JACK BROWNE | Contributing Editor

Digital Techniques Train Cognitive EW Systems

In cognitive electronic-warfare systems, designers are recruiting artificial intelligence and machine learning for intelligent, automated responses to detected threats.

Electronic-warfare (EW) systems are often considered the most stable and dependable portions of a military electronics suite. But efforts to "modernize" defense electronics systems apply very much to EW technology. They're drawing from advances not just in spectrum extending to millimeter-wave (mmWave) frequencies, but also in the improved capabilities of more powerful microprocessors, faster data converters, and expanded artificial intelligence (AI). In terms of global EW technology, the U.S. hopes to close the gaps between the EW technologies employed by its own troops and the advanced EW systems being developed by Russian and Chinese researchers for their troops.

By applying AI and machine-learning (ML) techniques to EW systems, threats can be identified by machines and computers rather than human pilots and system operators. Subsequently, the process of selecting an electronic-countermeasures (ECM) response to a threat can be automated.

While that may sound like taking the human element out of warfare, it's following current trends for the growing use of robotics, unmanned ground vehicles (UGVs), and unmanned aerial vehicles (UAVs) in defensive warfare strategies. EW systems are leveraging the benefits of smarter electronic devices and circuits that meet reduced size, weight, and power (SWaP) requirements to provide increased signal-processing capabilities within smaller equipment enclosures.

More Robust Cyber Systems

Military campaigns are typically fought within a few domains at once, such as on land, at sea, in the air, or in space. Cyberspace is becoming yet another domain for warfare, with computers linked via the internet and attempting to manage the electromagnetic spectrum (EMS) so vital for radar and secure communications. Increasingly, "smarter" or cognitive EW systems provide many of the functions needed for control or some level of comfort when operating in the EMS.

Newer EW system designs are more fully adopting digital

1. The U. S. Army Combat Capabilities Development Command's Army Research Laboratory (ARL) is investing heavily in future EW capabilities through its Foundational Research for Electronic Warfare in Multi-Domain Operations (FREEDOM) program. (Courtesy of ARL)

EW system (DEWS) architectures promoted by each branch of the U.S. armed forces, such as the Army. DEWS approaches shift from traditional broadband analog radar warning receivers (RWRs) and signal-intelligence (SIGINT) subsystems to more thoroughly digital electronic subsystems.

For example, one program funded by the U.S. Army Combat Capabilities Development Command's Army Research Laboratory (ARL) in support of DEWS research, the Foundational Research for Electronic Warfare in Multi-Domain Operations (FREEDOM) research effort, is a starting point for much of the work in digitizing EW equipment suites. The EW enhancements include improving secure communications among allied troops and creation of techniques to measure the effectiveness of electronic attack (EA) and electronic protection (EP) techniques *(Fig. 1)*.

As part of FREEDOM, Army researchers are also hoping for greater integration of cyber electronics with EW systems

2. The Silent Crow EW pod can fit under the wing of the MQ-1C Grey Eagle UAV. (Courtesy of Lockheed Martin)

as part of an initiative called cyber electromagnetic activities (CEMA), resulting in increased mobility of electronic systems within the battlefield and cyberspace.

Dr. Matthew Higgins, FREEDOM Program Manager, explains, "Electronic warfare is increasingly vital to Army preparations to defeat any potential threat. The Army's focus on large-scale combat operations highlights the need for a robust ground electronic warfare force to support multi-domain operations and enable the Army to fight and win in a complex world.

"In the long term, we are looking at multi-function RF capabilities from distributed platforms with research focused on adaptive filters, wideband amplifiers, and adaptive manufacturing-enabled antenna technology. The soldier will have freedom to maneuver on the battlefield and to dynamically access the congested and contested electromagnetic spectrum."

Newer cognitive EW systems are being designed with advanced digital hardware, even to the extent of exploring different approaches to computer processing, such as quantum computing (which may be a few years away). Although development of these EW systems follows SWaP requirements for UGVs as well as UAVs, they're also taking advantage of the large capacities of solid-state memories. Extended memories are needed in cognitive EW systems in companion with threat-recognition algorithms to locate known or anticipated threat emitters and respond with an ECM such as a jammer.

By building a library of transmitters, such as for radars and other threats, for a particular nation or adversary, a cognitive EW system can be programmed to quickly detect and identify a known emitter. This would avoid spending long hours scouring through bandwidth for every emitter on the planet that might be a threat. As additional data is collected, these threat libraries can be expanded, and the cognitive capabilities of the EW system extended, as part of an electronic order of battle (EOB) that includes optimum ECM responses for each type of threat.

Speeding the EW Evolution

Acknowledging the need for more modern EW systems, the U.S. Army is working with Lockheed Martin among others on several cognitive EW strategies. For Lockheed Martin, one approach involves a prototype tactical electronic warfare system (TEWS). The terrestrial layer system (TLS) is intended for ground-based vehicles, such as the Humvee. And long-range airborne and ground-based jammers currently in process at the company will work their way into ECM response systems. The Army has encouraged a modular open architecture for the TEWS's C4ISR/EW suite of standards.

Lockheed Martin has quietly and secretly worked on a next-generation EW pod for attachment to ground vehicles and aircraft, even small UAVs. Called the Silent Crow EW pod *(Fig. 2)*, it can fly under the wing of the MQ-1C Grey Eagle UAV. Smaller versions of the EW pod are being developed for the Army's multifunction EW Air Large (MFEW-AL) unmanned aircraft, such as the RQ-7 Shadow and the Future Tactical UAS. The Army recently awarded the company $74.85 million for further development of the EW pods used in the Silent Crow, seeking modernization of EW technologies beyond simply 2 to 18 GHz, RWRs, and jammers.

The prime contractor has been working on a set of ML algorithms to feed the cognitive EW pod's AI capabilities. It has even employed the latest 3D-printing technologies to shrink the size of some components, such as antennas.

Silent Crow is an example of how a newer EW system can process available sensor data with high-speed processors, AI, and ML techniques to provide a pilot with more detailed information about a received signal source and a possible threat. The DEWS pods come in relatively compact housings per SWaP design guidelines and can be miniaturized for use on smaller UASs. Lockheed Martin also developed a version of the Silent Crow EW technology for ground-based vehicles, called ground RF intelligence node (GRFIN), to supply ground troops with an optimized EW system.

The Surface Electronic Warfare Improvement Program (SEWIP) Block 3 involves adding advanced electronic counterattack capability to an EW system. The U.S. Navy is working closely with Northrop Grumman so that maritime AN/SLQ-32(V) systems can outmaneuver emerging long-range missile threats. The block upgrade will provide EA capability to surface users with growth for EW using information-operations (IO) capability.

The upgraded EW system will be able to detect and disrupt inbound threats, such as guided missiles, and operate against an adversary's radar and communications systems. It employs active electronically scanned array (AESA) technology to detect and identify multiple threats, using narrow EM beams to avoid detection. It can also operate in a "silent" mode—no beams are transmitted, but it can still detect threat signals. The

3. Current work on the F-35 for future EW duties involves a 360-degree suite of sensors and ECM systems, and will ultimately replace F-16 and F/A-18 fighters. (Courtesy of Raytheon Technologies)

system's initial installation design targets Navy DDG-51 Class Destroyers.

Futuristic Flight

BAE Systems is doing its part to make the F-35 the EW fighter of the future for the U. S. Navy and Air Force in terms of air-to-air and air-to-ground combat *(Fig. 3)*. It's being groomed, for example, as a replacement for the Air Force's F-16 and the Air Force and Marine Corps' F/A-18s. The aircraft features a 360-deg. array of sensors and display units built into the visor of a pilot's helmet so that the detected information moves with the pilot.

The Air Force is also looking to BAE Systems for its AN/ALQ-250 Eagle Passive Active Warning Survivability System (EPAWSS) EW system to modernize upgraded F-15 fighter aircraft, such as the F-15E and the F-15EX from Boeing. The modular DEWSs provide many advanced capabilities to counter new and emerging threats.

The ALQ-239 platform features fully integrated radar warning, geolocation, situational-awareness, and self-protection capabilities for detecting and defeating both airborne and surface-based threats, even in dense signal environments. It includes an advanced ECM subsystem with rapid response capabilities and features multispectral RF and infrared (IR) countermeasures subsystems, a digital RWR, digital RF memory jamming, and integrated ECM dispenser to speed responses to detected threats.

In response to growing use of EW technologies, L3Harris is working on adaptive EW systems, such as its HalcyonLink equipment. These systems employ interference cancellation techniques to maintain critical tactical communications even during an adversary's efforts at jamming. In some cases, it may even be a pilot's own equipment that's doing the jamming, since an aircraft's EW suite has been known to block the same aircraft's communications equipment.

Such interference cancellation techniques allow troops to simultaneously perform EW, cyber operations, and tactical communications effectively within the small space of an in-flight fighter aircraft. For example, the interference cancellation system (INCANS) on the EA-18G Growler airborne electronic attack (AEA) carrier-based aircraft enables tactical communications even when the on-board ALQ-99 tactical jammer system is operating.