Section 5 Trends in Cyberspace

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. Meanwhile, cyber attacks[1] against critical infrastructures, namely, information and communications networks, have the potential to seriously impact the lives of individuals.

Types of cyber attacks include functional interference, data falsification, and data theft caused by unauthorized access to information and communications 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[2] becoming more sophisticated and skillful by the day.

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 communications 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, actors attempting to cause harm to nations, etc. have all realized that attacking through cyberspace is often easier than attacking directly using physical means.[3] Moreover, it is said that the information and communications networks of countries are being compromised for the purpose of gathering intelligence. As more confidential information begins to be stored in cyberspace, cyber espionage through cyber attacks is causing more serious damage.

As such, cybersecurity 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 communications networks of government organizations and military forces of various countries.[4]

Some of these cyber attacks are said to involve a range of organizations including China's PLA, intelligence agencies, security agencies, private hacker groups, and companies.[5,6] According to the defense white

1 The targets of cyber attacks are wide-ranging. Beginning with large targets, they range from global-level targets, including interstate targets, as well as nations and government institutions, local communities, business communities and infrastructures, companies, and individuals. As such, it is said that measures to counter cyber attacks need to be optimal relative to the size of the target.

2 In the Japanese MOD's "Toward Stable and Effective Use of Cyberspace" of September 2012, cyber attacks are characterized as follows: (1) diversity: cyber attacks involve diverse actors, methods, objectives, and context; (2) anonymity: actors can easily conceal and disguise their identity; (3) stealth: some cyber attacks are difficult to identify and can take place without causing any realization of damage; (4) offensive dominance: attack tools are easy to acquire depending on the tool, and it is difficult to completely eliminate software vulnerabilities; and (5) the difficulties of deterrence: retaliatory strikes and defensive measures have minimal deterrence effect.

3 According to the "Cybersecurity National Action Plan" unveiled by U.S. President Obama in February 2016.

4 According to the U.S. Office of Management and Budget's "Annual Report to Congress: Federal Information Security Management Act" (February 27, 2015), the United States Computer Emergency Readiness Team (US-CERT) recorded that in FY2014 there were 69,851 incidents of cyber attacks against the U.S. government, and that a total of 640,222 incidents of cyber attacks were reported to US-CERT, including attacks against government agencies and companies. The U.S. Director of National Intelligence's "Worldwide Threat Assessment" of February 2016 names Russia, China, Iran, North Korea, and non-state actors as threat actors to cyberspace, expressing the opinion that, for example: (1) Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations; (2) China continues to conduct cyber espionage against the U.S. government, its allies, and U.S. companies, and uses cyber attacks against targets it believes threaten Chinese domestic stability or regime legitimacy; (3) North Korea is likely capable and willing to launch disruptive or destructive cyber attacks to support the achievement of its political objectives; (4) Iran conducts information theft, propaganda, and cyber attacks to support its security priorities, influence the situation, and counter threats; and (5) ISIL targeted and released sensitive information about U.S. Forces personnel as a new tactic to spur "lone-wolf" attacks. See Part I, Chapter 2, Section 1 "Situation in Syria and Iraq" regarding the ISIL's use of cyberspace.

5 "APT 1: Exposing One of China's Cyber Espionage Units," released in February 2013 by Mandiant, a U.S. information security company, concludes that the most active cyber attack group targeting the United States and other countries is Unit 61398 under then Third Department of the PLA General Staff Department. The report also states that then Third Department of the General Staff Department, which constituted the cyber unit, had 130,000 personnel.

6 The Annual Report of the U.S.-China Economic and Security Review Commission (November 2015) notes that the Chinese government supports large-scale cyber espionage and has stolen information from private companies and the U.S. government. The report states that China seeks to acquire offensive capabilities, identifying space and cyberspace as strategically vital realms, and is capable of standing up to a militarily superior adversary by deploying its cyber warfare capabilities.

paper "China's Military Strategy" (May 2015),[7] China will accelerate efforts to build up its cyber capacity. Furthermore, it has been suggested that cyber warfare units have been formed under the Strategic Support Force that was created as part of China's military reforms[8] in late December 2015. In May 2014, the U.S. Department of Justice announced that officers in "Unit 61398," the cyber attack unit of the Chinese PLA, and others were indicted, alleging that they conducted cyber attacks against U.S. companies.[9] 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. While Chinese involvement in this attack is also suggested,[10] China denies government involvement and explains that it was a "crime" involving Chinese hackers. Additionally, in July 2014, the Canadian government alleged that it was a target of a Chinese cyber attack, mentioning China by name for the first time.[11] As regards China's intention behind these cyber attacks, it is suggested that the Chinese PLA and espionage services steal information from U.S. companies and feed that back into Chinese companies as part of the national strategy to win economically.[12]

In October 2014, the White House's unclassified information system was hacked.[13] In December 2015, a large-scale power outage occurred in Ukraine.[14] It is said that Russia was involved in these attacks. It has been pointed out that the Russian military, intelligence and security agencies, and other organizations engage in cyber attacks.[15] Furthermore, the Russian military is considered to be establishing its own cyber command, which will be responsible for conducting offensive cyber activities, including inserting malware into enemy command and control systems.[16] It has been indicated that such Russian activities reflect objectives including: (1) intelligence gathering to support Russian decision-making on the issues of Ukraine and Syria; (2) operations to support military and political objectives; and (3) continuing preparation of the cyberspace environment for future contingencies.[17]

In March 2013, cyber attacks hit broadcasting stations and financial institutions in the ROK. In June and July 2013, cyber attacks hit the ROK President's Office, government agencies, broadcasting stations, and newspaper companies. In addition, a cyber attack against the Seoul subway system has been reported. 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.[18] 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

7 The defense white paper notes that, "Cyberspace has become a new pillar of economic and social development, and a new domain of national security," "As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces," and China is "one of the major victims of hacker attacks."

8 Since September 2015, China has publicized a series of its decisions on military reforms, and in January 2016, announced the establishment of the Strategic Support Force and other units. While the details of the Force's tasks and organization have not been revealed, it is suggested that it is in charge of outer space, cyber, and electronic warfare.

9 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 asserted that the United States "fabricated facts" and announced 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.

10 See the Annual Report of the U.S.-China Economic and Security Review Commission (November 2015). In addition to this attack, the report states that a U.S. airline company was attacked by the same method used in the attack against the U.S. OPM.

11 According to a Canadian government release dated July 2014.

12 According to Dennis F. Poindexter's testimony at the hearing of the U.S.-China Economic and Security Review Commission in June 2015. The Commission's Annual Report (November 2015) notes that the technology sectors of China's strategic emerging industries, such as high-end manufacturing equipment, next-generation IT, new materials, and biotechnology, have become a target of interest for Chinese hackers' activities.

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

14 In February 2016, the New York Times reported that there were doubts about the involvement of the Russian military with which Ukraine is in a standoff over the annexation of Crimea and other matters.

15 "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.

16 According to 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.

17 According to the U.S. Director of National Intelligence's "Worldwide Threat Assessment" (February 2016).

18 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.

sufficient evidence to conclude that the North Korean government was responsible for these cyber attacks.[19] It has been suggested that North Korean government organizations are involved in such cyber attacks[20] and that North Korea is training personnel on a national scale.[21] It is considered that these cyber attacks are conducted for political purposes.[22]

Stuxnet, a malware designed to attack industrial control systems (ICS) was discovered in June 2010, followed by discoveries of advanced malware on multiple occasions.[23]

Cyberattacks on the information and communications networks of governments and militaries,[24] 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.

Meanwhile, in Japan, the Japan Pension Service was a target of a cyber attack in May 2015, which led to the leak of the personal information of pension recipients and policyholders. Hacker groups and others have also carried out cyber attacks against Japanese government agencies and companies.

In addition, supply chain risks, such as companies supplying products embedded with deliberately and illegally altered programs, have been also pointed out.[25] Furthermore, it has been suggested that the rise in devices that connect to the Internet, including "smart" devices incorporated into household appliances, can increase network complexity, and that private infrastructures and government systems could become more vulnerable, including to malicious attacks aimed at causing malfunctions to systems equipped with artificial intelligence.[26]

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.[27]

A number of issues have been raised 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, it is regarded that the international community has diverging views concerning the fundamental matters of cyberspace, including how international law applies. It is suggested that countries have clashing claims, with the United States, Europe, and Japan calling for maintaining a free cyberspace, while many countries including Russia, China, and emerging countries call for strengthening national control of cyberspace. Against this backdrop, there has been a movement to promote the rule of law in cyberspace in the international community. In August 2015, a UN Group of Governmental Experts (GGE) released a

19 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.

20 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 Secretary of the Korea Workers' Party 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 "2015 Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea" published in February 2016, it is stated that North Korea has an 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.

21 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.

22 According to U.S. Director of National Intelligence Clapper's written testimony on "Worldwide Cyber Threats" to the House Permanent Select Committee on Intelligence in September 2015.

23 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.

24 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 June 2015, the "Syrian Electronic Army" attacked and hacked the U.S. Department of Defense's Army website. Furthermore, in November 2015, the international hacker group "Anonymous" announced that it attacked accounts linked to ISIL over the terror attacks in Paris. As these examples demonstrate, there are also frequent cyber attacks by hacker groups.

25 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 Chinese Communist Party, 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.

26 According to the U.S. Director of National Intelligence's "Worldwide Threat Assessment" of February 2016.

27 Generally, the trends at the governmental level are thought to include the following: (1) organizations related to cybersecurity 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.

report containing recommendations on how to apply the principles of international law to acts using cyberspace and on voluntary, non-binding norms of state behavior.[28]

See>> Part III, Chapter 1, Section 2-7 (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 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 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[29] 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.[30] Additionally, the DoD states that the aforementioned cyber capabilities include cyber operations to disrupt an adversary's military-related systems.

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 cyberspace. U.S. 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, U.S. Cyber Command has created the Cyber National Mission Forces to support U.S. defense against national-level threats, and the Cyber Combat Mission Force that supports the operations conducted by unified combatant commands on the cyber front. These three forces are collectively referred to as the Cyber Mission Force.[31]

In February 2016, President Obama unveiled the Cybersecurity National Action Plan. In his FY2017 budget request, the President announced that the budget for cybersecurity investments would be increased significantly, identifying cybersecurity as one of the top national security issues.[32] According to the Cybersecurity National Action Plan, the federal government as a whole will take actions, including establishing the Commission on Enhancing National Cybersecurity and making additional investments in the federal government's cyber-related technologies, education, and personnel recruitment.

The DoD, too, appropriated US$6.7 billion for cyber

28 The U.N. 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. In its report released in August 2015, the GGE expresses the following views regarding the application of international law to states' use of ICT, namely, that: (1) states must observe state sovereignty and other principles in their use of ICT; (2) the GGE must note the "inherent right" of states to take measures consistent with international law and as recognized in the U.N. Charter; (3) states must not use proxies to commit internationally wrongful acts using ICT; and (4) states should ensure that their territory is not used by non-state actors to commit such acts. Furthermore, with regard to voluntary norms of state behavior, the report recommends, for example, that a state should not conduct or support ICT activity that intentionally damages critical infrastructure.

29 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.

30 In order to execute these missions in cyberspace, 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.

31 According to a statement made in April 2015 by the commanding officers of U.S. Cyber Command to the U.S. Senate Committee on Armed Services, among other sources, the three forces are made up of several teams, and dozens of them are currently operating. Employing the National Guard and reserve units, the Cyber Mission Force is set to have 133 teams (National Mission Teams [13 teams], Cyber Protection Teams [68 teams], Combat Mission Teams [27 teams], Support Teams [25 teams]) and 6,200 personnel by September 2018.

32 In the U.S. President's budget request for FY2017, approximately US$19 billion in total is appropriated for the overall government budget for cybersecurity, up 35% from the FY2016 budget.

operations in its FY2017 budget request, up 15.5% from the FY2016 budget. It includes the budget for developing the readiness of the U.S. Cyber Command, including continuing to organize the Cyber Mission Force, and the budget for improving defensive cyber operation capabilities[33] and offensive cyber operation capabilities.[34]

The United States deems that China continues to conduct cyber-enabled theft targeting a broad set of U.S. interests ranging from information related to national security, to sensitive economic information and U.S. intellectual property.

In September 2015, U.S. President Obama and Chinese President Xi Jinping agreed at their summit meeting that the two countries would not conduct cyber-enabled theft of intellectual property.[35] In December 2015, the U.S. and Chinese governments held their first ministerial dialogue on cyber issues and reached an agreement regarding the establishment of guidelines for combatting cybercrime, implementation of a tabletop exercise, and establishment of a hotline.

2 NATO

The new 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, 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.[36]

Since 2008, NATO has been conducting cyber defense exercises on an annual basis to boost 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 action plans for capability enhancement, establishment of norms, cooperation with other countries, and personnel training. In November 2015, the United Kingdom released the NSS-SDSR2015. It commits 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. It also commits to publishing the second National Cyber Security Strategy in 2016.

In terms of organization, the Office of Cyber Security and Information Assurance (OCSIA) was established within the Cabinet Office to form and coordinate cybersecurity strategy for the overall government, as well as the Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) to monitor cyberspace. In addition, the Defence Cyber Operations Group (DCOG), which unifies cyber activities within the Ministry of Defence, was established.[37] The "NSS-SDSR2015" released in November 2015 states that the National Cyber Centre would be established under GCHQ, the unit that first responds to cyber attacks, in order to respond swiftly and effectively to cyber attacks.

In January 2015, Prime Minister Cameron and President Obama agreed to strengthen cooperation in the area of cyber defense.[38] Furthermore, the United Kingdom and China agreed that they would not conduct or support cyber-enabled theft of intellectual property and other information.[39] In such ways, the United Kingdom is working to deepen its collaboration with other countries.

33 In March 2016, U.S. Secretary of Defense Carter announced that a pilot program would be launched in April 2016 that would invite private hackers to hack the DoD website in order to study the security weaknesses. Furthermore, the DoD is making innovative efforts to strengthen its defensive cyber capabilities.

34 The U.S. Forces have disclosed that their offensive cyber capabilities are already operational. For example, they place excessive burden on the networks of ISIL aimed at disrupting its chain of command.

35 During the summit meeting, President Obama allegedly expressed deep concerns over China's cyber attacks and stated that the United States would exercise all possible tools, hinting at the application of economic sanctions. Meanwhile, the two sides agreed that they would hold U.S.-China ministerial dialogues on fighting cybercrime.

36 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.

37 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 defense, and approved the establishment of the Joint Cyber Reserves.

38 According to a White House release, the U.K. GCHQ and Security Service (SS) and the U.S. National Security Agency (NSA) and Federal Bureau of Investigation (FBI) will work together closely on cybersecurity and cyber defense. In addition, in November 2015, the U.K. and U.S. governments conducted a joint exercise to strengthen their bilateral cyber cooperation as well as their effective response capabilities to cyber incidents in the financial industry, with the participation of their cyber, financial, and intelligence agencies, among other participants.

39 In October 2015, Chinese President Xi Jinping visited the United Kingdom as a state guest, and conducted a summit meeting with U.K. Prime Minister Cameron.

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 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.

In terms of organization, the Australian Cyber Security Centre (ACSC) that brings cybersecurity capabilities from across the government into a single location was established in November 2014 to respond to major cybersecurity issues related to government agencies and critical infrastructures.[40] In July 2015, the ACSC issued its first report on cybersecurity,[41] which contended that the number, type, and sophistication of cyber threats to Australia are all increasing.

In addition, the Defence White Paper released in February 2016 notes that cyber attacks are a direct threat to the Australian Defence Force's warfighting ability given its reliance on information networks, and commits to strengthening the Department of Defence's cyber capabilities and systems.

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[42] in responding to cyber attacks. It places particular emphasis on strengthening the following five areas: prevention, detection, response,[43] 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 operates under the direct control of the Ministry of National Defense.[44] In April 2015, to strengthen its measures against cyber attacks, the ROK government established the cybersecurity advisor post at the National Security Office of the President's Office.

40 The ACSC, comprised of staff from the Australian Crime Commission, the Australian Federal Police, the Australian Security Intelligence Organisation, the Australian Signals Directorate, the Australian Computer Emergency Response Team, and the Defence Intelligence Organisation, analyzes threats in cyberspace and responds to both public and private sector incidents. The ACSC is set to have approximately 300 personnel by 2017.

41 According to the report, adversaries in cyberspace targeting Australia are: (1) foreign government-sponsored adversaries; (2) serious and organized criminals; and (3) groups motivated by certain issues and individuals with personal grievances.

42 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.

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

44 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 one of the military reforms for the future.