Section 6 New Efforts Based on Recent Trends

1 Efforts for Development and Use of Space

Japan, a country which has an exclusively defense-oriented policy, is strongly required to use outer space, which does not belong to the national territory of any country and is not constrained by conditions such as surface topography, to strengthen information gathering functions for detecting signs of various contingencies in advance, and warning and surveillance functions in sea and air space surrounding Japan, and to ensure lines of communication during the international peace cooperation activities of the SDF.

The enactment of the Basic Space Law[1], passed by the Diet in May 2008, has made it clearer that the development and use of space by Japan shall be carried out under the pacifism enshrined in the Constitution of Japan in compliance with international commitments. The law also stipulates that the Government of Japan shall take necessary measures to promote the development and use of space that contributes to ensuring the peace and security of the international community, as well as to the security of Japan.

In 2009, the strategic Headquarters for Space Policy Cabinet Secretariat which was established based on the Basic Space Law formulated the Basic Plan for Space Policy, which includes the six key elements such as the realization of a secure, pleasant, and affluent society utilizing space, as well as the enhancement of national security utilizing space.

Furthermore, the 2010 NDPG stipulate promotion of the development and the use of outer space with a view to strengthening information gathering and communications functions, etc.

Meanwhile, on January 2009, the Committee on Promotion of Space Development and Use established in the Ministry of Defense formulated the "Basic Guidelines for Space Development and Use of Space" (Basic Guidelines). The Basic Guidelines stipulates that it is extremely beneficial to take advantage of the nature of space for defense purpose and it will be an effective means to strengthen C4ISR[2] capability in light of the focus of the buildup of defense capabilities on enabling accurate situational awareness, information sharing, command and control operations, and thereby achieving systemization – maximizing of the equipment's performance as an ensemble.

The Ministry of Defense will promote new development and use of space for the national security in coordination with related ministries, based on the Basic Plan for Space Policy, the 2010 NDPG, and the Basic Guidelines. In FY2012, it will address projects such as 1) research for enhancement of C4ISR utilizing space, 2) enhancement, maintenance, and operation of X-band SATCOM functions, and 3) participation in the USAF Space Fundamentals Course.

Of these, with regard to the enhancement of X-band SATCOM, in light of the fact that two of the communications satellites (Superbird-B2 and Superbird-D) used by the Ministry of Defense and Self-Defense Forces for command and control of tactical forces are due to reach the end of their service lives in FY2015, these satellite communications networks will be reorganized. This reorganization will facilitate high-speed, large-capacity communications that are more resistant to interference, in order to accommodate the recent growth in communications requirements, as well as integrating communications systems, thereby contributing to the construction of a dynamic defense force. Moreover, from the perspective of maximizing cost-effectiveness, it has been decided to implement the project by means of the PFI (private finance initiative)[3] system, and 19 years' worth of costs (approximately 122.4 billion yen) has been allocated in the FY2012 budget, to cover expenses from the manufacture of the satellites through to the end of their service life. In this project, after guaranteeing transparency and fairness in tenders, etc. through open tendering, the content of the proposals will be screened impartially, from the perspective of security, with bidders being asked to implement the appropriate management systems and conservation measures.

2 Initiatives Related to the Stable Use of Cyberspace

Information and communications technology has developed and been widely adopted at great speed and, as a result, it is now essential as the infrastructure for socioeconomic activities. On the other hand, this means there is a possibility that people's lives and economic activities will be severely affected if the computer systems or networks are compromised. Based on this awareness, the Information Security Policy Council, which decides the basic strategy for Japan's information security measures, and its implementation agency, the National Information Security Center (NISC), were established in 2005, and since then a variety

1 See <http://www.kantei.go.jp/jp/singi/utyuu/about2.html>

2 Abbreviation "Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance" which is the collective term of each function.

3 See Part Ⅲ, Chapter 4, Section 2

of initiatives related to the information security problems of Japan have been undertaken by public and private sector entities with the NISC playing the leading role[1].

In May 2010, the Information Security Policy Council formulated the Information Security Strategy for Protecting the Nation as a comprehensive strategy for the period from FY2010 to FY2013[2]. This strategy document incorporated extremely important policies with respect to the national security, including preparation of the government's initial response to a large-scale cyber attack, reinforcement of protection against cyber attacks, and reinforcement of international alliances against cyber attacks, etc.

Along with the National Police Agency, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry, the Ministry of Defense is designated one of the government agencies which must cooperate particularly closely with the NISC. Therefore, the Ministry contributes to the cross-sector initiatives led by the NISC by providing it with the knowledge and skills possessed by the Ministry of Defense/the SDF. For example, the Ministry participates in cyber attack response drills and personnel exchanges, and provides information about cyber attacks, etc.

Moreover, in light of the cyber attacks on companies involved in the defense field which were reported in September 2011, the Ministry of Defense has conducted deliberations regarding the strengthening of measures to ensure information security in procurement, and revised its contractual agreements with companies that use internal servers, etc. to handle Ministry of Defense intelligence that should be protected, as follows:

1) Obligation introduced to submit a report to the Ministry of Defense immediately, in the event that a server or computer on which information that should be protected is stored becomes infected with a virus, etc. or is subject to unauthorized access, or if a server/computer connected to the same network as that server/computer is infected with a virus, etc.
2) Compilation of a communication diagram that clarifies those in charge and those who should be contacted
3) Implementation of a full scan by anti-virus software at least once a week
4) 24/7 year-round monitoring to ensure that no information that should be protected is leaked outside the company
5) Preservation for at least three months of records of access to information that should be protected
6) Strengthening of encryption measures
7) Audits of the status of education and training of staff

Furthermore, in response to cyber attacks on defense-related companies, the Government has conducted deliberations concerning measures to deal with these, via the Subcommittee for Strengthening Public-Private Cooperation, which was established in October 2011; the results of these deliberations were submitted to the Information Security Policy Council in the form of a report entitled Approaches to Public-Private Cooperation in Information Security Measures[3]. This report points out the need for all government bodies, ministries and agencies to put in place a computer security incident response team (CSIRT)[4] within their organizations and to seek expert, working-level collaboration between the CSIRT within each organization, including both the public and private sector; in addition, it highlights the importance of forming a cyber incident version of the disaster medical assistant team (DMAT), in which capable personnel (primarily those from the NISC) can provide flexible support that transcends organizational boundaries in the event of an emergency. The Ministry of Defense will also make a significant contribution through active participation in deliberations concerning concrete measures aimed at improving security throughout the government.

3 Efforts Relating to the Environment

1 Effects Exerted by Climate Change on the Security Environment

With the mounting concern for climate change caused by global warming, there has been a growing tendency in recent years to give thought to the effects exerted by climate change on security. For example, in the Quadrennial Defense Review (QDR) published by the U.S. Department of Defense on February 2010, climate change is positioned as one of the factors which exert an important effect on the shape of the security environment of the future.

In this way, there is increasingly shared understanding of the fact that a range of effects may be brought about by climate change even on the security environment. The 2010 NDPG recognizes that from a long-term perspective, Japan should be aware of the impact which climate change may have on the security environment. Therefore, for Japan too, it is necessary to pay attention to the effects that climate change will exert on the security environment.

1 For more details about the activities, etc. of the National Information Security Center, see <http://www.nisc.go.jp>

2 See <http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf>

3 See <http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28shiryou1-1.pdf>

4 A specialist unit with the ability to respond in the event of an emergency relating to incidents that might pose a risk to information security. In the Ministry of Defense and Self-Defense Forces, bodies such as the Self Defense Forces C4 Systems Command (see Part III, Chapter 2, Section 3) correspond to this

2 Efforts for Environmental Conservation

As part of the government, the Ministry of Defense is developing action plans based on various government programs, and actively promoting a variety of efforts for the environment[1].

In 2001, the Ministry of Defense "Environment Month" and "Environment Week" were established. Garrisons nationwide also took part, performing diverse activities for the purpose of environmental conservation in areas such as preventing global warming. Their objective was to raise consciousness of people including SDF personnel in relation to environmental conservation.

In managing and maintaining its facilities and equipment, the SDF is promoting a range of efforts[2] to thoroughly conserve and reduce burdens on environment. Specifically, progress is being made in areas such as the installation of energy conservation equipment at SDF buildings, and the replacement of worn out vehicles with eco-cars, which are compatible with exhaust gas regulations, and which have excellent mileage. Thanks to efforts like these, great results can be expected in environmental conservation, such as reduced exhaust CO2, not to mention the substantial economic benefits.

Moreover, the Ministry of Defense is working on environmental conservation initiatives for the facilities and areas of the U.S. forces in Japan as well. The result of the comprehensive review of the Host Nation Support in December 2010 stipulated that, as part of the Japan-U.S. cooperation under the Green Alliance in the "2+2" joint statement issued in May that year, the two countries would endeavor to develop facilities that take the environment into account, for example by introducing designs that are environmentally-friendly because they are more energy-efficient.

4 Efforts for Ocean Policy

Under various circumstances regarding the ocean, including the sea areas surrounding Japan, the Basic Act on Ocean Policy[1] was put into force in July 2007 with the aim of the sound development of the economic society and the stability and improvement of the lives of the people in Japan as well as our contribution to the coexistence of the ocean and human beings, recognizing that it is critical for Japan, as a maritime nation, to establish a new Oceanic State which harmonizes peaceful and proactive development and use of the sea with the preservation of the marine environment. Then, the Headquarters for Ocean Policy was established within the Cabinet as a system to promote ocean policy intensively and comprehensively.

Based on this act, a cabinet decision was made in March 2008 to adopt the Basic Plan on Ocean Policy[2], which stipulates the basic policy of various measures with regard to the oceans in order to promote such measures comprehensively and systematically.

The Basic Plan on Ocean Policy includes extremely important measures in terms of the security of our country: for example, maintaining order at sea carried out from the viewpoint of securing maritime safety, efforts for maritime transport safety, countermeasures against marine-derived natural disasters, and securing maritime transport.

The Headquarters for Ocean Policy has been discussing coordination between ministries on the integration of marine survey data and the preservation and management of islands[3]. The Ministry of Defense participates in these discussions so that works in the related fields can be performed in closer coordination with other ministries.

The Basic Plan on Ocean Policy stipulates: the systematic development of ships and aircraft for the purpose of ensuring maritime safety; and the conducting of exercises based on the manuals on joint response to suspicious ships. Accordingly, the Ministry of Defense is engaging in a number of efforts in FY2012, including 1) build-up of equipment for ensuring maritime safety, such as construction of a destroyer and a submarine, acquisition of minesweeping and transporting aircrafts, and extension of the operating life of destroyers and rotary-wing patrol aircrafts, 2) research and development of

3 - 1 The action plan of the Ministry of Defense which was devised in October 2007 on the back of the "Action Plan for Greenhouse Gas Emission Reduction in Government Operations" (Cabinet decision made in the same year), the "Defense Agency Guidelines on Environmental Consideration" enacted in 2003 based on the government's Basic Environment Plan, and a review of those guidelines carried out in January 2005, etc. For details on Ministry of Defense guidelines for environmental consideration, see <http://www.mod.go.jp/j/approach/chouwa/index.html>.

2 Specifically, this includes measures for the purpose of conservation of the atmospheric environment, water quality conservation, recycling and waste disposal, improvement of environmental conservation facilities, and environmental surveys.

4 - 1 See <http://www.kantei.go.jp/jp/singi/kaiyou/about2.html>

2 See <http://www.kantei.go.jp/jp/singi/kaiyou/kihonkeikaku/index.html>

3 In order to appropriately manage the sea under jurisdiction, the area of which (approximately 4.47 million km2) includes exclusive economic zones extending to roughly 12 times the land area (of approximately 380,000 km2), in December 2009, the Headquarters for Ocean Policy formulated the "Basic Policy concerning Preservation Management of Islands for Management of the Sea." Then, on May 2010, a bill was passed that pertained to the conservation of exclusive economic zones and the continental shelf, and to improvement of base facilities. On July, based on that same bill, the Cabinet approved a basic plan on the conservation and development of base facilities in low-water mark areas for the conservation and promotion of the utilization of the Exclusive Economic Zone and Continental Shelf.

sonar technologies and capabilities that can detect noise-reduced submarines, and improved torpedoes for submarines, 3) dealing with pirates off the Coast of Somalia and in the Gulf of Aden, and 4) strengthening cooperation with the Japan Coast Guard through joint training to deal with unidentified ships.

See Part III, Chapter 3, Section 3

P-3C maritime patrol aircraft conducting surveillance activities

Column VOICE Commentary Q&A

Activities Related to Maritime Security

The Maritime SDF participated in the Indian Ocean Naval Symposium (IONS) for the first time as an observer in April 2012. At the symposium chiefs of naval staff from countries surrounding the Indian Ocean, including African nations, discussed issues relating to maritime security.

In response to the recent changes in the security environment, the 2010 National Defense Program Guidelines call for the development of Dynamic Defense Force focusing on operation. The MSDF has thus far been actively engaging not only in activities to deal with emergencies in areas surrounding Japan, such as warning and surveillance, but also in activities to create a more stable security environment at the regional and global levels, particularly those relating to maritime security, in order to maintain the free and open maritime order. As a maritime country, Japan depends on imports from abroad for the supply of most natural resources, so it is important to maintain the maritime order including ensuring the freedom of navigation at the global level, not to mention the security of maritime traffic leading to Japan.

The MSDF will share the results achieved through past various activities not only with the Asia-Pacific region but with countries around the world, including those surrounding the Indian Ocean, through which the sea lanes of communication leading to Japan go, by making use of this symposium and other multilateral frameworks, and it will thereby make efforts to improve the global security environment.

The IONS members comprise 32coastal countries of the Indian Ocean region

Indian Ocean Naval Symposium

5 Guidelines for the Overseas Transfer of Defense Equipment, etc.

Taking into account the National Defense Program Guidelines for FY 2011 and beyond, which stated that Japan will study measures to respond to the major changes regarding peace contributions, international cooperation, and international joint development and production, the Guidelines for Overseas Transfer of Defense Equipment, etc. were issued in December 2011 as a statement by the Chief Cabinet Secretary.

Based on this guidelines, the Government, in line with the ideas behind the individual exemption measures of the Three Principles on Arms Exports conducted so far, and there related policy guidelines here in after referred to as the "Three Principles" takes comprehensive exemption measures in overseas transfer of defense equipment, etc. 1) for cases related to peace contribution and international cooperation, 2) for cases regarding international joint development and production of defense equipment, etc., that contributes to Japan's security.

The overseas transfer of defense equipment, etc. will be allowed on the premise that strict control is in place, i.e. the counties participating in the pursuing in the projects are obliged to gain prior consent of the Government of Japan when pursuing extra-purpose use or transfer to third parties of the equipment, etc.

The Government is aware that the Three Principles are based on the basic philosophy of Japan as a peace-loving nation that seeks to avoid the aggravation of international conflicts, and will maintain the basic philosophy which underpins the Three Principles.

See References 20, 21