Section 5 Trends in Cyberspace

1 Cyberspace and Security

Owing to the advancement of information and communications technology (ICT) in recent years, information and communication networks such as the Internet have become essential components across all facets of life. Meanwhile, cyber attacks[1] against critical infrastructures, namely, information and communication networks, have the potential to seriously impact the lives of individuals.

As regards the types of cyber attacks, they include functional interference, data falsification, and data theft caused by unauthorized access to information and communication networks or through the transmission of viruses via e-mail, as well as functional impairment of the networks through simultaneous transmission of large quantities of data. Internet-related technologies are constantly evolving, with cyber attacks growing more sophisticated and complicated by the day. The characteristics of cyber attacks[2] include the following.

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) Offensive dominance: Easiness to obtain means of attack and difficulty of completely eliminating software vulnerabilities
5) The difficulties of deterrence: Limited deterrence effects gained through the threat of retaliatory attacks and defense measures

For military forces, information and communications form the foundation of command and control, which extend from central command to ground-level forces. In this regard, ICT advancements are further enhancing the dependence of units on information and communication networks. Furthermore, military forces rely on various social infrastructures, including electricity, to execute their missions. Accordingly, cyber attacks against such social infrastructures could become a major impediment to their missions. For this reason, cyber attacks are regarded as an asymmetrical strategy capable of mitigating the strengths of adversaries by exploiting the weaknesses of an adversary's forces. It is believed that many foreign military forces are developing offensive capabilities in cyberspace. In addition, it is said that the information and communication networks of countries are being compromised for the purpose of gathering intelligence.

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

2 Threats in Cyberspace

Under such circumstances, cyber attacks have frequently been carried out against the information and communication networks of government organizations and military forces of various countries[3].

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[4]. China is presumed to be strongly interested in cyberspace[5]. It has been pointed out that the PLA has organized and is training a cyber unit, and that the PLA and security agencies are hiring IT companies' employees

1 The targets of cyber attacks are wide-ranging. Beginning with large targets, they range from: global-level targets, including interstate targets; state-level targets, including nations and government institutions; societal-level targets, including local communities; sectoral-level targets, including business communities and infrastructure; industry-level targets, including companies and groups; and down to minimum-level target of individuals. As such, it is said that measures to counter cyber attacks need to be optimal relative to the size of the target.

2 Ministry of Defense Japan, "Toward Stable and Effective Use of Cyberspace," September 2012.

3 According to a statement made by the Chairman of the U.S. House Committee on Homeland Security (November 2014), the United States Computer Emergency Readiness Team (US-CERT) reports that the number of cyber attacks against the U.S. government in 2013 was 46,605. Furthermore, US-CERT responded to a total of 228,700 cyber attacks, including those against federal agencies and companies, which was more than double the number in 2009. In addition, the February 2015 "Worldwide Threat Assessment" of the U.S. Director of National Intelligence states that cyber espionage targets the U.S. government, military, and companies on a daily basis. The report presents the view that "attackers" include: (1) nation states with highly sophisticated cyber programs (such as Russia or China); (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea); (3) profit-motivated criminals; and (4) ideologically motivated hackers or extremists.

4 The annual report of the U.S.-China Economic and Security Review Commission of November 2014 states that the Chinese government has conducted large-scale cyber espionage against the United States since at least the mid-2000s, and that China has compromised a range of U.S. networks, including those of the Department of Defense, defense contractors, and private enterprises. In addition, the U.S. Department of Defense's "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China" of June 2014 states that the PLA continues to invest in offensive cyber capabilities.

5 In a report delivered at the 18th National Congress of the Chinese Communist Party (CCP), then-CCP General Secretary Hu Jintao remarked that China would give serious consideration to maritime, outer space, and cyber space security.

and hackers[6]. For example, a report published in February 2013 by a U.S. information security company concluded that a unit belonging to the PLA had carried out cyber attacks on companies in the United States and other countries since 2006[7]. In May 2014, the U.S. Department of Justice announced that it indicted officers in Unit 61398, the Chinese PLA's cyber attack unit, and others for conducting cyber attacks against U.S. companies[8]. In July 2014, the Canadian government stated that it was a victim of cyber attacks by China, referring to China by name for the first time[9].

In October 2014, the White House's unclassified information system was hacked. Russian involvement in this incident has been suggested[10]. It has been pointed out that the Russian military, intelligence and security agencies, and other organizations are involved in cyber attacks[11]. Furthermore, the Russian military is presumed to be considering the creation of a cyber command and recruiting hackers[12].

In March 2013, cyber attacks hit broadcasting stations and financial institutions in the Republic of Korea (ROK). In June and July 2013, cyber attacks hit the ROK President's Office, government agencies, broadcasting stations, and newspaper companies. The ROK government has stated that the tactics used in these incidents were the same as those used in past cyber attacks by North Korea[13]. Furthermore, from November to December 2014, a U.S. film company was hit with cyber attacks. In December 2014, the U.S. Federal Bureau of Investigation (FBI) announced that there was sufficient evidence to conclude that the North Korean government was responsible for these cyber attacks[14]. It has been pointed out that North Korean government organizations are involved in such cyber attacks[15] and that North Korea is training personnel on a national scale[16].

Stuxnet, an advanced malware with a complex structure, was discovered in June 2010[17], followed by discoveries of the advanced malware on multiple occasions.

Cyber attacks on the information and communication networks of governments and militaries[18], 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 related to 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

6 An annual report released in 2009 by the U.S.-China Economic and Security Review Commission stated that the PLA was hiring personnel with specialized skills in computers from private companies and the academia, established an information warfare militia, and was conducting exercises using cyberspace. The report also stated that the PLA may be hiring personnel from the hacker community.

7 "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.

8 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.

9 According to a Canadian government release dated July 2014.

10 In October 2014, the Washington Post reported that hackers with alleged Russian government involvement conducted the cyber attack.

11 "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, intelligence, and security agencies in cyber attacks.

12 In 2013, the online version of the Russian newspaper Izvestia quoted a senior Russian military official 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 recruiting hackers.

13 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 MSIP, 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 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.

14 The FBI presented the following three items as evidence. (1) The malware used in this cyber attack was similar to malware that North Korean actors previously used. (2) North Korean Internet protocol (IP) addresses were hardcoded into the data deletion malware. (3) The tools used in the attack had similarities to a cyber attack in March 2013 against ROK broadcasting stations and financial institutions, which was carried out by North Korea.

15 In November 2013, ROK media outlets reported that the ROK National Intelligence Service made revelations about North Korean cyber warfare capabilities in the national audit of the Information Committee of the National Assembly, and that Kim Jong-un, First Chairman of the National Defense Commission of North Korea, stated that, "Cyber attacks are omnipotent swords with their power paralleled with nuclear power and missiles." In the U.S. Department of Defense's "2013 Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea" published in March 2014, it is stated that North Korea probably has a military offensive cyber operations capability. The 2014 Defense White Paper published by the ROK in January 2015 notes that North Korea has concentrated on boosting its cyber unit to nearly 6,000 personnel.

16 For example, a North Korean defector association in the ROK, "NK Intellectual Solidarity," held a seminar entitled "Emergency seminar on cyber terrorism by North Korea 2011" in June 2011, and presented material entitled "North Korea's cyber terrorism capabilities," explaining that North Korean organizations conducting cyber attacks were supported by government agencies employing superior human resources from all over the country, giving them special training to develop their cyber attack capabilities.

17 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 to steal information or alter systems. The discovery of various malware has also been reported: "Duqu," discovered in October 2011; "Flame" in May 2012; "Gauss" in June 2012; and "Shamoon" in August 2012.

18 CyberBerkut, a Ukrainian pro-Russian group, carried out cyber attacks against multiple websites of NATO in March 2014 and against the websites of the German government and the German parliament, the Bundestag, in January 2015. In October 2014, in the midst of the large-scale demonstrations led by the pro-democracy camp in Hong Kong, the international hacker group "Anonymous" declared that it would conduct cyber attacks against the Chinese and Hong Kong governments. Multiple websites of both governments were hit with cyber attacks. Furthermore, in January 2015, the hacker "Cyber Caliphate," which appears to endorse Islamic extremism, is alleged to have made fraudulent posts on the official Twitter account of the U.S. Central Command, in addition to hacking nearly 20,000 websites, including the websites of French domestic forces and private companies. As these examples demonstrate, hacker groups have carried out numerous cyber attacks.

Police Agency, after the Japanese government made a cabinet decision concerning the acquisition of three of the islands of the 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.

In addition, supply chain risks, such as companies supplying products embedded with deliberately and illegally altered programs, have been also pointed out[19].

3 Initiatives against Cyber Attacks

Given these growing threats in cyberspace, various initiatives are under way at the overall government level and the ministry level, including defense ministries[20].

Analysts have raised a number of issues that need to be dealt with to allow for an effective response to cyber attacks, which have become a new security challenge in recent years. For instance, there is no broad consensus on norms related to the conduct of states in cyberspace as well as on international cooperation. Based on this awareness of the issues, there has been a movement to establish some codes of conduct in cyberspace pursuant to international consensus[21]. It has been suggested, however, that countries have conflicting assertions, with countries such as the United States, European countries, and Japan calling for maintaining free and unrestricted cyberspace, while many countries such as Russia, China, and emerging countries call for strengthening the national control of cyberspace.

See Part III, Chapter 1, Section 1-6 (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 partnership with other nations and people 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 capacity development, and Internet freedom.

In the United States, the Department of Homeland Security is responsible for protecting Federal government networks and critical infrastructure against cyber attacks, and the Department's Office of Cybersecurity and Communications (CS&C) works to protect the networks of government agencies.

In the National Security Strategy (NSS) which was released in February 2015, the United States identifies cyber attacks as one of today's major threats. As regards the Department of Defense's (DoD) efforts, the Quadrennial Defense Review (QDR) published in March 2014 describes that cyber threats, which pose risks to U.S. national interests, are composed of the activities of a variety of actors, including individuals, organizations, and countries, and that unauthorized access to the DoD and industry networks and infrastructure threatens the critical infrastructure of the United States, its allies, and partners. Based on this understanding, the report designated the

19 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 CCP, and the PLA augmenting supply chain risks. A similar move has been taken by other countries, including France, Australia, Canada, India, and Taiwan. Some countries, including the United Kingdom and the ROK, have issued warnings.

20 Generally, the trends at the governmental level are thought to include the following: (1) organizations related to cyber security that are spread over multiple departments and agencies are being integrated, and their operational units are being 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 given to international cooperation. At the level of the defense ministry, 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.

21 The United Nations Group of Governmental Experts (GGE) on Cyber Issues has continued to hold consultations since 2004, with the participation of experts from a total of 15 countries (a total of 20 countries since the July 2014 meeting), including Japan, the United States, Russia, and China. The GGE's June 2013 report to the U.N. General Assembly recommends that international law, and in particular, the U.N. Charter is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment.

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

With regard to cyber threats, "The DoD Cyber Strategy" released in April 2015 expresses the view that the United States faces serious cyber threats, noting that state[22] and non-state actors intend to carry out destructive cyber attacks against U.S. networks, as well as steal U.S. military technology information. In this light, the DoD has set out the following three primary missions in cyberspace: (1) Defend the DoD networks, systems, and information; (2) Defend the United States and its interests against cyber attacks of significant consequence; and (3) Provide integrated cyber capabilities to support military operations. Furthermore, the DoD states that the aforementioned cyber capabilities include cyber operations to disrupt an adversary's military-related systems. In order to execute these missions in cyber space, the DoD presents the following five strategic concepts: (1) Build and maintain ready forces and capabilities to conduct cyberspace operations; (2) Defend the DoD information network and data, and mitigate risks to DoD missions; (3) Establish arrangements to defend the United States and its interests from cyber attacks of significant consequence through collaboration with relevant departments and companies; (4) Use cyber options to control conflict; and (5) Build close cooperative relations with allies and partners.

From an organizational perspective, U.S. Cyber Command, a sub-unified command of U.S. Strategic Command, oversees the cyber forces of the U.S. Army, Navy, Air Force, and Marine Corps, and manages operations in cyber space. Cyber Command has expanded along with the expansion of its missions, and has already established the "Cyber Protection Force" that operates and defends the information infrastructure of the DoD. In addition, Cyber Command has created the "Cyber National Mission Force" to support U.S. defense against national-level threats, and the "Cyber Combat Mission Force" that supports the operations conducted by the Unified Command on the cyber front. These three forces are collectively referred to as the "Cyber Mission Force." Multiple teams are thought to belong to these three forces, with over ten teams currently in operation. Furthermore, Cyber Command has stated that 133 teams consisting of 6,200 personnel would be created by September 2018, using National Guard and reserve personnel[23].

2 NATO

The new NATO (North Atlantic Treaty Organization) Policy on Cyber Defence, and its action plan, which were adopted in June 2011: (1) clarify the political and operational mechanisms of NATO's response to cyber attacks; (2) clarify that NATO would provide assistance to member states to develop their cyber defense, and provide assistance to member states if they are subject to cyber attacks; and (3) set out principles on cooperation with partners. Furthermore, at the NATO Summit in September 2014, agreement was reached that NATO's collective defense applies to cyber attacks against member states.

As for its 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 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. CCD COE organizes the International Conference on Cyber Conflict annually, as well as carries out other activities, including commissioning experts to compile the Tallinn Manual[24].

Since 2008, NATO has been conducting cyber defense exercises on an annual basis to boost cyber defense capabilities.

22 "The DoD Cyber Strategy" states that Russia and China have acquired advanced cyber capabilities and strategies. It goes on to say that Russian activities are carried out stealthily and their intentions are difficult to discern. The Strategy notes that China steals intellectual property to benefit Chinese companies. Furthermore, it states that while Iran and North Korea do not have developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests.

23 Based on a statement made in April 2015 by the U.S. Cyber Command Commander to the U.S. Senate Committee on Armed Services.

24 In June 2013, the NATO Defense Ministers' Meeting placed cyber attacks at the top of 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.

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 action 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[25].

In January 2015, Prime Minister David Cameron and President Barack Obama agreed to strengthen cooperation in the area of cyber defense[26]. In such ways, the United Kingdom is working to deepen its collaboration with other countries.

4 Australia

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

In terms of organization, the Cyber Policy Group (CPG), which coordinates and supervises the cyber security policies of the whole government, was established under the Cyber Policy Coordinator (CPC). The Australian Cyber Security Centre (ACSC) of the Australian Signals Directorate (ASD) responds to major cybersecurity issues on governmental agencies and critical infrastructures[27].

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[28] in responding to cyber attacks. It places particular emphasis on strengthening the following five areas: prevention, detection, response[29], 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[30].

Section 6 Trends Concerning Military Science and Technology as well as Defense Production and Technological Bases

1 Military Science and Technological Trends

Recent developments in science and technology, as represented by the dramatic advancement of Information and Communication Technology (ICT), has impacted a variety of areas, triggering significant and revolutionary changes in many areas such as economy, society, and lifestyle.

The military is no exception. Developed countries, including the United States, consider that transformations driven by advances in ICT can dramatically improve combat and other capabilities, and therefore, continue to pursue a variety of ICT research and policies.

For example, if information on enemy forces collected using information-gathering systems, including reconnaissance satellites and unmanned aircraft, is shared on a network, command and control can be exercised immediately, even from remote headquarters. By extension, offensive power can be directed swiftly, precisely, and flexibly against targets.

Major countries with sophisticated and modernized military forces, including the United States, engage in research and development related to improving the destructive capabilities of weapons, precision guidance technology, information-related technology including

25 In addition, the U.K. Ministry of Defence announced in September 2013 that it would recruit hundreds of computer experts as reserves working on the front line of British cyber defence, and approved the establishment of the Joint Cyber Reserves.

26 According to a White House release, the U.K. GCHQ and Security Service (SS) and the U.S. National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) will work together closely on cyber security and cyber defense. In addition, the U.K. and U.S. Governments announced that they would conduct their first joint exercise in the second half of 2015 to test their ability to defend against cyber attacks on critical infrastructure.

27 ACSC, comprised of staff from the Australian Crime Commission, the Australian Federal Police, the Australian Security Intelligence Organisation, the Department of Defence, and the Attorney-General's Department, analyzes threats in cyber space and responds to both public and private sector incidents.

28 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.

29 In February 2014, it was reported that the ROK Ministry of National Defense briefed the National Assembly that it planned to develop cyber weapons for attacking other countries.

30 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.