ASYMMETRIC THREAT SYMPOSIUM XIII
Cyber, Electronic Warfare, and Spectrum Operations: Critical Capabilities for Protecting America
REPORT 2 · AUGUST 2020

Multi-Platform SIGINT, Cyber, and EW Convergence

Jerry Parker, SVP, Electronic Warfare, CACI International Inc

The U.S. has recognized the necessity of addressing the complexities involved with potential peer state engagements. These conflicts require different mission profiles, more sophisticated operations, and, in many cases, different technologies. For example, dismounting a vehicle to hunt high value targets by their radio frequency (RF) emissions is critical in counter insurgency (COIN) operations, but rare in peer state engagements. In contrast, overcoming long-range, stand-off weapon systems is critical in peer state conflict, but is an essentially non-existent threat in COIN operations. Additionally, the proliferation of commercial technologies by our adversaries has presented even more challenges. These technologies evolve much faster than the traditional response time for developing counter technologies.

How does the U.S. keep up with training and equipping for this highly volatile battlespace? One solution is multi-function, multi-platform convergence, which blurs the operational lines between signals intelligence (SIGINT), electronic warfare (EW), and cyber while providing a common set of technologies that can be built in various form factors.

The technology element can be addressed through an analogy with commercial industry. Millions of dollars in research and development (R&D) pour into commoditizing hardware that has increased processing density and network capacity while providing modular scalability. Similarly, on the software side of the equation, commercial investments in developing high-speed open system architectures and message buses enable interoperability across systems. These fundamental elements create the infrastructure for the developer community to provide value through innovative software applications.

The same approach can be applied to military systems. The U.S. can take advantage of R&D spending and advancements in processing and network technologies to drive down material solution costs. The modular scalability of hardware enables multi-platform designs where size, weight, and power (SWaP) concerns vary between platforms. Whether the platform is a ground vehicle, an unmanned aircraft system (UAS), or a ship, ruggedized commercial hardware provides the highest performing, lowest cost solution with the longest possible life span.

Avoiding custom hardware is imperative. Custom hardware is expensive to upgrade, while commoditized hardware is not. Software is even more cost effective. When architected correctly, it can be updated on the fly to adapt to nearly any mission profile. Embedded artificial intelligence can be used to make the system even more adaptable to new threats. This enables truly multi-function systems. The same building blocks can be adapted to address electronic protection requirements for counter-UAS, counter-improvised explosive device (IED), and counter-ISR, as well as sophisticated techniques for kinetic targeting and electronic attack.

Operationally, often cited roadblocks to convergence are classification and authorization. These can be easily overcome technically with proper segmentation of data and better distinction between collection and exploitation of data. Additionally, remote operation can be built in to provide forward channels for advanced cyber operations without local operator exposure.

The importance behind this approach is efficiency; the technology and industrial base is there. As funding becomes scarce, developing adaptable, multi-function systems used across military services, platforms, and missions is imperative. This convergence will enable true multi-domain operations in a joint environment. ■