Section 4 Electromagnetic Domain Trends

1 Electromagnetic Domain and Security

Electromagnetic spectrum represents the spectrum that are propagated by the oscillations of electric and magnetic fields. In everyday life, they are used for various purposes ranging from television and mobile communications to positioning information through global positioning systems.

In the defense field, electromagnetic spectrum is used for command and control communications equipment, radar systems for detecting enemies, missile guidance systems, and other equipment. Securing superiority in the electromagnetic domain is indispensable for modern operations.

See Figure 1-3-4-1 (How to Use the Electromagnetic Domain in the Defense Field)

Therefore, major countries have recognized electronic attacks for interrupting adversaries' use of electromagnetic spectrum as an asymmetric means similar to cyber attacks to effectively hamper adversaries' military performance, giving priority to and enhancing electronic warfare capabilities, including electronic attacks.

2 Each Country's Electronic Warfare Initiatives

1 The United States and Europe

The United States has committed to expanding electronic warfare training and equipment, and to enhancing cooperation with its allies under an initiative to aggressively achieve its dominance in the electromagnetic domain. Major U.S. electronic warfare units include the Navy's 13 electronic attack squadrons armed with EA-18G electronic warfare aircraft as well as Marine and Air Force flight squadrons with electronic warfare aircraft. The Army plans to deploy electronic warfare units in the future.

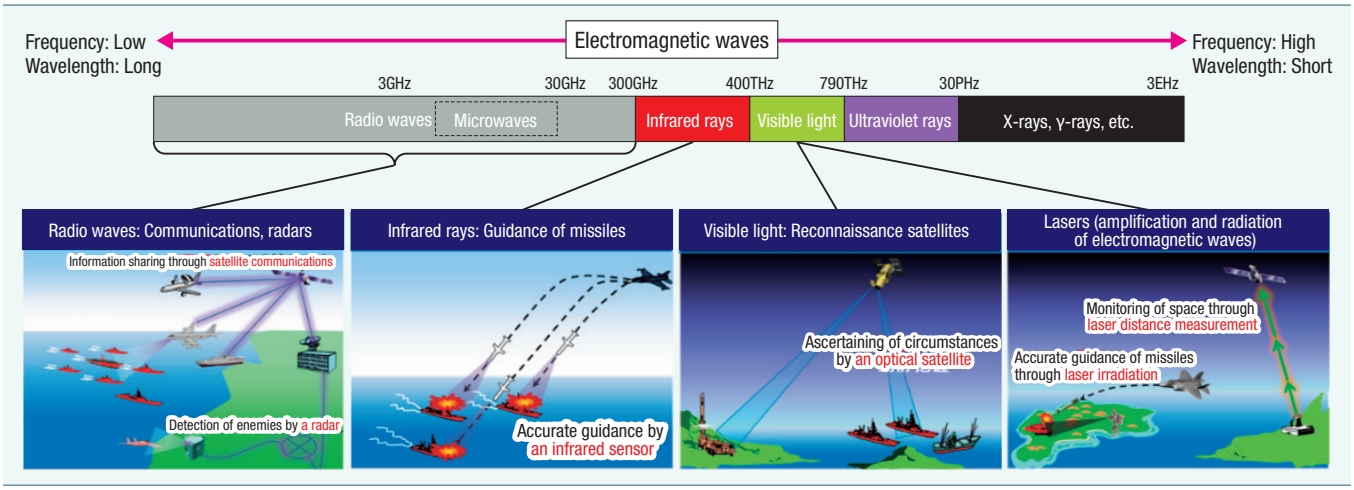
The U.S. Forces used EA-18G aircraft for military operations in Libya in 2011 to jam the Libyan government forces' ground radar and prevent Libyan attacks on NATO aircraft.

Many other NATO member countries are also developing equipment for severe electronic warfare environments and allegedly conducting electronic warfare-oriented exercises with Russian forces' electronic warfare equipment in mind.[1]

2 China

China has set an initiative to put cyber warfare and other electronic elements, and physical destruction and other non-electronic elements under unified control.[2] Under the initiative, China has conducted exercises to effectively accomplish missions in complicated electromagnetic

Fig. I-3-4-1 How to Use the Electromagnetic Domain in the Defense Field



1 According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defense Review, April 2018
2 According to "The Military Balance 2019" by the U.K. International Institute for Strategic Studies

EA-18G Growler【Jane's by IHS Markit】

Krasukha-4【Jane's by IHS Markit】

environments, improving practical capabilities. The new Strategic Support Force, created for improving overall military operational capabilities, may be responsible for such domains as electronic warfare, cyber and space.

It is reported that PLA electronic warfare units routinely conduct jamming operations against communication and radar systems and GPS satellite systems in exercises.[3] China's TU-154 electronic intelligence and Y-8 electronic warfare aircraft have been seen flying around the Nansei Islands and the Sea of Japan in the vicinity of Japan. It is also reported that China has mounted electronic warfare pods for jamming missions on J-15 fighters, H-6 bombers, and other aircraft, and deployed a jamming system on Mischief Reef of the Spratly Islands.[4]

3 Russia

Russia, in its federal Military Doctrine, positions electronic warfare equipment as important equipment in modern military conflict. It is pointed out that Russian forces have positioned electronic warfare as part of offensive means and improved practical electronic warfare capabilities in recent years.[5]

Russia's electronic warfare force reportedly has five brigades led mainly by the Army.[6] It is reported that Russia used various electronic warfare systems in eastern Ukraine to block Ukrainian forces' command and control traffic and jam GPS waves to interrupt their drone operations, affecting Ukraine's military performance.[7] It is also reported that Russia used Krasukha-4 and other electronic warfare systems in Syria to interrupt NATO forces' command and control traffic and radar systems.[8] In the vicinity of Japan, Russian electronic reconnaissance aircraft's long-range flights over the Sea of Japan have been seen.

3 According to "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018" by the U.S. DoD
4 According to "An Accounting of China's Deployments to the Spratly Islands" by the U.K. International Institute for Strategic Studies in May 2018
5 According to "Russia's Electronic Warfare Capabilities to 2025" by the Estonian Ministry of Defense
6 According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defense Review, April 2018
7 "Russia's Electronic Warfare Capabilities to 2025" by the Estonian Ministry of Defense cites 10 electronic warfare systems as used by Russia in Ukraine, including the RB-341V Leer-3.
8 According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defense Review, April 2018

column Electronic Warfare

Electronic warfare generally represents battles in which radio and other electromagnetic waves are used. In general, the warfare is divided into three categories – electronic attack, electronic protection, and electronic warfare support.

An electronic attack emits more powerful or deceptive radio waves toward adversaries' communications and radar systems to jam radio waves from these systems so as to reduce or neutralize adversaries' communications and search capabilities. It includes not only such jamming but also physical target destruction using high-power electromagnetic waves (including high-power laser beams and high-power microwaves) such as the U.S. laser weapon system and the Russian Peresvet.

See Part I, Chapter 3, Section 1-1-2 (4) (High-Power Laser Weapons)

Electronic protection includes making defense equipment too stealthy to be detected and reducing or neutralizing adversaries' electronic attacks by changing electromagnetic wave frequencies or enhancing electromagnetic wave power in response to an electronic attack on communications and radar systems. For example, Sweden's Giraffe 8A air surveillance radar is said to be able to automatically select the most invulnerable frequencies in response to jamming and maintain its air surveillance radar function.

Electronic warfare support means collecting adversaries' electromagnetic wave data. To implement effective electronic attack or protection, it is required to recognize and analyze electromagnetic waves used by adversaries' communications, radar systems and electronic attack aircraft and how these waves are used under normal circumstances.

In electronic warfare, it is desirable to implement effective electronic protection even without adversaries' jamming waves recognized or analyzed in advance. In this respect, using artificial intelligence technology for defense equipment is under consideration to immediately analyze jamming waves and automatically select frequencies that are the most invulnerable to jamming.

Laser weapon system

【Jane's by IHS Markit】

<Description>
Capable of using high-power laser beams to destroy small unmanned aircraft, etc.

Giraffe 8A

【Jane's by IHS Markit】

<Description>
The Giraffe 8A of Sweden's Saab AB can automatically select frequencies that are the most invulnerable to jamming.