## **New Domains**

Nowadays, various kinds of satellites have been launched for observation, communication/broadcasting and positioning, making outer space key infrastructure for both the public and private sectors in such areas as society, economics and science. Also in the security area, major countries have been making proactive efforts to use outer space for maintaining peace and safety.

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.

Owing to the advancement of information and communications technology in recent years, information and communications networks such as the Internet have become essential components across all facets of life. Therefore, cyber attacks against information and communications networks have the potential to seriously impact the lives of individuals. Under such circumstances, cyber attacks have frequently been carried out against information and communications networks of not only government organizations and military forces but also business corporations and academic organizations in various countries. Attacks attempting to steal critical technologies, secrets or personal information have been confirmed. For 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.

In everyday life, electromagnetic spectrum is used for various purposes ranging from television and mobile communications to geolocation information through global positioning systems. In the security area, electromagnetic spectrum 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 the frontline of the offense-defense dynamic in today's warfare. Therefore, ensuring superiority in electromagnetic domains such as these is essential for realizing cross-domain operations.



Special Feature

## **Cross-Domain Operations**

Contemporary warfare combines the traditional domains of land, sea, and air with new domains such as space, cyberspace, and electromagnetic spectrum. In such situation, it is essential to block and eliminate attacks by leveraging capabilities in such new domains as space, cyberspace, and electromagnetic spectrum so as to effectively deter and counter threats. Cross-domain operations that organically fuse capabilities in the new domains and the traditional domains of land, sea, and air to exercise domain-crossing capabilities have thus become vitally important.



Cross-Domain Operation (image of domain-crossing exercise of capabilities)

Overcome ability differences with other countries by taking advantage of a synergy effect obtained through organically integrating abilities in multiple domains, not by exercising abilities separately in each domain

\*1 C4ISR: Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance

\*2 The networks of the MOD/SDF consist of Riku-Shiki, (GSDF command system), Maritime Self Defense Force Command, Control, and Communication Service Foundation System (MARS), Japan Aerospace Defense Ground Environment (JADGE) and other systems.