Section 3 Trends in Cyber Domain

1 Cyberspace and Security

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

Types of cyber attacks include functional disruption, data falsification and data theft caused by unauthorized access to information and communications networks or through the transmission of viruses via e-mail, functional impairment of the networks through simultaneous transmission of large quantities of data, and attacks intended to shut down or take over a system belonging to critical infrastructure, such as power systems. Also, network-related technologies are constantly evolving, with cyber attacks becoming more and more advanced and sophisticated by the day.

For military forces, information and communications capability form the foundation of command and control, which extend from central command to ground-level forces. In this regard, ICT advancements are further increasing the dependence of military forces on information and communications networks. Furthermore, in some cases, military forces need various critical infrastructures, including electricity, to execute their missions. Accordingly, cyber attacks against such critical infrastructures could become a major impediment to their missions. For this reason, cyber attacks are recognized as an asymmetrical means to impede the military activities of adversaries at low cost. It is believed that many foreign military forces are developing offensive capabilities in cyberspace. It has been pointed out that China and Russia in particular are bolstering the offensive cyber capabilities of their militaries for the purpose of obstructing the networking of adversaries' military forces and destroying their infrastructure.[1]

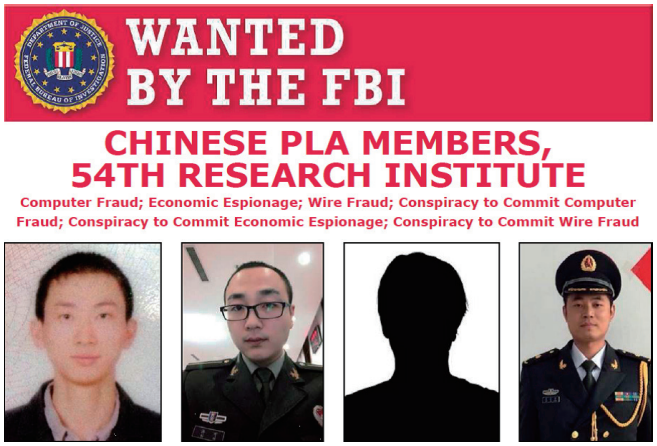
2 Threats in Cyberspace

Under such circumstances, cyber attacks have frequently been carried out against information and communications networks of not only government organizations and military forces but also business corporations and academic organizations in various countries. Attacks attempting to steal critical technologies, secrets or personal information have been confirmed. For example, advanced persistent threat (APT) and other relentless cyber attacks focusing on specific bodies require abundant resources, arrangements and capabilities, being viewed as organized activities. To respond to such advanced cyber attacks, Japan is required to share threat awareness with foreign countries for technological and operational cooperation. The United States has assessed that China, Russia, Iran and North Korea have been conducting more diverse and aggressive cyber attacks,[2] indicating that their military forces have enhanced their offensive cyber capabilities.

1 China

It has been alleged that cyber warfare units have been formed under the Strategic Support Force that was created as part of China's military reforms in late December 2015. The units are estimated to consist of 175,000 troops, including 30,000 for cyber attacks. In its "National Cyberspace Security Strategy" published in 2016, China recognized sovereignty in cyberspace as an important component part of national sovereignty. Its 2019 defense white paper, released in July 2019 and titled "China's National Defense in the New Era," stated that China's armed forces accelerate the building of

1 According to "Worldwide Threat Assessment," Director of National Intelligence (March 2018)
2 According to "Worldwide Threat Assessment," Director of National Intelligence (January 2019)



Four individuals indicted for suspected involvement in the cyberattack targeting a U.S. consumer credit information company in 2017 [FBI]

their cyberspace capabilities. Given the above, China is believed to have been enhancing its military's cyber warfare capabilities.

See Chapter 2, Section 2-5 (Military Posture)

China is suspected of conducting cyber attacks and other activities to steal confidential information even in peacetime.[3] For example, its involvement in the following incidents has been pointed out.

- In June 2015, the U.S. Office of Personnel Management (OPM) became a target of a cyber attack in which, as it later came to light, personal information of about 22 million people, including U.S. federal employees and U.S. Forces personnel, were stolen.[4]
- In January and February 2018, Chinese government hackers hacked a U.S. Navy contractor, leading to a leak of classified information on supersonic anti-ship missiles mounted on submarines.
- In December 2018, such countries as the United States announced that the APT10 cyber group related to China's Ministry of National Security conducted cyber attacks on intellectual and other properties in at least 12 countries.
- In Japan, it has been confirmed that the APT10 group conducted extensive cyber attacks on private enterprises, academic organizations and other targets.
- In 2017, a U.S. consumer credit information company came under a cyber attack stealing personal information including names, birthdates, social security numbers, driver's license numbers, and credit card numbers. In February 2020, the U.S. Department of Justice prosecuted four Chinese military-related persons for their alleged involvement in the cyber attack.

2 Russia

It has been pointed out that the Main Intelligence Directorate of the General Staff of the Russian Armed Forces (GRU) and the Federal Security Service of the Russian Federation (FSB) are involved in cyber attacks. It has also been revealed that the Russian military has its own cyber command unit,[5] which is believed to be responsible for conducting offensive cyber activities, including inserting malware into command and control systems of adversaries,[6] with approximately 1,000 personnel. Russia's "Doctrine of Information Security," released in December 2016, acknowledged an increase in threats related to the use of information technology for military and political purposes. In November 2019, Russia enforced the so-called sovereign Internet law to secure the continuity of Russian networks by shutting them out from global networks in the event of an incident like a cyber attack.

It is pointed out that Russia has taken advantage of cyberspace for intelligence operations not only to steal information and conduct sabotage operations but also to challenge democratic processes[7] and has been involved in the following incidents:

KEY WORD Malware

Malware stands for malicious software, meaning software that takes advantage of various vulnerabilities for cyber attacks.

3 According to "Cyber Strategy," U.S. DoD (September 2018)
4 According to the Annual Report of the U.S.-China Economic and Security Review Commission (November 2015).
5 According to a statement made by Russian Minister of Defence Shoigu during a briefing for the lower house in February 2017, that the Russian military has a cyber command for countering political propaganda in Russia's ongoing information war with Western countries. However, the minister fell short of naming the command.
6 According to then U.S. Director of National Intelligence Clapper's written testimony on "Worldwide Cyber Threats" at the House Permanent Select Committee on Intelligence in September 2015.
7 According to the "Cyber Strategy," U.S. DoD (September 2018)

- In 2014, more than 500 million user accounts were leaked from a major U.S. Internet company. In March 2017, the U.S. government indicted four hackers, including two officers of the Russian Federal Security Service, for their alleged cyber attack on the company.[8]
- In December 2015, a cyber attack triggered a large-scale power outage in Ukraine. It was reported that military forces of Russia confronting with Ukraine over the Crimea annexation and other issues were suspected of having contributed to the cyber attack.
- Cyber attacks to affect the outcome of the 2016 U.S. presidential election.[9]
- In June 2017, cyber attacks using the so-called NotPetya ransomware occurred in Ukraine and other countries. In February 2018, the U.S. and U.K. governments attributed the attacks to the Russian military.
- In October 2018, the U.S. and U.K. governments announced that the Main Intelligence Directorate of the GRU was responsible for cyber attacks on the World Anti-Doping Agency, the Organization for the Prohibition of Chemical Weapons, the U.S. Democratic convention, and other targets.
- In February 2020, U.S., U.K., Georgian and other governments announced that the GRU was responsible for large-scale cyber attacks on Georgian government agencies and media organizations in October 2019.[10]

3 North Korea

It has been pointed out that the North Korean authority trains hackers[11] and has intensively built up cyber units operating some 6,800 personnel.[12] In September 2019, the U.S. Department of the Treasury announced sanctions targeting three cyber groups[13] supported by the North Korean authority responsible for their involvement in malicious cyber activities targeting key infrastructure.

North Korea is believed to have been developing capabilities to steal money and secret military information through cyber attacks and inflict such attacks on key foreign infrastructure. It is suspected of having been involved in the following incidents.

- In September 2016, cyber attacks occurred in the internal network of the ROK Armed Forces. In May 2017, the ROK Ministry of National Defense was reported to have concluded that the cyber attacks had been conducted by what was believed to be a North Korean hacker group.[12] Moreover, it has been pointed out that documents containing military secrets of the ROK were stolen through the cyber attacks.
- In May 2017, a cyber attack used a malware called WannaCry to encrypt and neutralize electronic data held by hospitals, schools, businesses, and other entities in more than 150 countries. Japan, the United States, the United Kingdom, Australia, Canada, and New Zealand announced a statement blaming North Korea for its involvement in the attack. It has been pointed out that this cyber attack succeeded in collecting 140,000 dollars in Bitcoins.
- In September 2017, multiple U.S. electric power utilities were inflicted with cyber attacks using spear phishing emails. In October 2017, FireEye, a U.S. cybersecurity company, announced that the attacks had been conducted by a cyber threat group allegedly affiliated with North Korea.
- According to the final report released by the Panel of Experts of the UN Security Council Sanctions Committee on North Korea in April 2020, the Panel concluded, based on information provided by member states and publicly available information, that North Korea has continued to carry out cyber attacks on financial institutions and cryptocurrency exchanges and that the attacks are becoming more sophisticated.

4 Trends Concerning Other Threats

Supply chain risks, including products embedded with deliberately and fraudulently altered programs, and the existence of advanced malware designed to attack industrial

8 According to a U.S. Department of Justice release in March 2017.
9 According to the joint statement issued in October 2016 by the U.S. Department of Homeland Security and the Director of National Intelligence of the United States, and the joint report issued in December of the same year by the U.S. Department of Homeland Security and the FBI concerning Russian cyber attacks on the United States, as well as the U.S. intelligence community report on Russia's cyber attacks on the U.S. presidential election released in January 2017.
10 According to a U.S. Department of Justice release in February 2020.
11 According to the ROK's 2016 Defense White Paper (January 2017)
12 According to the ROK's 2018 Defense White Paper (January 2019)
13 In the private cybersecurity industry, the North Korean APT attack groups are known as Lazarus Group, Bluenoroff, and Andariel.

control systems are also pointed out. In this respect, the U.S. Congress in August 2018 passed the National Defense Authorization Act of 2019 including provisions prohibiting government agencies from using products of major Chinese communications equipment manufacturers, such as Huawei Technologies Co. The United States has provided its allies with information about risks accompanying Chinese communications equipment and urged them not to use such equipment. In response, Australia has banned China's Huawei and ZTE Corporation from taking part in its 5G next-generation mobile network development project.

Cyber attacks on telecommunication networks of a government and military forces or on critical infrastructure could have a serious effect on the security of states, and it is believed that state-sponsored cyber attacks have been on the rise in recent years. Given this situation, there is a need for continuous monitoring of trends in the threats in cyberspace.

3 Initiatives against Cyberspace Threats

Given these growing threats in cyberspace, various initiatives are under way.

It is regarded that the international community has diverging views concerning the fundamental matters of cyberspace, including how international law applies. For instance, the United States, Europe, and Japan have called for maintaining a free cyberspace, while Russia, China, and most emerging countries sought to strengthen state control on cyberspace. Against this backdrop, there has been a movement to promote the rule of law in cyberspace in the international community. For instance, discussions are being held on the establishment of international rules within the framework of global conferences on cyberspace.

See Part III, Chapter 1, Section 3-2 (Response in Cyber Domain)

1 The United States

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 Cybersecurity Infrastructure Security Agency (CISA) works to protect the networks of government agencies.

The U.S. NSS (December 2017) points out that many countries now view cyber capabilities as tools for projecting influence and that cyberattacks have become a key feature of modern conflict. It also notes that the United States would deter, defend, and when necessary defeat malicious actors who inflict cyber attacks on the United States. The U.S. DoD in its National Defense Strategy (January 2018) described a policy of investing in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Furthermore, the DoD Cyber Strategy (September 2018) points out that the United States is engaged in a long-term strategic competition with China and Russia, and that China and Russia have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the United States as well as to its allies and partners. The strategy presents such approaches as (1) the acceleration of cyber capability development, (2) defense to counter and deter malicious cyber activity, and (3) the promotion of cooperation with U.S. allies and partners.

In April 2019, at the U.S.-Japan Security Consultative Committee (2+2), the two countries agreed to enhance cooperation on cyber issues and affirmed that international law applies in cyberspace and that a cyber attack could, in certain circumstances, constitute an armed attack for the purposes of the U.S.-Japan Security Treaty.

The U.S. Forces include Cyber Command, which was elevated to a unified combatant command in May 2018 to control cyberspace operations. The Command consists of the Cyber Protection Force (68 teams), which operates and defends the DoD Information Network, the Cyber National Mission Force (13 teams), which supports the U.S. defense against national-state threats, and the Cyber Combat Mission Force (27 teams), which supports the operations conducted by unified combatant commands on the cyber front (these three Forces are collectively referred to as the Cyber Mission Force, consisting of 133 teams including 25 support teams, with approximately 6,200 personnel).

2 North Atlantic Treaty Organization (NATO)

The NATO 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, an agreement was reached that NATO's collective defense applies to cyber attacks against member states.

On the organizational front, in November 2017, an agreement was reached on the creation of a new Cyber Operations Center and the integration of NATO member countries' cyber defense capabilities into NATO missions and operations. The Cyber Operations Center located in Belgium is expected to be fully operational with cyber attack capabilities by 2023. Furthermore, NATO has conducted cyber defense training exercises annually since 2008 to heighten cyber defense capabilities. In addition, NATO has expanded cooperation with the EU in the fields of cybersecurity and cyber defense.

In 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was authorized to serve as a research and training institution, and was established in Estonia's capital of Tallinn. CCDCOE carries out research on the relationship between cyber activities and international law, creating the "Tallinn Manual." In February 2017, "Tallinn Manual 2.0" was published as the second edition of the previous manual based on a review of broad discussion points, from peacetime legal regimes, such as laws on state responsibility, human rights, aviation, space, and maritime affairs, to contingency legal regimes, such as laws on armed conflict. In December 2019, NATO held its "Cyber Coalition 2019" exercise, in which Japan officially participated for the first time in addition to 27 NATO member countries and the EU.

3 The United Kingdom

The United Kingdom, in its "National Security Strategy and Strategic Defence and Security Review (NSS- SDSR2015)" released in November 2015, committed to investing £1.9 billion over the next five years in increasing its cyber defense capabilities to strengthen the functions for identifying and analyzing cyberspace threats. In November 2016, the country announced a new "Cyber Security Strategy" that presents a vision for the United Kingdom, which is to be secure and resilient to cyber threats, prosperous and confident in the digital world. To achieve this vision, the Strategy requires the United Kingdom to deter cyber threats by having effective defensive and offensive means and to "develop" cutting-edge technologies.

On the organizational front, in October 2016, the National Cyber Security Centre (NCSC) was newly established under the Government Communications Headquarters (GCHQ) to promote public-private partnerships for responses to national cyber incidents.

4 Australia

In its first "National Security Strategy" published in January 2013, Australia positions integrated cyber policies and operations as one of the top national security priorities. In April 2016, a new "Cyber Security Strategy" through 2020 was released, which provides that Australia will ensure the safety of the people, that private companies will participate in cybersecurity, and that threat information will be shared.

On the organizational front, cybersecurity capabilities across the government were converged to establish the Australian Cyber Security Center (ACSC), which addresses major cybersecurity issues related to government agencies and critical infrastructure. In July 2015, the ACSC issued its first report on cybersecurity, which contends that the number, type, and sophistication of cyber threats to Australia are all increasing. Moreover, the Australian Defence Force created the Information Warfare Division under the Joint Capabilities Group in July 2017 and established the Defence Signals Intelligence and Cyber Command under the division in January 2018. In October 2019, the Royal Australian Air Force offered to recruit cyber skills officers to protect networks, data and information systems.

5 The ROK

In December 2018, the ROK released the "National Security Strategy of the Moon Jae-in Government," pledging to enhance cyber threat prevention and response capabilities based on cooperation among private, government and

military sectors in responding to cyber threats and to activate relevant international cooperation. The ROK also formulated its first "National Cybersecurity Strategy" in April 2019 to protect the safety of the people and enhance national security, and released the "National Cybersecurity Basic Plan" to materialize the strategy in September 2019.

In the national defense sector, the Cyber Measures Technology Team was established by the Ministry of National Defense to respond to cyber and hacking threats. The sector has also worked out procedures for quick response to cyber crises under the "National Cyber Security Strategy" and the "National Cybersecurity Crisis Response Manual." In 2015, the Joint Chiefs of Staff centralized the cyber attack tactical system mainly around the Joint Chiefs of Staff by newly establishing the Cyber Tactics Department, assigning control authority concerning cyber tactics to the Chairman of the Joint Chiefs of Staff, and issuing a field manual on "joint cyber tactics."