

Section
3**Responses in the Domains of Space, Cyberspace and Electromagnetic Spectrum**

Among the roles that must be served by Japan's defense capability as set forth in the NDPG, the idea of "(3) response in space, cyberspace and electromagnetic domains during all phases" is as follows.

In order to prevent any actions that impede its activities in space, cyberspace and electromagnetic domains, the SDF, on a steady-state basis, conducts persistent monitoring as well as collection and analysis of relevant information. In the event of the above-mentioned interference, the SDF will promptly identify incidents and take such measures as

damage limitation and recovery. In case of an armed attack against Japan, the SDF will, on top of taking these actions, block and eliminate the attack by leveraging capabilities in space, cyberspace and electromagnetic domains.

Furthermore, in light of society's growing dependence on space and cyberspace, the SDF will contribute to comprehensive, whole-of-government efforts concerning these domains under appropriate partnership and shared responsibility with relevant organizations.

1 Responses in Space Domain**1 The Whole-of-Government Approach**

The National Space Policy Secretariat¹ established in the Cabinet Office in April 2016 engages in the planning, drafting, coordinating, and other policy matters relating to the Government's development and use of space. In light of the environmental changes surrounding space policy and the new security policies stated in the National Security Strategy (NSS) that was approved by the Cabinet in 2013, the Basic Plan on Space Policy was decided upon in the Strategic Headquarters for National Space Policy which was established within the Cabinet in June 2020. This Basic Plan was prepared as a 10-year development plan focusing on approximately the next 20 years to sufficiently secure necessary budgets and strengthen the space policy to which the Government of Japan provides full efforts, including measures seen from the perspective of space security, setting goals of (1) Contributions to a variety of national interest; and (2) Strengthening comprehensive bases that support Japan's space activities, including industrial and science and technology bases. In particular, concerning the contributions to a variety of national interest, the plan states that Japan should advance: (1) Ensuring space security; (2) Contributing to conducting disaster responses, building national resilience and solving global issues; (3) Creating new knowledge based on space science and exploration; and (4) Realizing economic growth and innovations using space as an impetus.

Responding to Japan's progress in development and use of outer space, the Diet approved the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

(Remote Sensing Data Act) and Act on Launching of Spacecraft, etc. and Control of Spacecraft (Space Activities Act) in November 2016, and the Remote Sensing Data Act and part of the Space Activities Act went into effect in November 2017. The Space Activities Act fully went into effect in November 2018.

The Space Activities Act stipulates matters necessary to secure public safety and provide prompt protection of the victims from damages in Japan's space development and use, such as a launch permit system, obligation for reparation, and government compensation. In addition, the Remote Sensing Data Act established (1) a license pertaining to use of satellite remote sensing instruments, (2) a certification of persons handling satellite remote sensing data and (3) a system that enables the Prime Minister to issue an order to a satellite remote sensing data holder to prohibit provision of data under certain occasions.

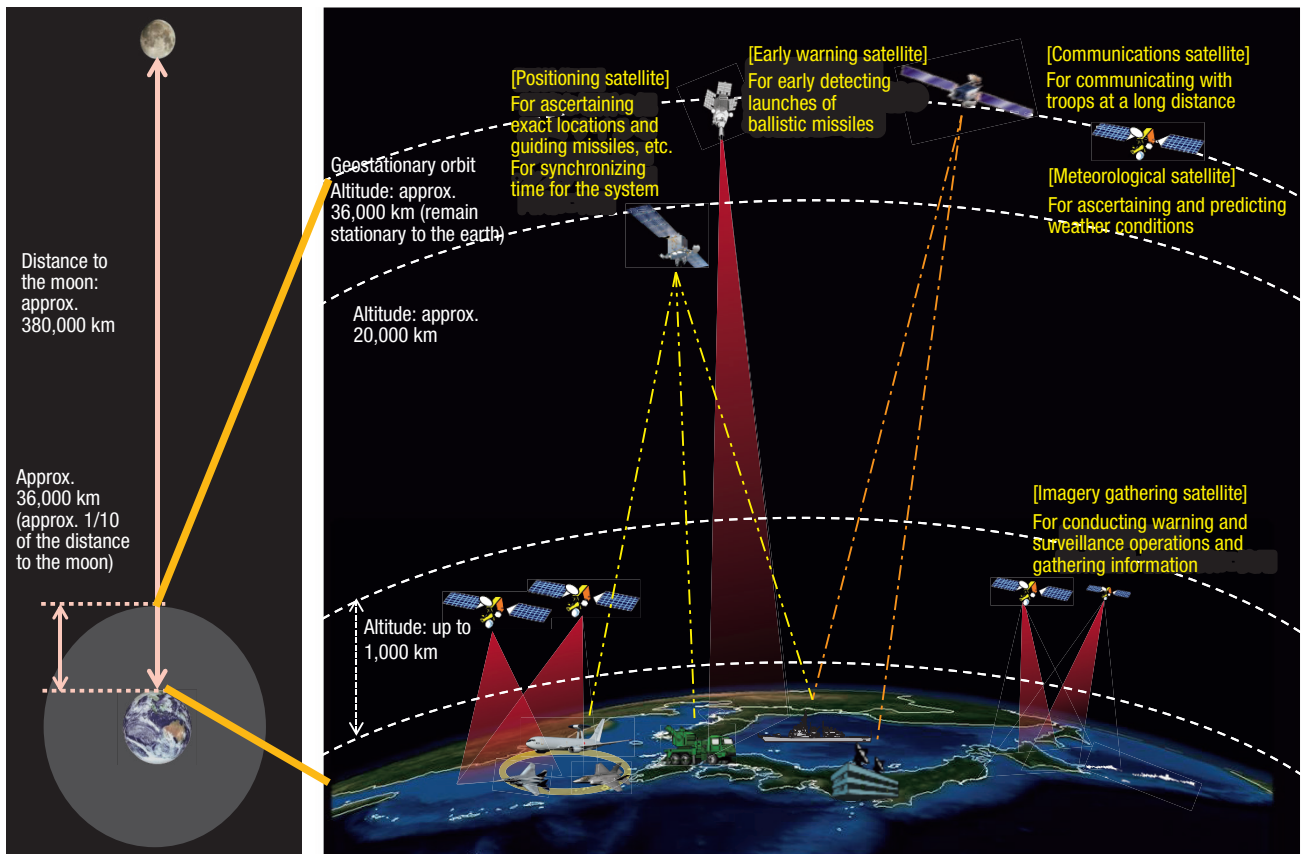
2 Initiatives of the MOD/SDF

Effective use of satellites for such purposes as information-gathering, communication and positioning is essential for realizing cross-domain operations. On the other hand, threats to the stable use of space are increasing.

The MOD/SDF has sought to ensure effective and efficient use of space by strengthening information gathering, C2 (command & control) and communication capabilities by using satellites and through Space Situational Awareness (SSA). In addition to these initiatives, based on the Mid-Term Defense Program (MTDP), the MOD/SDF will work

¹ In April 2016, the Office of National Space Policy was reorganized into the National Space Policy Secretariat.

Fig. III-1-3-1 Conceptual Image of Utilization of Space in the Security Field



to enhance capabilities to ensure superiority in the use of space at all stages from peacetime to armed contingencies. The efforts include (1) establishing an SSA system in order to secure the stable use of space; (2) improving various capabilities that leverage space domain including information-gathering, communication and positioning capabilities, and; (3) building the capability to disrupt C4I (command, control, communication, computer, and intelligence) of opponents in collaboration with the electromagnetic domain.

In so doing, the SDF will (4) work to enhance cooperation with relevant agencies, including the Japan Aerospace Exploration Agency (JAXA), and with the United States and other relevant countries. The SDF will also engage in such organization building as the creation of units specializing in space and a dedicated career field, and develop human resources and accumulate knowledge and expertise in the space domain. In FY2020, a space domain planning section (tentative name) responsible for planning pertaining to joint operation in the space domain will be established in the Joint Staff.

Q See Fig. III-1-3-1 (Conceptual Image of Utilization of Space in the Security Field)

(1) Development of the SSA System

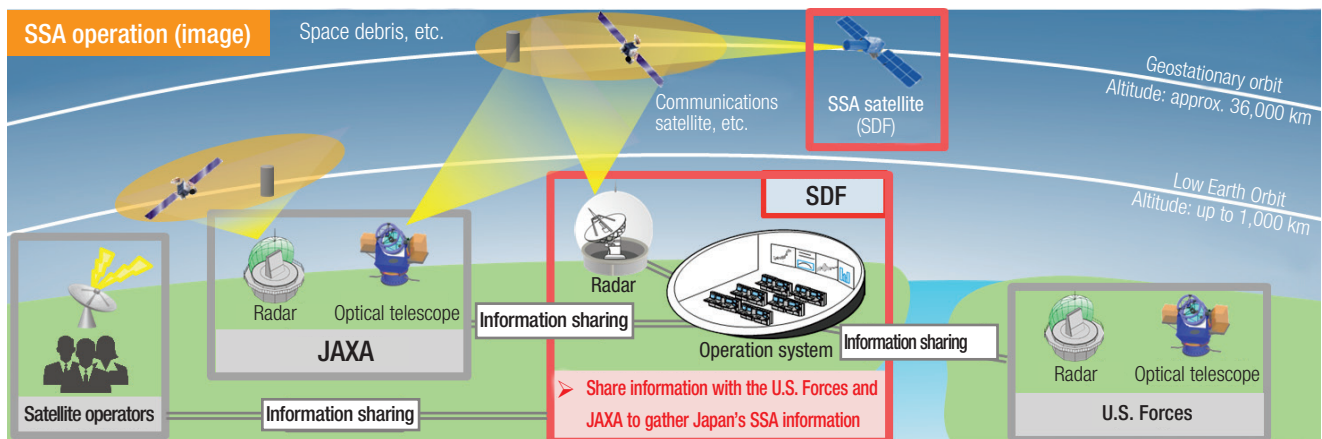
When using outer space, it is necessary to ensure its stable use. However, there has been a rapid increase in the volume

of space debris in outer space, raising the risk of significant damage to satellite functions caused by collision between debris and satellite.

In addition, it is pointed out that the development and verification test of a killer satellite, which approaches a target satellite to disturb, attack, and capture it, is underway, increasing the threat to the stable use of outer space.

That is why the MOD, based on the Basic Plan on Space Policy and through cooperation with relevant domestic institutions, such as the JAXA, and the United States, aims to establish SSA system by FY2022 to monitor and maintain an accurate picture of conditions in space. It is also working to deploy radar to monitor threats to Japanese satellites, such as space debris, and its operating system for information gathering, processing and sharing. In addition, the ASDF established the Space Operations Squadron in May 2020 as the unit specialized in the space domain to operate the system. In preparation for full-scale SSA operation and introduction of defense equipment, the ASDF is pursuing (1) study of unit operations pertaining to the space domain, (2) development of human resources with knowledge of the space domain, and (3) establishment of a network of cooperation with JAXA, the United States and others.

For this to happen, the government agencies and ministries concerned need to work together to build an effective operating system. On this point, JAXA is devising a plan to

Fig. III-1-3-2 Initiatives for Developing the SSA System

deploy radar able to monitor low Earth orbit (at altitudes of up to 1,000 km) and a ground-based optical telescope to monitor geostationary orbit (at altitudes of around 36,000 km). Combined with the radar of the MOD that will principally be dedicated to geostationary orbit monitoring, Japan is planning an effective SSA program. For its operation system, necessary adjustment is in progress to link the system to the U.S. Forces' system in addition to JAXA by FY2022.

For the future, in addition to radar to monitor threats to Japanese satellites such as space debris as mentioned above, the MOD will introduce SSA satellites that are space-based optical telescopes and ground-based SSA laser ranging devices to measure distance from low earth-orbit satellites. The expenses necessary for acquisition of SSA satellite components are included in the FY2020 budget.

Q See Fig. III-1-3-2 (Initiatives for the Development of the SSA System)

(2) Improving Various Capabilities to Leverage Space Domain Including Information-Gathering, Communication and Positioning Capabilities

The MOD/SDF has conducted information-gathering, communication and positioning using satellites, but in order to fulfill its missions effectively and efficiently, it is necessary to further enhance these capabilities.

For this purpose, the MOD/SDF will strengthen its intelligence and surveillance capabilities through multi-layered acquisition of satellite images using Information Gathering Satellites (IGS) and commercial satellites, including microsats. It will also continue to use images from the satellite operated by JAXA (ALOS-2) and information from Automatic Identification System (AIS), etc., and conduct research on dual wavelength infrared sensors.²

Regarding communications, the MOD/SDF launched X-band defense communications satellites called Kirameki-2 in January 2017 and Kirameki-1 in April 2018, owned and operated by the MOD for the first time, to be used for the communications, which is essential for command and control in unit operations. Going forward, in light of the future increase in communication requirements, the MOD will conduct steady development of Kirameki-3 to realize integrated communications as well as high-speed and large capacity communications, thereby aiming for the early realization of a three-satellite constellation with all of the three X-band defense communications satellites. The ministry will also conduct research and surveys on the next defense communication satellites.

With regard to positioning, the MOD/SDF has mounted GPS receiving terminals on a large number of equipment and used them as important means to support troop movement,



Commander of the Space Operations Squadron granted the unit flag by Minister of Defense Kono (May 2020)

² Research is underway to mount dual wavelength infrared sensors with excellent detection and identification performance on the Advanced Optical Satellite planned at JAXA and activate them in the space environment.

VOICE

Activities of Personnel Dispatched to JAXA

Tsukuba Space Center,
Space Tracking and Communications Center,
Japan Aerospace Exploration Agency (JAXA)
Major SAITO Takuya,
Defense Plans/Policies and Program Division,
Defense Planning and Policy Department, Air Staff Office

“Evolution into the Air and Space Self-Defense Force is no longer a pipe dream.” This is a statement made by Prime Minister ABE at the MOD Ichigaya in September 2019.

I am working as a member of ASDF personnel at JAXA Tsukuba Space Center. However, unlike the Astronaut YUI, former member of ASDF and my great senior, I am not aspiring to become an astronaut.

Unwanted artificial objects orbiting around the earth are called space debris. It is said that there are almost 20,000 of space debris that are larger than a softball. In order to prevent crashing of space debris with positioning, communication, broadcasting, weather and other satellites that are closely related to our daily lives, we need the ability to know what is happening in space right now (Space Situational Awareness (SSA)).

Currently, the MOD is working to gain and strengthen abilities in new domains, including outer space. For this purpose, the ASDF is preparing to establish an SSA operation system in cooperation with JAXA. In order to establish the



The author (second from right) receiving education on SSA systems at a meeting with JAXA personnel.

operation system, I am involved in coordination pertaining to data-sharing by the MOD and JAXA and specific cooperation procedures, while at the same time gaining specialized knowledge concerning SSA at JAXA.

Because the ASDF established a new job specialty in the space domain, the development and securing of human resources specialized in space will become essential. If you are inspired by this article, would you like to evolve into space people with me? “We are aerospace people!”

including highly accurate self-positioning and improvement of missile guidance. In addition to these efforts, the Quasi-Zenith Satellite System (QZSS)³ of the Cabinet Office started service in November 2018. With this in mind, the MOD/SDF will secure redundancy by using multiple positioning satellite signals, including QZSS.

(3) Enhancing Capabilities to Ensure Superiority in Use of Space

Utilization of satellites plays a vital role as the basic infrastructure for security, while some countries appear to be developing anti-satellite weapons, including killer satellites and anti-satellite missiles. In this context, the MOD/SDF needs to improve the resilience of the X-band defense communications satellite and other satellites.

To this purpose, the SDF will newly introduce training devices to study and train responses to the vulnerabilities

of Japanese satellites, and devices to grasp the state of electromagnetic interference against Japanese satellites. Expenses necessary for acquisition of devices to grasp the state of electromagnetic interference are included in the FY2020 budget.

The SDF will build the capability to disrupt C4I of opponents in coordination with the electromagnetic domain capabilities.

(4) Enhancing Cooperation with Relevant Agencies and with the United States and Other Relevant Countries

For the MOD to promote space development and use effectively, it is essential to enhance cooperation with relevant agencies with advanced knowledge, including JAXA, and with the United States and other relevant countries.

Currently the MOD and JAXA are cooperating in the development of SSA described above and technical

³ This refers to satellites set into orbit so that the satellites are capable of staying nearly right above one specific area by tilting the orbit, while ordinary stationary satellites stay on the equator. Multiple satellites are usually launched since a single satellite cannot stay for 24 hours by itself. Users are able to receive signals from such satellites without being affected by obstacles, such as mountains and buildings, since the satellites pass nearly right above the users.

demonstration of dual wavelength infrared sensors. In addition, the ministry exchanges human resources, including the dispatch of ASDF personnel to the JAXA Tsukuba Space Center.

Also, from the perspective of further promoting cooperation in the space field between the defense authorities of Japan and the United States, the two countries established the “Japan-US Space Cooperation Working Group (SCWG)” in April 2015 and so far held six meetings. The SCWG continues to promote consideration in broader fields such as: (1) promotion of space policy-related consultation, (2) closer information sharing, (3) cooperation for training and securing space experts, and (4) implementation of tabletop exercises.

As part of such initiatives, the MOD has taken part in the Global Sentinel, an annual SSA multinational tabletop exercise hosted by the U.S. Strategic Command since 2016 with the purpose of acquiring knowledge related to the SSA operation as well as of strengthening cooperation with the



ASDF personnel participating in Global Sentinel 19 (September 2019)

United States and other partner countries. These efforts to enhance the SSA capabilities also contribute to enhancing deterrence against new threats in outer space. Japan engages in space security dialogues not only with the United States but also with France, the European Union (EU), and India.

Q See Chapter 3, Section 3-1 (Cooperation in the Use of Space Domain)

2 Response in Cyber Domain

1 The Whole-of-Government Approach and Other Initiatives

With regard to cybersecurity, the number of cases that were detected as suspicious communication to Japanese governmental organizations and required confirmation as to whether or not they need coping, there were 111 suspicious malware infections and 66 targeted attacks in FY2018. This is a situation which requires sufficient and continuous attention.⁴

In order to deal with the increasing threat to cybersecurity, in November 2014, the Cybersecurity Basic Act was enacted. The Act aims to contribute to the security of Japan by comprehensively and effectively promoting the measures regarding cybersecurity.

In response to this, in January 2015, the Cybersecurity Strategic Headquarters was established in the Cabinet, and the National center of Incident readiness and Strategy for Cybersecurity (NISC)⁵ was established in the Cabinet Secretariat. The NISC is responsible for planning and promotion of cybersecurity-related policies and serves as the control tower in taking measures and responding to significant cybersecurity incidents in government organizations and agencies, as well as critical infrastructures. Furthermore, in

September 2015, the Cybersecurity Strategy was formulated for the comprehensive and effective promotion of measures pertaining to cybersecurity, with the aims to create and develop free, fair and safe cyber space to enhance the vitality of the economy and society and realize their sustainable development, to realize a society in which citizens can live safely and with peace of mind, and to contribute to the peace and stability of the international community as well as the security of Japan. Furthermore, in July 2018 the strategy was reviewed to promote cybersecurity for sustainable development and initiatives from three perspectives ((1) mission assurance by service providers, (2) risk management, and (3) participation, cooperation and collaboration), while sticking with the basic position of the strategy.

2 Initiatives of the MOD/SDF

Information and communications networks that leverage cyberspace form a foundation for the SDF’s activities in various domains, and any attack against them would seriously disrupt the organized activities of the SDF.

The MOD/SDF has engaged in holistic measures including the following: introduction of intrusion prevention systems, in

⁴ Cybersecurity 2019 (approved by the Cybersecurity Strategic Headquarters on May 23, 2019)

⁵ With the enactment of the Basic Act on Cybersecurity in January 2015, the National Information Security Center (NISC) was reorganized as the National center of Incident readiness and Strategy for Cybersecurity (NISC). The NISC is responsible for the planning and promotion of cybersecurity-related policies and serves as the control tower in taking measures and responding to significant cybersecurity incidents in government organizations and agencies, as well as critical infrastructures.

order to ensure the safety of information and communication systems; development of defense systems, such as the security and analysis devices for cyber defense; monitoring of MOD/SDF communications networks around the clock and response to cyber attacks⁶ by the SDF C4 (Command, Control, Communication & Computers) Systems Command and others; enactment of regulations⁷ stipulating postures and procedures for responding to cyber attacks; research on cutting-edge technology; development of human resources, and collaboration with other organizations.

In addition to these initiatives, based on the NDPG, the SDF will fundamentally strengthen its cyber defense capability, including the capability to disrupt, during an attack against Japan in time of emergency, the opponent's use of cyberspace for the attack. Specifically, the MTDP stipulates (1) establishment of the necessary environment for ensuring cybersecurity, (2) keeping abreast of the latest information including cyber-related risks, counter measures and technological trends, (3) development and securing of human resources, and (4) contribution to the whole-of-

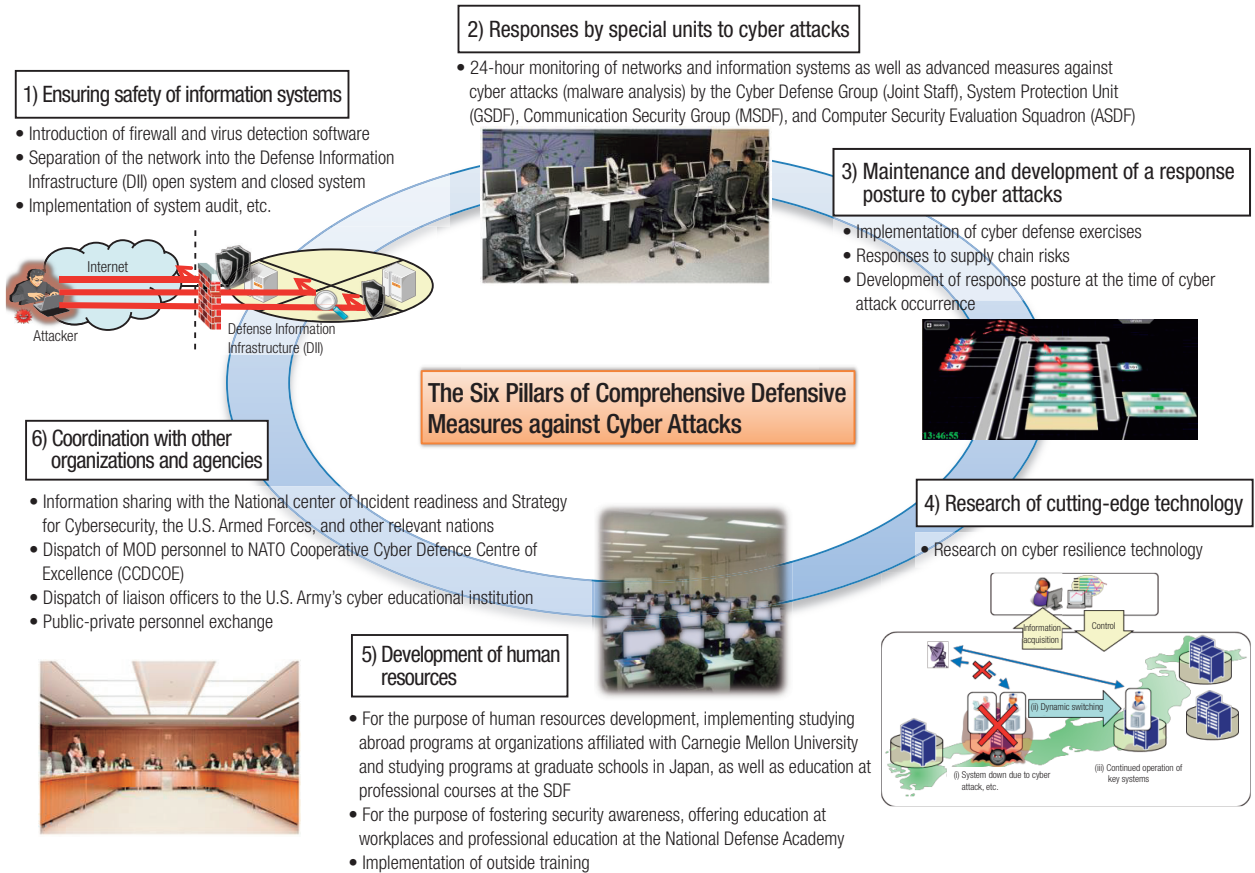
government initiatives.

Q See Fig. III-1-3-3 (MOD/SDF Comprehensive Measures to Deal with Cyber Attacks); Reference 13 (Efforts in Recent Years by the MOD on Cybersecurity)



Member of Cyber Defense Group responding to increasingly sophisticated, skillful cyber attacks

Fig. III-1-3-3 MOD/SDF Comprehensive Measures to Deal with Cyber Attacks



6 Illegal intrusion, information theft, alteration or destruction, operation stop/malfunction of information system, execution of unauthorized program, DDoS (distributed denial of service) attacks, etc. which are made through cyberspace by abusing information communication networks, information systems, etc.
 7 There are directives relating to the information assurance of the MOD (MOD Directive No. 160 of 2007).

(1) Establishing an Environment for Ensuring Cyber Security

a. Expanding the System of Cyber Defense Group and Other Units

The Cyber Defense Group was established under the SDF C4 Systems Command in March 2014. In order to appropriately deal with cyber attacks that are becoming more sophisticated and skillful day by day, the Cyber Defense Group has strengthened the system. The group will be further expanded by about 70 personnel to approximately 290 in FY2020.

b. Strengthening Capabilities of Information Gathering, Research and Analysis

In order to secure functions of the system and network of the MOD/SDF under any circumstance, it is necessary to strengthen the capabilities of information gathering, research and analysis, and develop a practical training environment.

To this end, the MOD/SDF will continue initiatives such as (1) upgrade of information gathering devices for indications and techniques of cyber attacks, (2) enhancing functions of analysis devices for cyber protection taking advantage of AI and other advanced technologies, and (3) development of an environment for cyber exercises carried out as competition between an attacking team and a defense team.

(2) Keeping Abreast of the Latest Information Including Risks, Counter Measures and Technological Trends

In order to respond to cyber attacks in a swift and appropriate manner, it is necessary to keep abreast of the latest information, including cyber-related risks, counter measures and technological trends, through cooperation with the private sector, and strategic talks, joint exercises and other opportunities with allies and other parties. For this purpose the MOD/SDF will effectively cooperate with private companies and foreign countries, including the United States, which is Japan's ally.

a. Cooperation with Private Companies and Others

In Japan, in July 2013, the Cyber Defense Council (CDC) was set up, and its core members consist of around ten companies in the defense industry with a strong interest in cybersecurity. The MOD/SDF and the defense industry have made efforts to deal with cyber attacks through joint exercise and other initiatives. The MOD/SDF will further expand the cooperation.

b. Cooperation with the United States

Since comprehensive defense cooperation, including joint response, between Japan and its ally the United States is vital, the two countries set up the Cyber Defense Policy

Working Group (CDPWG) as a framework between the defense authorities of Japan and the United States. Under this framework, meetings have been held seven times to discuss the following topics: (1) promotion of policy discussions regarding cyber issues, (2) closer sharing of information, (3) promotion of joint exercises incorporating response to cyber attacks, and (4) matters such as cooperation for training and retaining experts. Moreover, in May 2015, the two countries announced a joint statement on the specific future direction of the cooperation.

In addition, Japan's cooperation with the United States is to be further strengthened by such means as participation in the Japan-U.S. Cyber Dialogue, a whole-of-government approach by both nations, holding of the Japan-U.S. IT Forum, a framework between the defense authorities since 2002, and dispatching liaison officers to the U.S. Army's cyber educational institution.

c. Cooperation with Other Countries etc.

Japan has held cyber dialogues with the respective defense authorities of the United Kingdom, the North Atlantic Treaty Organization (NATO), and others. Furthermore, Japan has participated in cyber defense exercises organized by NATO or the Cooperative Cyber Defence Centre of Excellence (CCDCOE). In December 2019 the MOD for the first time officially participated in "Cyber Coalition 2019," a cyber defense exercise organized by NATO, to enhance cooperation with NATO. In addition, the IT Forum has been held between the defense authorities of Singapore, Vietnam, and other countries to exchange views on initiatives in the information communications area including cybersecurity and current trends in technology.

 Chapter 3, Section 3-2 (Cooperation in the Use of Cyber Domain)

(3) Development and Securing of Human Resources

In order to strengthen the cyber defense capability of the SDF, it is necessary to secure human resources who have advanced and broad-ranging knowledge on cybersecurity. To this end, a common cyber course⁸ to learn common and sophisticated knowledge on cyber security has been provided since FY2019. The FY2020 budget includes expenses for sending SDF personnel to universities and educational institutions, both international and domestic, including the National War College of the United States, which provides a course for cyber warfare commanders. It also includes expenses necessary for holding a cyber competition to identify highly skilled cyber talents in the private sector. The MOD/SDF will also work to ensure appropriate treatment for security and IT human resources who work as a bridge

⁸ Common cyber security education provided for graduates of an IT-related program that is provided by each SDF service

between highly professional human resources and general administration departments in the MOD⁹ and consider the utilization of external human resources through a public-private personnel exchange system to employ people with practical experience in private companies as well as contracts for service, for example.

(4) Contribution to the Whole-of-Government Approach

Along with the National Police Agency, the Ministry of Internal Affairs and Communications, the Ministry of Economy,

Trade and Industry, and the Ministry of Foreign Affairs, the MOD, as one of the five government agencies that are members of Cybersecurity Strategy Headquarters, participates in cyber attack response training and personnel exchanges, and provides information about cyber attacks, etc. to the cross-sector initiatives led by the NISC as well as sending personnel to the CYber incident Mobile Assistant Team (CYMAT).

The MOD is considering applying the knowledge and experience of the SDF to penetration tests of the IT systems of government ministries and agencies conducted by NISC.


3 Response in Electromagnetic Domain

Electromagnetic spectrum¹⁰ has been used for command/communication, and warning/surveillance. With the development of the technology, its use has expanded in range and purpose, and it is now recognized as a major operational domain situated on the frontline of the offense-defense dynamic in today's warfare.¹¹ In response, the MOD/SDF, based on the NDPG, etc., will (1) enhance its ability to appropriately manage and coordinate the use of electromagnetic spectrum, (2) strengthen information collection and analysis capabilities related to electromagnetic spectrum, and develop an information sharing posture, (3) strengthen capabilities to neutralize the radar and communications of opponents who intend to invade Japan, and thereby acquire and enhance capabilities to ensure superiority in the electromagnetic domain.¹²

1 Enhancing the Ability to Appropriately Manage and Coordinate the Use of Electromagnetic Spectrum

In order to gain an advantage in warfare by using electromagnetic spectrum proactively and effectively, it is necessary to build capabilities to manage electromagnetic spectrum by centrally grasping and coordinating wave frequencies and status of use, and appropriately allocating frequency resources to units, etc. in addition to electronic warfare capabilities to ensure the use and effect of electromagnetic spectrum while interfering with the use and effect by an enemy.

For this purpose, the FY2020 budget includes expenses for capacity building in electromagnetic management, which includes the start of research on electromagnetic management supporting technologies that help with grasping and visualizing electromagnetic utilization status in order to effectively conduct electronic warfare, etc.

 See Fig. III-1-3-4 (Electronic Warfare Capabilities and Electromagnetic Spectrum Management Capabilities [concept])

2 Strengthening Information Collection and Analysis Capabilities Related to Electromagnetic Spectrum, and Building an Information Sharing Posture

In order to gain an advantage in electromagnetic warfare, it is important to gather and analyze information on electromagnetic spectrum at all phases from peacetime to armed contingencies and appropriately share the information among SDF units.

To this end, the MOD/SDF plans to enhance information gathering and analysis capabilities through: establishment of electromagnetic operation units to gather information regarding electromagnetic spectrum as subordinate units of the Ground Component Command; and, under the FY2020 budget, implementation of research for improving the capabilities of electromagnetic information gathering units for combatant vessels. In order to share the information among SDF services while ensuring security of the information, the SDF will continue to promote the upgrade of the JADGE system, the connection of each SDF service's systems, including the Defense Information Infrastructure

⁹ Measures based on the Comprehensive Policy for Enhancing the Development of Security and IT Human Resources at Governmental Organizations (Approved by the Cybersecurity Strategic Headquarters on March 31, 2016)

¹⁰ Collective term for radio waves, infrared rays, visible rays, etc. Concerning radio waves used in Japan, the Ministry of Internal Affairs and Communications has centralized control over radio wave frequencies, and the MOD/SDF obtains approval for radio wave frequencies from the Ministry when using them in training and other initiatives.

¹¹ One of the attacks using electromagnetic waves is electromagnetic pulse (EMP) attacks, which place an extreme burden on electronics by generating instantaneous powerful electromagnetic waves through nuclear explosions and other means leading to their malfunctioning or destruction. This type of attack would impact not just the defense field but Japanese people's lives in general. The Government of Japan as a whole will deliberate on necessary countermeasures.

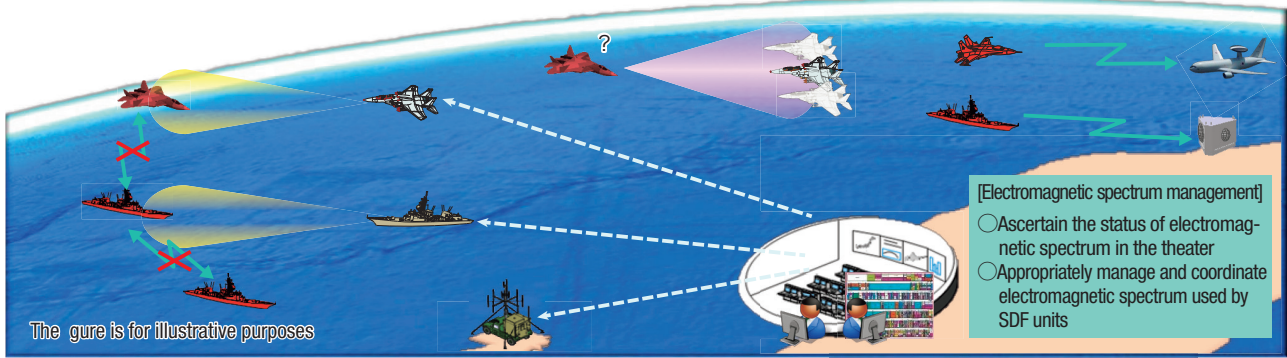
¹² In addition, the MOD/SDF is advancing the multiplication of the communications network required for information sharing among the services, and conducting research in light of the viewpoint of EMP protection.

Fig. III-1-3-4 Electronic Warfare Capabilities and Electromagnetic Spectrum Management Capabilities (image)

Electronic warfare capabilities: Warfare (electronic warfare*) capabilities to effectively and proactively utilize electromagnetic spectrum to ensure the use and effect of electromagnetic spectrum while interfering with the use and effect by an enemy
 Electromagnetic spectrum management capabilities: Capabilities to appropriately manage and coordinate the use of electromagnetic spectrum among SDF units by ascertaining the status of electromagnetic spectrum in the theater and preventing interference with the aim of securing electronic warfare capabilities

* In general, the warfare is divided into three categories – electronic attack, electronic protection, and electronic warfare support.

- [Electronic attack]**
 - Emit electronic waves to communication devices and radars of an enemy, thereby reducing or disabling their communication
- [Electronic protection]**
 - Reduce or nullify the impact of electromagnetic spectrum used by an enemy by using stealth technology
- [Electronic warfare support]**
 - Collect and analyze such information as electromagnetic spectrum used by an enemy



(DII)¹³ and the improvement of each SDF service’s data links.

3 Strengthening Capabilities to Neutralize Radar and Communications of an Opponent who Intends to Invade Japan

Neutralizing use of electromagnetic spectrum, including radar and communications of an opponent who intends to invade Japan based on information gathering and analysis in peacetime is effective as a means for the defense of Japan so that even when inferiority exists in individual domains such inferiority will be overcome and national defense accomplished.

For this purpose, in FY2020, the SDF will proceed with capability development through the procurement of fighters (F-35A/B) superior in electronic countermeasures for self-protection and network electronic warfare devices, capability enhancement like installation of new electronic warfare equipment on fighters (F-15), as well as development of standoff electronic warfare aircraft for jamming from outside of the threat envelopes of the opponent, and research on

surface-to-air electronic war devices. Furthermore, the SDF will also swiftly proceed with studies and R&D aimed at the procurement of potentially game-changing technologies, such as high-power microwave devices that can instantaneously disable a large number of drones, etc., a high-energy laser system (HEL) that responds to such threats as drones and mortar shells at a low cost and with a short reaction time.

4 Training /Exercise and Human Resource Development

In order to strengthen the SDF’s capability in the electromagnetic domain, it is also important to enhance training/exercise and education.

In the FY2020 budget, in addition to usual training/exercise and education, the SDF will start to install the latest electronic warfare education devices used by the ASDF. Furthermore, ASDF personnel is planned to be joining to the electronic warfare education course in the United States again this year.

¹³ This refers to a common network across all SDF as an information communication infrastructure necessary for the SDF to perform its duties, in which the SDF makes use of a variety of communication lines: self-employed micro lines that the MOD owns as well as external lines and satellite lines that it leases from communication carriers, thereby composing data communication networks and sound communication networks.