 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 foreign militaries are developing offensive capabilities in cyberspace. It has also been pointed out that

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

intrusions into information and communication networks by other countries are carried out for the purpose of gathering intelligence.

As such, cyber security has become one of the most important issues concerning national security for countries.

2 Threats in Cyberspace

Under such circumstances, cyber attacks have frequently been carried out against the information and communication networks of governmental organizations and armed forces of various countries[2].

With regard to some of those attacks, it has been pointed out that Chinese organizations, including the People's Liberation Army (PLA), intelligence and security agencies, private hackers' groups and companies have been involved[3]. China is presumed to be strongly interested in cyberspace[4], 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 agencies are hiring IT companies' employees and hackers[5]. 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[6]. In May 2014, the U.S. Department of Justice announced that it indicted officers in Unit 61398, the Chinese

---

[2] 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.

[3] 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. Furthermore, the U.S. Department of Defense published an annual report entitled "Military and Security Developments Involving the People's Republic of China" in May 2013, stating that part of the cyber attacks targeting the U.S. Government in 2012 are considered to be directly attributable to the Chinese Government and armed forces. In June 2013, U.S. Secretary of Defense Chuck Hagel made a statement at the Asia Security Summit (Shangri-La Dialogue) that a part of cyber attacks are related to the Chinese Government and armed forces.

[4] 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.

[5] An annual report released in 2009 by the U.S.-China Economic and Security Review Commission stated that the PLA was hiring personnel with expert skills concerning computers from among private companies and the academic circles, 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.

[6] "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 was Unit 61398 under the PLA General Staff Department Third Department.

PLA's cyber attack unit, and others for conducting cyber attacks against U.S. companies[7].

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[8]. It has been pointed out that the Russian military, intelligence and security agencies, and other organizations are involved in cyber attacks[9]; and the Russian military is presumed to be considering the creation of a cyber command and job offers to hackers[10].

In March 2013, cyber attacks hit broadcasting stations and financial institutions in the Republic of Korea (ROK). In June and July of 2013, cyber attacks once again hit the ROK President's Office, government agencies, broadcasting stations, and newspaper companies. The ROK Government says that these events show the same characteristics related to cyber attacks triggered by North Korea in the past[11]. 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[12].

---

[7] On May 19, 2014, James Comey, FBI Director, stated that, "For too long, the Chinese government has blatantly sought to use cyber-espionage to obtain economic advantage for its state-owned industries." On the same day, the Spokesperson of the Ministry of Foreign Affairs of China announced that the United States "fabricated facts" and that China has decided to suspend the activities of the Cyber Working Group established under the framework of the U.S.-China Strategic and Economic Dialogue.

[8] 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 preparing 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] An article carried by the Los Angeles Times (online version) in November 2008 reported that senior military U.S. officials made an extraordinary report 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 comments concerning the origin of those attacks, experts inside and outside the U.S. government suspected involvement by the Russian intelligence agency.

[10] "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 (Currently the Institute for Security, Technology, and Society), pointed out the possible involvement of the Russian military and intelligence and security agencies in cyber attacks.

[11] The ROK Ministry of Science, ICT and Future Planning (MSIP) announced in its press releases in April and July 2013 the result of an investigation made by the joint response team of public-private-military collaboration (composed of 18 organizations including the Ministry of Science, ICT and Future Planning, the Ministry of National Defense, the National Intelligence Service, and domestic security companies). MSIP is a central government agency overseeing administration related to science and technology policies and Information and Communication Technology (ICT). This agency was established in March 2013 by transferring science and technology tasks handled by the Ministry of Education, Science and Technology, and part of the tasks handled by the Korea Communications Commission and the Ministry of Knowledge Economy.

[12] For example, a North Korean defector association in the Republic of Korea, "NK Intellectual

Stuxnet, an advanced computer virus with a complex structure, was discovered in June 2010[13], followed by discoveries of the advanced computer virus on multiple occasions.

Moreover, supply chain risks, such as the risk that products in which deliberately and illegally altered programs are embedded may be supplied by companies, have been also pointed out[14].

Cyber attacks on the information and communications networks 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 at 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 the three Senkaku Islands in September 2012, cyber attacks occurred and caused damage to at least 19 websites of Japanese courts, administrative organizations, and university hospitals for several days.

3 Initiatives against Cyber Attacks

Given these growing threats in cyberspace, various initiatives are under way on the overall

---

Solidarity," held a seminar entitled "Emergency seminar on cyber terrorism by North Korea 2011" in June 2011, and presented a material entitled "North Korea's Cyber terrorism capabilities," explaining that North Korean organizations conducting cyber attacks were supported by the government agencies employing superior human resources from all over the country, giving them special training to develop their cyber attack capabilities. In November 2013, many ROK newspapers reported that the National Intelligence Service clarified North Korean cyber attack capabilities in the national audit at the Information Committee of the National Assembly, and that Kim Jong-un, First Chairman of the National Defense Commission of North Korea, said, "Cyber attacks are omnipotent swords with their power paralleled with nuclear power and missiles."

[13] Stuxnet was the first virus program confirmed to target control systems with specific software and hardware incorporated. It is also pointed out that it has abilities to access targeted systems without being detected and steal information or alter systems. The discovery of various computer worms was also reported: "Duqu," discovered in October 2011; "Flame" in May 2012, "Gauss" in June 2012; and "Shamoon" in August 2012.

[14] In October 2012, the U.S. House Information Special Committee published an investigation report, entitled "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE." The report advised that products manufactured by Huawei Technologies and Zhong Xing Telecommunication Equipment (ZTE) (major Chinese communications equipment manufacturers) should not be used, due to their threats to national security based on strong concerns over China's cyber attack capabilities and intentions targeting critical U.S. infrastructure, as well as opaque relations between Chinese major IT companies and the Central Government, the Communist Party, and the People's Liberation Army augmenting supply chain risks. A similar move was taken by other countries including France, Australia, Canada, India, and Taiwan, and some countries, including the U.K. and the Republic of Korea, issued warnings.

government level and the ministry level, including defense ministries[15].

Attention has been drawn to issues which 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 norms covering the conduct of states and international cooperation in cyberspace. In consideration of these problems, debate has been taking place with the aim of promoting new initiatives, such as formulating certain norms of conduct within cyberspace based on international consensus[16].

See ▸ Part III, Chapter 1, Section 1-5 (Response to Cyber Attacks)

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 the 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 Federal government networks and critical infrastructure, and the National Cyber Security Division (NCSD) of the Department is in charge of overall coordination.

The Quadrennial Defense Review (QDR) published by the Department of Defense in March 2014 describes that cyber threats, which pose risks to U.S. national interests, are composed of activities of a variety of entities, including individuals, organizations, and countries, and that unauthorized access to the Department of Defense and industry networks and infrastructure threatens critical infrastructure of the United States, its allies and partners. Based on these understandings, the report designated the cyber warfare capabilities of the U.S. forces as a critical element to be maintained for the defense of the homeland, and spells out that the United

---

[15] 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 centralized; (2) policy and research units are being enhanced by establishing specialized posts, 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 the defense 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.

[16] The U.N., NATO, and international conferences in cyberspace are working on discussions for the creation of international rules by studying the positioning of cyber attacks in international law including whether they can be interpreted as armed attacks.

States continues to retain and develop required human resources and enhance cyber forces.

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. The report then 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 just like 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 government-wide 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.

From an organizational perspective, U.S. Cyber Command, a sub-unified command of U.S. Strategic Command, oversees cyber forces in the U.S. Army, Navy, Air Force, and Marine Corps, and manages operations in cyber space. The Cyber Command has been enhancing its organization in response to an increase of its tasks and already established the "Cyber Protection Force" that operates and defends information infrastructure of the Department of Defense. In addition, the "Cyber National Mission Force" to support U.S. defense against national-level threats, and the "Cyber Combat Mission Force" that supports planning process of offensive cyber capabilities by the Unified Command, are planned to be established by September 2015[17]. Moreover, U.S. Ground Force headquarters announced a doctrine named "Cyber Electromagnetic Activity" in February 2014 to prepare for the creation of guidelines.

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 mechanisms of NATO's response to cyber attacks, and the framework for NATO assistance to member states in their own cyber defense initiatives and provision of assistance in the event of a cyber attack against one of its member states, as well setting out principles on cooperation with partners.

As for its organization, the North Atlantic Council (NAC) provides political oversight on

[17] Based on a statement made, and a report submitted, in March 2013 by the U.S. Cyber Command Commander in the U.S. Senate and House Committees on Armed Services

policies and operations concerned with NATO's cyber defense. In addition, the Emerging Security Challenges Division formulates policy and action plans concerning cyber defense. Furthermore, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) was authorized to serve as NATO's cyber defense-related research and training institution[18].

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, 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 Defence Cyber Operations Group (DCOG), which unifies cyber activities within the Ministry of Defence, was established in April 2012 as a provisional measure. It is scheduled to acquire full operational capability by March 2015[19].

4 Australia

In January 2013, Australia published its first National Security Strategy, which positions integrated cyber policies and operations as one of the top priorities concerning national security.

In terms of organization, the Cyber Policy Group (CPG), which coordinates and supervises cyber security policies 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

[18] In June 2013, the NATO Defense Ministers' Meeting placed cyber attacks top on the agenda for the first time. They agreed to establish an emergency response team and to implement a cyber defense mechanism on a full scale by October 2013.

[19] In addition, the U.K. Ministry of Defence announced in September 2013 to hire hundreds of computer experts as reserves working on the front line of British cyber defence, and approved the establishment of the Joint Cyber Reserves.

and critical infrastructures[20].

5 Republic of Korea

The ROK formulated the National Cyber Security Master Plan in August 2011, which clarifies the supervisory functions of the National Intelligence Service[21] in responsive actions against cyber attacks. It 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 currently serves as the division under the direct control of the Ministry of National Defense[22].

See ▸ Part III, Chapter 1, Section 1-5; Part III, Chapter 2, Section 2-4

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

[21] Under the Director of the National Intelligence Service, the National Cybersecurity Strategy Council has been established to deliberate on important issues, including establishing and improving a national cybersecurity structure, coordinating related policies and roles among institutions, and deliberating measures and policies related to presidential orders.

[22] 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.