Section 4

Trends in Electromagnetic Domain

0

Electromagnetic Domain and Security -

The electromagnetic spectrum is propagated by the oscillations of electric and magnetic fields. In everyday life, it is used for various purposes ranging from television and mobile communications to geolocation information through global positioning systems.

In the defense field, the 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. Activities using the electromagnetic domain include electronic warfare and electromagnetic spectrum control. Electronic warfare means or approaches are generally classified into three – electronic attack, electronic protection and electronic warfare support.

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

"Electronic attacks" are designed to reduce or neutralize adversary communications and search capabilities by sending stronger radio waves or radio waves pretending to be adversary waves aimed at an adversary's communications and radar equipment to jam waves coming from such equipment. They include radio wave jamming, radio wave deception and physical destruction using high-power electronic waves (such as high-power laser and high-power microwaves).

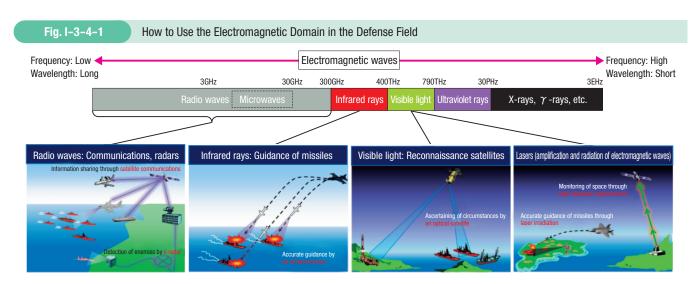
See Section 1-1 (3) of this Chapter (High-power Energy Technology)

"Electronic protection" makes equipment stealthy

or difficult to be detected by adversaries and reduces or neutralizes adversary electronic attacks on communications and radar equipment by changing electronic wave frequency for use or increasing its power.

"Electronic warfare support" consists of activities designed to collect information on adversary electromagnetic spectrum for electronic warfare purposes. It is necessary for effective electronic attacks or protection to detect and analyze what electromagnetic spectrum is usually used by adversaries for communications equipment, radar and electronic attack aircraft. It is desirable to be able to conduct electronic warfare effectively even if electromagnetic spectrum used by adversaries is not detected or analyzed in advance. For example, AI may be mounted on or used for equipment to immediately analyze jamming and automatically select frequency bands that are the most invulnerable to jamming.

"Electromagnetic spectrum control" means the control and adjustment of electromagnetic spectrum use to facilitate electromagnetic domain activities such as electronic attacks and protection. Specific measures for the control include the detection of how electromagnetic spectrum is used in a theater of operation, as well as the adjustment of frequencies, directions and durations of electromagnetic spectrum used for friendly forces and equipment to avoid electromagnetic spectrum interference. At present, research is being conducted on technologies for detecting and visualizing how electromagnetic spectrum is used.



Chapter

3

Major countries apparently recognize electronic attacks as an asymmetric means similar to cyber attacks to effectively hamper adversaries' military performance, emphasizing

and enhancing electronic warfare capabilities, including electronic attacks.

Each Country's Electronic Warfare Initiatives

1 The United States and Europe

The United States is 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 Corps flight squadrons with electronic warfare aircraft. As an example of military operations using electronic warfare equipment, there is an assessment that U.S. electronic warfare units used EA-18G aircraft in Libya in 2011 to jam ground radar of the Libyan government forces, preventing their attacks on NATO aircraft. It is pointed out that the LMADIS (Light Marine Air Defense System) counter unmanned aircraft system with electronic warfare capabilities was used for leading an Iranian drone to crash over the Strait of Hormuz in July 2019.

The U.S. Air Force activated the 16th Air Force in October 2019 to integrate functions for ISR, cyber warfare, electronic warfare and information warfare. The Army plans to deploy multi-domain task forces integrating long-range precision



Counter unmanned aircraft system "LMADIS" [U.S. Marines]

attack, electronic warfare, cyber and other capabilities in the Indo-Pacific and other regions from FY2021.

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 conducts force-on-force exercises on a routine basis to effectively accomplish missions in complicated electromagnetic environments, improving practical capabilities. It is pointed out that China's armed forces have taken advantage of such exercises to assess electronic warfare weapon research and development achievements.3 The Strategic Support Force, established for improving overall military operational capabilities, may be responsible for such domains as electronic warfare, cyber and space.

China's TU-154 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 In a military parade to mark the 90th anniversary of the Chinese People's Liberation Army in July 2017, unmanned aircraft reported as mounted with electronic warfare equipment were displayed.

According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defence Review (April 2018)

According to "The Military Balance 2019," U.K. International Institute for Strategic Studies

According to "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019," U.S. DoD

According to "An Accounting of China's Deployments to the Spratly Islands," Center for Strategic and International Studies (May 2018)

3 Russia

Russia, in its Military Doctrine, positions electronic warfare equipment as important equipment in modern military conflict. It is noted that Russia used electronic warfare equipment in the "Vostok 2018" exercise in September 2018, the "Tsentr 2019" exercise in September 2019 and other exercises. It is also 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



Krasukha-4, electronic warfare system 【Russian Ministry of Defence】

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.

⁵ According to "Russia's Electronic Warfare Capabilities to 2025," Estonian Ministry of Defense

⁶ According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defence Review (April 2018)

⁷ According to "Russia's Electronic Warfare Capabilities to 2025," Estonian Ministry of Defense

⁸ According to "All quiet on the eastern front: EW in Russia's new-generation warfare," Jane's International Defence Review (April 2018)