3 The United Kingdom

In November 2011, the United Kingdom announced a new Cyber Security Strategy, which set goals for the period until 2015 and specified action plans for capability enhancement, establishment of norms, cooperation with other countries, and personnel training.

In terms of organization, the Office of Cyber Security and Information Assurance (OCSIA) was established within the Cabinet Office to form and coordinate cyber security strategy for the overall government, as well as the Cyber Security Operations Centre (CSOC) under the Government Communications Headquarters (GCHQ) to monitor cyberspace. The Defence Cyber Operations Group (DCOG), which unifies cyber activities within the Ministry of Defence, was established in April 2012 as a provisional measure. It is scheduled to acquire full operational capability by March 2015[25].

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

4 Australia

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

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

5 Republic of Korea

The ROK formulated the National Cyber Security Master Plan in August 2011, which clarifies the supervisory functions of the National Intelligence Service[28] in responding to cyber attacks. It places particular emphasis on strengthening the following five areas: prevention, detection, response[29], systems, and security base. In the national defense sector, the Cyberspace Command was established in January 2010 to carry out planning, implementation, training, and research and development for its cyberspace operations, and currently serves as the division under the direct control of the Ministry of National Defense[30].

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

1 Military Science and Technological Trends

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

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

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

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

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

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

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

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

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

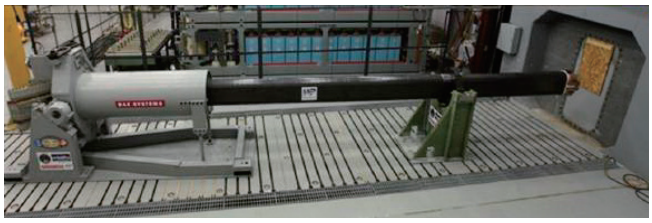
30 The basic plan for national defense reform (2012-2030) that was submitted to the President in August 2012 by the Ministry of National Defense proposed significant enhancement of cyber warfare capability as a future military reform.

C4ISR, and unmanned technology (e.g. drones[1]) to be able to carry out more precise and effective attacks. To this end, these countries also place emphasis on R&D activities related to stealth technology for reducing the risk of attrition of military power as a result of increased preemptive attacks due to improvements in stealth capacity, and as a result of improved survivability, and nanotechnology used for parts and materials related to these technologies. Recently, reports have been published of successful tests of railguns[2] and high energy laser weapons[3] that are expected to provide effective firepower compared to existing weapons, such as artillery, in terms of their cost per firing, range, precision, promptness, among other aspects. Furthermore, there have been reports about the development of high speed strike weapons (HSSW) that can strike even long-range targets with conventional weapons, quickly and with pinpoint accuracy[4]. The Quadrennial Defense Review (QDR), published by the U.S. Department of Defense in March 2014, states that the proliferation of state-of-the-art technologies[5] will transform the mode of warfare.

Recent advancements in military science and technology[6] are also largely attributed to the advancement of civil technology. In recent years, as the capabilities of existing equipment are improved and new equipment is developed, spin-on and dual-use technology[7] based on civil technology have been leveraged frequently. In particular, ICT-related civil technology has been applied to a variety of equipments on a larger scale.

On the other hand, it is expected that countries having difficulty possessing high-tech forces for technological and economic reasons as well as non-state actors including terrorist organizations will carry out research and development on weapons and other equipment that will enable them to gain superiority in fighting against countries with state-of-the-art technology, and illegitimately obtain technology through ICT or other means. In short, these countries and organizations tend to focus on asymmetrical means of attack that can be developed or obtained with relatively low cost, enabling them to attack their opponents' vulnerability without using conventional military capabilities. These asymmetrical means of attack include weapons of mass destruction, such as nuclear, chemical, and biological weapons; ballistic missiles; terrorist attacks; and cyber attacks.

As asymmetrical means of attack may spread throughout the world, the research and development of technology[8] that responds to these asymmetrical threats is also recognized as an important challenge.



Electromagnetic railgun under development at the U.S. Office of Naval Research (ONR) [ONR]

1 Drones for military use which have been developed include unmanned aerial vehicle (UAV), unmanned ground vehicle (UGV), unmanned maritime vehicle (UMV), unmanned surface vehicle (USV), and unmanned undersea vehicle (UUV). It is suggested that these drones could shift from human-operated types to fully autonomous types, as known as Lethal Autonomous Weapons Systems (LAWS). In May 2014, an informal meeting of the United Nations Convention on Certain Conventional Weapons (CCW) discussed for the first time the humanitarian, legal, and other issues related to the operation of LAWS that automatically kill an enemy without human judgment. These issues were again discussed at a meeting of the high contracting parties to the Convention in November 2014.

2 A railgun is a weapon that fires bullets by using the magnetic field generated from electric energy instead of gunpowder. The U.S. Forces have developed a railgun with a range of about 370km, or about ten times that of the existing 5-inch (127mm) ammunition. A single railgun shot reportedly costs 1/20th to 1/60th the price of a missile.

3 The U.S. Forces are developing laser weapons to defend against small boats and strengthen low-altitude air defense capabilities, including defense against drones. From September to November 2014, a laser was test fired onboard the USS Ponce. Observers suggest that high energy laser weapons systems would be miniaturized, with a view to placing the weapons also on light mobility vehicles. The cost of a laser shot is reported to be less than US$1.

4 The goal of the HSSW is to considerably shorten the time required for attack with a conventional weapon. The HSSW is deemed to travel at a low trajectory that is clearly different from the trajectory of ballistic missiles. According to observers, the United States and China are developing HSSWs.

5 The QDR describes that such technologies include "counter-stealth technology" that used to require large budgets, "automated and autonomous systems as well as robotics" that already have a wide range of commercial and military applications, "low-cost three-dimensional printers" that could revolutionize weapons manufacturing and logistics related to warfare, and "biotechnology breakthroughs" that could make new ways of developing weapons of mass destruction possible. The report notes that it remains unclear how these technologies will manifest on the battlefield.

6 In November 2014, then-U.S. Secretary of Defense Chuck Hagel unveiled the Defense Innovation Initiative (as known as the "Third Offset Strategy"). This initiative is designed to offset an enemy's military superiority, such as A2/AD, with cutting-edge technology and operational concepts in which the United States has superiority. See Part I, Chapter 1, Section 1-1-4.

7 In the field of military technology, "spin-on" generally means applying civil technology to military technology, "spin-off" means the reverse, and "dual-use technology" means technology available for use in both areas.

8 They include BMD or technologies for countering ballistic missiles, terrorist attacks, cyber attacks, etc. as well as ICT.

2 Trends Concerning Defense Production and Technological Bases

Recently, Western countries in particular have continued to face difficulties in significantly increasing defense budgets. On the other hand, the sophistication of military science and technology and the greater complexity of equipment, as explained in 1 above, have escalated development and production costs and raised unit prices for procurement, resulting in a reduced number of procured units. Under these circumstances, many countries are working on a variety of initiatives in order to maintain and enhance their national defense production and technological bases.

Western countries have set a target to increase competitiveness through realignment of their defense industry, based on the aforementioned situation related to national defense budgets. The United States has seen repeated mergers and integrations among domestic corporations, while Europe has experienced cross-border mergers and integrations of the defense industry, especially in Germany, France, the United Kingdom, and Italy[9].

In response to escalating development and production costs, Western countries are also promoting joint development and production and technological cooperation related to defense equipment among their allies and partners. This move can be attributed to such factors as (1) splitting development and production costs, (2) expanding demands in all countries participating in joint development and production, (3) mutual complementarity of technologies, and (4) raising domestic technology levels by obtaining the latest technology.

Furthermore, an international logistic support system called "Autonomic Logistics Global Sustainment" (ALGS) was adopted for the maintenance of the F-35 fighter aircraft, with the aircraft having been developed through international collaboration. This system enables all F-35 user countries to share its parts and components globally. The establishment of such international frameworks for logistic support and the progress of international joint development and production need to be observed closely.

See Part III, Chapter 2, Section 4 (Defense Equipment and Technology Cooperation)

Countries have been exporting defense equipment overseas since the Cold War era, and even in recent years, many countries have been promoting a policy of overseas exporting. As defense equipment has faced a dramatic increase in its development and production costs, countries aim to maintain and strengthen their domestic defense industry by expanding demands in foreign markets through overseas exports. Furthermore, it is considered that countries leverage exports as a diplomatic tool for expanding their influence in the export destination countries. In addition, countries such as China and the Republic of Korea have established the infrastructure required to manufacture weapons through their past imports of defense equipment and their improved capabilities in science and technology, enabling them to attain the status of an export country of affordable defense equipment and to increase their export volumes.

In recent years, defense equipment exports to the Asia-Pacific region have increased. The underlying factors suggested include the economic growth of the Asia-Pacific region, the greater influence of China, disputes over territorial sovereignty, and addressing the enhanced military capabilities of neighboring countries.

See Fig. I-2-6-1 (Top Ranking Countries in Major Conventional Arms Export (2010–2014))

Fig. I-2-6-1 Top Ranking Countries in Major Conventional Arms Export (2010–2014)

	Country	Global shares in defense equipment export (%), 2010–2014	Comparison with 2005–2009 export values (%)
1	United States	31%	+23%
2	Russia	27%	+37%
3	China	5%	+143%
4	Germany	5%	–43%
5	France	5%	–27%
6	United Kingdom	4%	+23%
7	Spain	3%	+32%
8	Italy	3%	+37%
9	Ukraine	3%	+73%
10	Israel	2%	+33%
11	Sweden	2%	+23%
12	The Netherlands	2%	–32%
13	Canada	1%	+16%
14	Switzerland	1%	–12%
15	Republic of Korea	1%	+14%
16	Norway	1%	+110%
17	Turkey	1%	+149%

Note: Created based on "SIPRI Arms Transfer Database." Countries with 1% or more share are listed (decimals are rounded).

9 Large corporations involved with the defense industry of Western countries have high defense business ratios in their total revenues. In particular, the United States and the United Kingdom have large corporations with most of their revenues attributed to the defense business.