WHITE PAPER

Electronic Warfare: Vying for Control of the Electromagnetic Spectrum

Advanced threats lead to open architecture approaches and new analysis of electronic countermeasures

KEYSIGHT

Over the past decade, preeminent countries involved in major military conflicts mainly focused on asymmetrical warfare — surprise attacks by small groups armed with modern, high-tech weaponry. During that same period, however, near-peer adversaries began attaining impressive electronic warfare (EW) capabilities. As a result, a plethora of new, dynamic threats flooded the EW spectrum, pushing threat detection and analysis to keep pace. Large military forces now face ongoing development and evolution to stay ahead of their adversaries, leading to a need for a more flexible, scalable approach to threat detection, analysis, and response.

Even the smallest military can now build powerful weapons systems, given the availability and low cost of advanced electronics with high computing power. The proliferation of technology also created a battlefield where weapons technology undergoes rapid, continuous change. Digital and programmable radio frequency equipment, such as software-defined radios, creates a more complex battlefield. In addition, radars can quickly change waveforms, making it challenging to locate, identify, and confuse hostile emitters.

These trends impact every aspect of EW, which uses the electromagnetic (EM) spectrum to sense, protect, communicate, and attack during warfare. Today, the ability to ensure spectrum-wide superiority during warfare is one of the biggest determinants of success or failure during a military operation.

Key points covered in this white paper:

- Electronic warfare is modern warfare
- The proliferation of new advanced threats
- Challenges of analyzing modern electronic countermeasures
- An open architecture to adequately model threats

Electronic Warfare Is Modern Warfare

Broadly defined, EW is the use or manipulation of the EM spectrum in warfare from air, land, sea, and space. It involves the use of EM energy, directed energy, or anti-radiation weapons for uses ranging from detection, denial, and deception to destruction and protection. EW uses radio and microwave frequencies for communications, radars, and satellites. Certain EW solutions also leverage infrared for intelligence and enemy targeting. Lasers use the spectrum to transmit data, communicate, and destroy a target.

EW includes any military action involving the use of EM and directed energy to control the electromagnetic spectrum or attack the enemy. EW comprises three main categories:

- Electronic protection involves protecting access to the EM spectrum for friendly military assets, including radio frequencies, radar frequencies, spread spectrum technology, GPS signals, and frequency coordination. Electronic protection also entails defeating electronic attacks that seek to disable the use of the EM spectrum. Examples include the use of flare rejection logic on an infrared (IR) missile, which allows a missile to function as intended despite the use of flares by an enemy to disrupt its navigation.
- EW support is broadly defined as surveillance and reconnaissance using EM energy. The data gathered can produce signal intelligence (SIGINT) to help with targeting for an electronic or physical attack. It also can produce measurement and signature intelligence.
- Electronic attack uses EM energy, direct energy, or anti-radiation weapons to confuse, disable, or destroy an enemy's electronic systems. Weapons used for electronic attack leverage lasers, electro-optical, infrared, and RF technologies.

The Proliferation of New Advanced Threats

Beyond their multifaceted forms and capabilities, EW threats boast high intelligence. With the increased use of adaptive programming, these systems continue to grow smarter. In response to observed effects on the battlefield, they will alter operation via radiated waveforms, techniques, or timing. Waveforms, in particular, change nearly instantaneously. Modern threats are more adaptable and reprogrammable, creating an urgent need to characterize them correctly.

The following are examples of modern warfare:

- self-propelled decoys
- jamming a radar using anti-radiation missiles to foil air defenses
- electronic deception techniques used to confuse an enemy's intelligence, surveillance, and reconnaissance (ISR) systems
- direct energy weapons with the potential to destroy people, materials, and equipment such as satellites, airborne optical sensors, and land-based forces

Modern threats and countermeasures flood the modern EM spectral environment with thousands of emitters, including radios, wireless devices, and radar transmissions. This, in conjunction with advanced digital signal processing (DSP), creates a dramatically complex electromagnetic spectrum. DSP led to advancements in digital dynamic range and algorithm complexity. This environment creates complex signal activity, leading to dynamic and evolving threats for EW systems. While many EW systems use technology advancements such as high-performance DSP and gallium nitride (GaN) amplifiers, the sheer number of possible scenarios from one threat creates difficult challenges.

Challenges of Analyzing Modern Electronic Countermeasures

As the pace of technological change for EW outpaces developmental life cycles, threats evolve more quickly than the time it takes to build countermeasures. With the near-constant evolution of threats and signals in EW, militaries are investing heavily in new technologies to gain a tactical advantage and keep up with evolving threats. Many militaries find themselves engaged in a head-to-head competition, where the countermeasures catch up only to discover that the threats moved yet another step ahead. The integration of machine learning (ML) and artificial intelligence (AI) into EW systems will help to sort through the vast array of signals and identify the correct ones on the fly.

Cognitive EW

Cognitive EW uses modern machine learning techniques to increase cognitive ability, including target recognition, intelligent decision-making, and autonomous learning. Complex and congested signal environments make it challenging to locate, identify, jam, and confuse enemy communications systems — especially if they are adaptive. For instance, adaptive radars make it challenging to isolate pulses from threatening radars, understand threats from hostile radars, and provide an adequate response.

Military technology is turning to machine learning to create cognitive EW weapons that can successfully operate in these environments. These weapons use software-defined capabilities to gain operational flexibility in congested (and contested) environments, quicker upgrades, and greater affordability.

Digital equipment can be programmed on the fly using software programs, allowing EW solutions like radars and software-defined radios to change waveforms and create unique signatures quickly. As more communications systems, radios, jammers, and IoT devices operate in the EM spectrum, spectrum awareness takes on increased importance. New EW systems look to understand the intent of each system using the spectrum, rather than relying upon assumptions about ideal scenarios regarding the environment, design/application challenge, or hardware like traditional systems. Such assumptions limit the potential for signal identification and other tasks, boosted by machine learning.

An Open Architecture to Adequately Model Threats

A primary challenge for EW systems is the shortened timeline for countermeasure advances compared to the long development and upgrade cycles of EW systems. Traditional EW solutions were designed to respond to specific, established threats that did not evolve. However, this closed-architecture approach cannot adequately respond to today's evolving EW threats due to increased component integration time, limited lifespan for parts, and a rise in technology obsolescence and refresh rates.

The procurement process also requires roughly three years for high-profile systems from order to delivery. Often, this timeline does not include further customization. Yet EW technology and threats progress at a nearly daily rate. In contrast, open architectures present a route to dynamically respond to the ever-changing threat environment.

An EW environment generation architecture that supports multiple hardware types and new technology insertion is key to keeping pace with rapidly evolving threats and reducing lead times for new systems and test capabilities. A common set of interfaces and non-proprietary file formats is also needed to develop simulator agnostic threat models that are not limited to use on only one vendor's hardware. In the US, for example, the Next-Generation Electronic Warfare Environment Generator (NEWEG) program allows participation from multiple vendors simultaneously via a shared interface and the use of non-proprietary formats.

A More Adaptive Future

Traditional military technology built on foundational systems needed additional engineering, software, and testing and took years to complete. In today's EW environment with fast-evolving technology, this approach is no longer adequate or feasible. A system that takes two to three years to finish is obsolete before delivery.

Modern EW systems continuously evolve as new and emerging technologies transform these systems. The warfare of the future is EW, where the EM system is the primary battlefield that every side tries to control. It's the field where computerized systems communicate, detect, attack, and protect assets.

As threats evolve and change, your system must adapt. Countermeasures must also keep pace, striving to prevail over a constant stream of new threats. As the battlefield becomes increasingly crowded with devices that demand more of a limited spectrum, sorting through signals and identifying them is imperative. Future systems will move from being adaptive to using new AI and machine learning capabilities to decipher constant changes in spectrum use. Software-defined weapon technology allows for continuous upgrades without needing to invest in entirely new systems. The new electromagnetic spectrum battlefield is increasingly challenging, and technology and weapons need to respond accordingly – even if it means breaking from the dependencies of past projects and adopting a flexible, scalable, open architecture approach.

Additional Resources

For more information on Keysight's EW solutions, visit www.keysight.com/find/ew.

For an overview of Keysight's EW test and evaluation solutions, check out our brochure.

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com

This information is subject to change without notice. © Keysight Technologies, 2020 - 2022, Published in USA, August 22, 2022, 7120-1079.EN