# 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, functional impairment of the networks through simultaneous transmission of large quantities of data, as well as attacks intending to shut down or take over a system belonging to critical infrastructure, such as power systems. Also, 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 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 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,

[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 then 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 3, Section 1 regarding ISIL's use of cyberspace.

intelligence agencies, security agencies, private hacker groups, and companies.[5,6] According to the defense white 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 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,[9] China denies government involvement and explains that it was a "crime" involving Chinese hackers. Additionally, it has been pointed out that China is using cyber attacks to obtain sensitive information concerning critical infrastructure, national security decision-making processes, and plans of military tactics of other countries.[10] China's cyber attacks have also shifted recently, from attacks by large numbers of amateurs to highly professional attacks by a select few individuals.[11]

In December 2015, a large-scale power outage occurred in Ukraine.[12] It is said that Russia was involved in this attack. The U.S. Government has also criticized Russian intelligence agencies for carrying out a cyber attack to affect the outcome of the 2016 U.S. presidential election.[13, 14] In March 2017, the U.S. Department of Justice announced that it indicted four hackers, including two personnel from Russia's Federal Security Service (FSB), for computer hacking in order to steal information from at least 500 million user accounts of a major Internet company in the United States. It is believed that the Russian military, intelligence and security agencies, and other organizations engage in cyber attacks. Furthermore, it is clear that the Russian military has its own cyber command.[15] This cyber command is believed to 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 December 2016, it was found that a cyber attack breached the internal network of the ROK Armed Forces. According to the ROK Ministry of National Defense, this was the first time that its military network had been hacked. This cyber attack resulted in the loss of certain military documents, including confidential information. The ROK's cyber command stated that it presumed

[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 2016) notes that China carries out cyber espionage led by the Ministry of State Security and military organizations as well as cyber espionage led by China's many non-state actors targeting the United States. These actors include hackers contracted by the government, civilian "patriotic hackers," and criminal organizations.

[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] 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.

[10] According to the Annual Report of the U.S.-China Economic and Security Review Commission released in November 2016.

[11] According to the Annual Report of the U.S.-China Economic and Security Review Commission released in November 2016.

[12] 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.

[13] Critical elections were held in major EU countries in 2017, notably the Dutch general election (House of Representatives) in March and the French presidential election in May, and there were concerns that similar cyber attacks would affect their outcomes. During the presidential campaign in France, Macron, known as a hardliner on Russia, was reportedly a target of a cyber attack, as well as a widespread fake news story about having hidden assets in a tax haven. After being appointed president, in a joint press conference of the French and Russian presidents, Macron criticized Russian media outlets by name, referring to them as organs of lying propaganda. German Bundestag elections will be held in autumn 2017, and it remains a concern that these elections too will be a target of similar incidents.

[14] According to the joint statement issued by the U.S. Department of Homeland Security and Director of National Intelligence Clapper in October 2016, the joint report issued by the U.S. Department of Homeland Security and FBI concerning Russian cyber attacks on the United States released in December 2016, and the U.S. intelligence community report on Russia's cyber attacks on the U.S. presidential election released in January 2017.

[15] According to a statement made by Russian Minister of Defence Shoigu during a briefing of lower house members in February 2017. According to this statement, the Russian military has a cyber command. Minister Shoigu emphasized that the command was "for opposing political propaganda activities" since there was an information war taking place between Russia and the West, indicating the purpose of the command was for defense. Also, it is pointed out that Russia's cyber force numbers around 1,000.

[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).

this incident to be a cyber attack by North Korea.[18] It has been pointed out that North Korea is involved in such cyber attacks on government institutions[19] and is training personnel nationally for such attacks.[20] It is viewed that such cyber attacks are implemented as a military operation.

Cyber attacks on the information and communications networks of governments and militaries,[21] 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 theft 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.[22] 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.[23] Also, in June 2010, a malware called "Stuxnet" designed to attack the Industrial Control System (ICS) was discovered, and since then sophisticated malware has been detected frequently.[24]

## 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.[25]

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,[26] 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. For example, in August 2015, a UN Group of Governmental Experts (GGE) released a

[18] Based on various media reports. The IP address (Internet address) used in the attack was Shenyang, China. It is pointed out that previous cyber attacks involving North Korea used this same IP address.

[19] 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 Korean 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 2016 Defense White Paper published by the ROK in January 2017 notes that North Korea has concentrated on boosting its cyber unit to nearly 7,000 personnel.

[20] 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.

[21] 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.

[22] 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.

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

[24] This was the first ever virus program confirmed to target control systems that combine specific software and hardware. It is pointed out that such a virus program has the ability to access the target system undetected and then steal information and make modifications to the system. Additionally, malware programs called "Duqu," "Flame," "Gauss," and "Shamoon" have been detected in October 2011, May 2012, June 2012, and August 2012, respectively.

[25] 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.

[26] These countries have called for a multi-stakeholder approach including free flowing information as well as private-sector companies and the civil society, in addition to governments.

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.[27]

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[28] for partnership with other nations and people to realize this vision. The Strategy also points out seven policy priorities.

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.

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]

The Trump administration that was inaugurated in January 2017 announced its policy on the rebuilding of the U.S. Forces on the day of its inauguration. It indicated that a variety of means must be employed to protect national security secrets and systems from cyber attacks, and that based on this awareness the U.S. Cyber Command would give top priority to developing both defensive and offensive cyber capabilities.

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, then 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.[32] Nevertheless, it is pointed out that cyber espionage from China continues unimpeded as before.[33]

[27] The UN 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 UN 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.

[28] The Strategy points out seven policy priorities: economy; protection of national networks; law enforcement; military; Internet governance; international development; and Internet freedom.

[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] During the summit meeting, then 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.

[33] According to the Annual Report of the U.S.-China Economic and Security Review Commission released in November 2016.

## 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, NATO has conducted cyber defense training exercises annually since 2008 to heighten the defense capabilities of its servers. NATO and the EU have expressed their intention to expand collaboration in the fields of cybersecurity and cyber defense.[34]

Also, in 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) was authorized to serve as NATO's cyber defense-related research and training institution,[35] and was established in Estonia's capital of Tallinn. CCD COE carries out research on the relationship between cyber activities and international law, and created the "Tallinn Manual."[36] In February 2017, "Tallinn Manual 2.0" was published as a continuation of this manual in which a total of 154 "black letter" rules are identified 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 the use of force and laws on armed conflict.

## 3 The United Kingdom

The United Kingdom, in November 2015 in its "NSS-SDSR2015", 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 presented 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 possess the means to effectively "defend" from cyber threats, to "deter" through having the means for offensive cyber action, and to "develop" cutting-edge technologies.

In terms of the Government's overall cybersecurity policy, the Office of Cyber Security and Information Assurance (OCSIA) has been set up to present strategic policies and to coordinate cybersecurity planning for the overall government. 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 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

[34] 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.

[35] According to the Joint Declaration issued after the NATO Summit in July 2016.

[36] The "Tallinn Manual" and the "Tallinn Manual 2.0" are both considered independent outputs of the members that participated in the project (Professor Michael N. Schmitt of the U.S. Naval War College served as project leader; members included professionals, scholars on international law, and experts in cyber technology in the West and other areas), and not the official view of NATO.

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.[37] In July 2015, the ACSC issued its first report on cybersecurity,[38] 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[39] in responding to cyber attacks. It places particular emphasis on strengthening the following five areas: prevention, detection, response,[40] 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.[41] 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. Furthermore, the Ministry of National Defense prepared the "National Cyber Security Strategy" that presents a vision for national cybersecurity and a direction for medium- to long-term development. It also created the "National Cybersecurity Crisis Response Manual" that stipulates rapid response procedures to cybersecurity crises. 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 publishing a field manual on "joint cyber tactics."

[37] 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 grow to approximately 300 personnel by 2017.

[38] 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.

[39] 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.

[40] 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.

[41] 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.