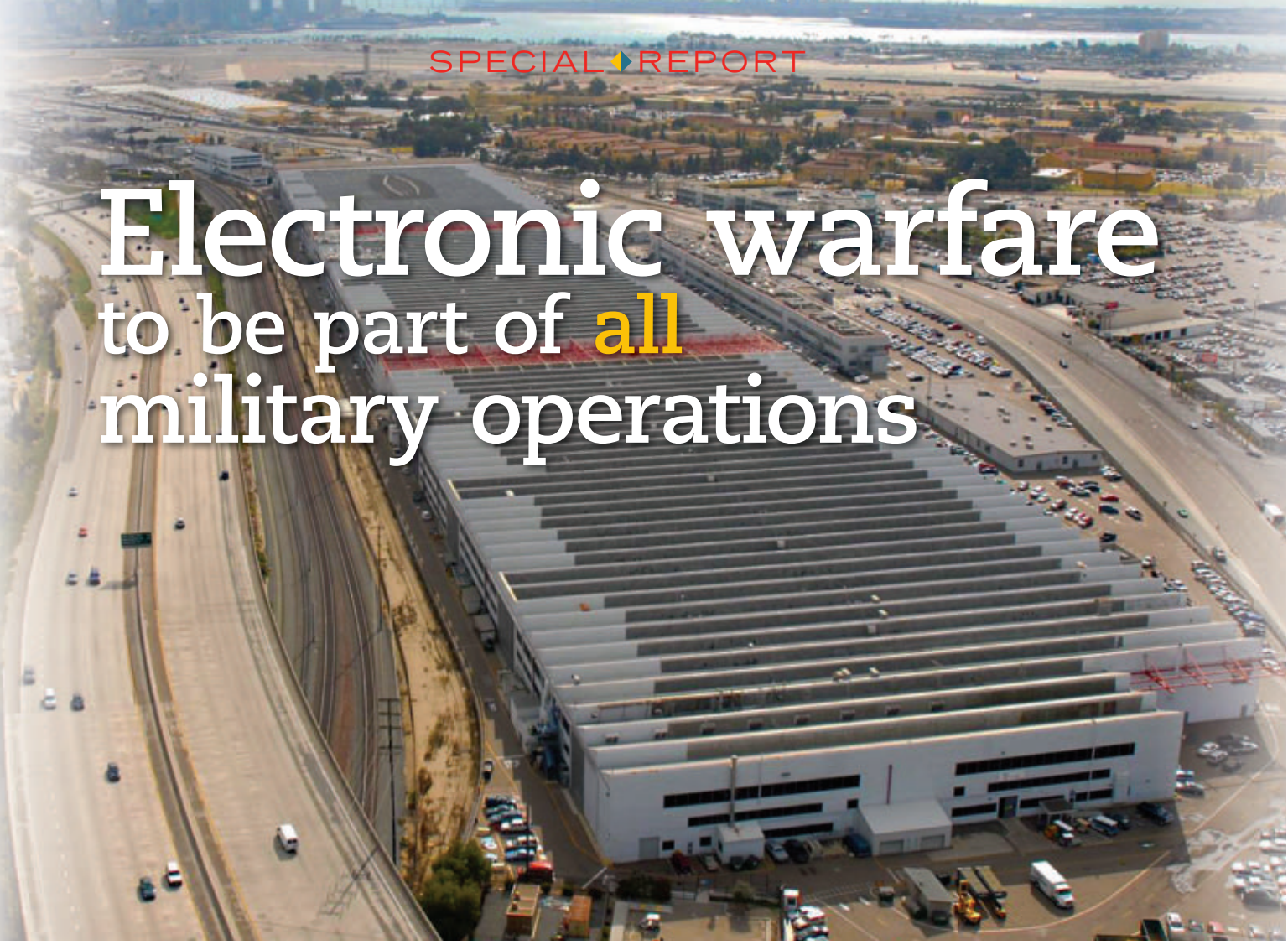


Electronic warfare to be part of all military operations

New threats and technologies are giving rise to terms like spectrum warfare that seek to blend electronic warfare, cyber warfare, and other technological approaches to controlling the RF spectrum.

BY **J.R. Wilson**

Electronic Warfare (EW) became an integral support component to more traditional warfare—offensive and defensive—in the late 20th Century. In 1973, having watched Israel jam Syrian guided missiles during the Yom Kippur War, a Soviet admiral summed it up succinctly: "The next war will be won by the side that best exploits the electromagnetic spectrum."

EW took on new dimensions and importance in post-9/11 Southwest Asia, where the enemy used electronic means to detonate their weapon of choice—improvised explosive devices (IEDs). The U.S. and its allies sought to combat those low-tech, but deadly, attacks with the components and capabilities arising from a technology boom that changed all aspects of warfare.

With the drawdown in Southwest Asia and the planned Pacific Pivot, EW now is entering yet another new stage of development, requirements and importance. Andrew Dunn, vice president of business development for Integrated and electronic warfare for Exelis Electronic Systems Division, calls it a "whole new mindset" for the U.S. military as the U.S. Department of Defense (DOD) shifts its focus to an area where uncontested access to the electromagnetic spectrum and physical battlespace may no longer exist. Instead, U.S. and allied forces must be ready to deal with near-peer anti-access/area denial (A2/AD) environments and a greater emphasis on the air-sea battle.

The fight against IEDs

In Southwest Asia, the Army and Marine Corps bore the brunt of low-tech attacks on the fringe of EW. That was especially true with the

An aerial view of the Space and Naval Warfare Systems Command (SPAWAR) headquarters in San Diego. SPAWAR is the Navy's technical lead for C4ISR, providing the hardware and software to connect sailors at sea, on land and in the air. (U.S. Navy photo)

Army, as the internal EW capabilities they had developed during the Cold War were determined no longer necessary. It would prove to be a costly mistake the Army does not want to repeat—but fears it may.

"When the USSR fell and the Cold War ended, all the organization in the U.S. Army dedicated to tactical jamming in combat EW intel battalions went away, leaving ourselves pretty vulnerable on the EW front," says Col. Rob Murray, outgoing branch chief for cyber electromagnetic activities (CEMA) at the Army Cyber Center of Excellence at Fort Gordon, Ga. "With the new challenges brought on by 9/11, going into Afghanistan and then Iraq, we found ourselves with no one responsible for EW in the Army. The enemy quickly found that seam and ways to exploit it. IEDs at first were pretty easy to spot, then they started burying the explosives and lines to them—command-detonated by hidden observers. Every time we developed a counter to what they were doing, they kept moving to new approaches."

CEMA Deputy Branch chief Matt Cullen said the insurgents' move to radio-controlled IEDs escalated the U.S. and allied death toll: "Our challenge was to 'reinvigorate' EW as the means to counter, combat and defeat RC IEDs." The Army turned for help to the U.S. Navy, which had become DOD's lead agent for EW, but it was far from a perfect solution because the EW requirements of a ground force differ from those of the Air Force and Navy.

"The Navy has a lot of its EW capability on airplanes flying off carriers and they don't turn that capability on until they are a couple of hundred miles away, so the possibility of those systems causing problems on the ship are minimal. Ships have their own EW defenses against missiles, of course, but when a missile is coming, they don't care what disruptions there may be," Cullen explains.

"But the Army has jammers in the middle of convoys in the middle of bad-guy territory—and when those jammers are turned on, they also disrupt our communications on the ground," Cullen continues. "Early in the war, the Army was buying jammers from the Air Force and Navy and support from those service's EW officers, but what they didn't understand was the jammers also disrupted our soldiers' communications."

CEMA's three pillars of EW are:

1. electronic attack;
2. electronic support—what frequencies and technologies do friendly forces use to defeat the enemy; and
3. electronic protection—keeping U.S. and friendly forces safe from fratricide and enemy EW

"The artillery guys—such as Col. Murray—take that very seriously regarding mortars. They figure out problems during planning. The same has to be done with jammers," Cullen explains. Military forces have important RF frequencies that are restricted from U.S. and allied electronic countermeasures called the Joint Restricted Frequency List (JFRL). Despite the best intention,

the JFRL does not protect against accidental disruptions—especially if using a frequency that is not on the JFRL. "In a modern Army, where we have portable computing and internet capabilities that can move information around the battlefield, we should be using radio frequency engineering during the planning process, to predict the effect of jammers on our own radios."

It was not until 2008 to 2010 that the Army was able to begin restoring an organic EW capability, says Lt. Col. Keith Cantrell, CEMA's incoming branch chief. That included standing up the Cyber Center of Excellence (COE), incorporating the work of the Signals COE it replaced, and slowly incorporating EW.

The U.S. National Security Agency (NSA) is a lead agency in signals intelligence and electronic warfare. This photo shows the NSA's National Security Operations Center floor in 2012 (NSA photo)

Shipboard and airborne EW

Despite the Navy's role as DOD's executive agency for EW, its leaders are being forced to redesign the Navy's own capabilities—air- and ship-borne. That includes the Surface Electronic Warfare Improvement Program (SEWIP) to upgrade existing shipboard signals technologies used to identify, assess and analyze EM signals and EW threats. A major problem, especially with aircraft carriers, is the massive number of radars, antennas, and other electronic systems operating simultaneously in a highly complex shipboard electromagnetic spectrum.

With the prospect of near-peer EW threats in the future, carriers and other combat and support vessels will need even greater capabilities to conduct offensive and defensive EW. That includes the NGJ, designed to give the EA-18G Growler advanced technologies for offensive EW missions when the jammer goes operational by 2020.

"The vision for the future is to take what our collection, exploitation, and early warning capabilities [find] and turn them into offensive ways to use electronic attack," says Christine Fox, who recently retired from the Pentagon after serving as acting deputy secretary of defense. "If we can go after the C2 or ISR pieces of a threat instead of putting a missile against a missile, I can potentially disrupt that missile's ability to find its target."

In addition, the Office of Naval Research (ONR) in Arlington, Va., is developing a prototype technology called Integrated Topside (InTop) to extend the range and flexibility of shipboard EW. For example, InTop would integrate the current forest of antennas on a ship's deck into a shared multi-function, multi-beam aperture array that could collect signals across a wide range of frequencies, then use a central resource allocation manager to share that information with several EW processes.

Perhaps equally important is the 21st Century version of "quiet running." The Chief of Naval Operations is pushing for greater education of officers and enlisted personnel on electronic spectrum awareness and understanding all aspects of a ship's electromagnetic signature.

"We have to be more mindful of how we operate in the electromagnetic domain and in cyberspace and how those capabilities come together," wrote Margaret Palmieri, director of the Navy's Integrated Fires Division, in the July 2014 issue of U.S. Naval Institute Proceedings. "We are working on better understanding how networks and signals and networks and information come together. What do we really look like to the enemy?

"Integrated-fires capabilities are a central part of the asymmetric advantage our Navy, joint and coalition forces bring to a fight. They include capabilities that disrupt adversary C4ISR systems, deliver electronic payloads that limit an enemy's freedom of maneuver and action and enhance the ability of our own forces to place ordnance on target," Palmieri wrote. "It integrates lethal and non-lethal fires, underpinned by superior battlespace awareness and assured C2, to provide commanders an expanded set of warfighting tools especially important in A2/AD environments, like Air-Sea Battle."

In that same issue, Vice Adm. Ted N. Branch, deputy chief of naval operations (CNO) for information dominance, discussed the Navy's need to dominate all segments of future battlespaces—on, above, and below the sea, as well as outer space—to sustain America's "global primacy'. "However, commanding, controlling and fighting our forces in these areas requires dominance in the information domain, to include the electromagnetic spectrum and cyberspace," he wrote. "The name we've given to this concept—information dominance—is still new and unfamiliar to some, but it's indispensable to Fleet operations, so much so that we've adopted it as a distinct warfare discipline.

"Formerly perceived by many as a collection of support activities performed by specialized restricted line officers, information dominance is increasingly recognized by Fleet operators as a critical force multiplier. It's no longer just an adjunct to warfighting. It is warfighting," Branch wrote.

Navy information dominance focuses on three goals: robust and agile C2 in all operating environments; superior knowledge of the battlespace, the physical environment as well as threat capability, disposition and intent; and projecting power through the integration of kinetic and non-kinetic effects. "We refer to these three elements, or pillars, as assured C2, battlespace awareness and integrated fires. Through them, information dominance creates decision superiority, provides asymmetric advantage and enhances the lethality of our deployed forces with non-kinetic options," Branch added. Those pillars, in turn, are designed to correspond to the CNO's three tenets: warfighting first; operate forward; and be ready.

"The critical element of the information dominance definition is integration, Branch wrote. "Blending the attributes of ISR, oceanography, meteorology, networks, cyber, and EW allows for better planning, smarter decisions and earlier results. Aligning the related restricted-line communities of naval oceanography, information warfare, information professional, intelligence and the space cadre into the information dominance corps has likewise advanced our concept and capability development and

improved data and system interoperability."

U.S. Marine Corps

While the Army and Marine Corps both are viewed as ground forces, the Marine Corps' EW requirements differ significantly from those of the Army, especially in meeting future anticipated threats. In recognition of that, the Corps has created a Marine Air/Ground Task Force (MAGTF) EW concept to develop an integrated system of distributed, platform-agnostic EW systems, including the progressive inclusion of technologies and capabilities from other services and commercial vendors.

Navy sailors on the watch-floor of the Navy Cyber Defense Operations Command monitor, analyze, detect and respond defensively to unauthorized activity within U.S. Navy information systems and computer networks. (U.S. Navy photo)

MAGTF EW elements have several programs in development. Among them are Intrepid Tiger II (IT-2): An EW pod for communications-based targets, expandable to radar-based targets, currently deployed to CENTCOM and with Marine expeditionary units in three different versions for fixed-wing aircraft, unmanned aerial vehicles (UAVs), and helicopters.

Another program is the Electronic Warfare Service Architecture (EWSA)—an extended data exchange and hardware protocol to connect EW/SIGINT airborne nodes, via an adaptive multi-waveform network, to ground operators, Cyber/EW Coordination Cells (C/EWCCs) and other air EW nodes. The Corps also has stood up several new or redefined units, including the Cyber and Electronic Warfare Integration Division (CEWID), the Capabilities Development Directorate's integration and execution authority for all Marine Corps warfighting development activities associated with Cyberspace and EW.

CEWID coordinates with operating forces, supporting establishment and mission partners in order to identify, prioritize and integrate capability solutions across DOD's Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) protocols. CEWID, in turn, comprises three branches: computer network attack, computer network defense, and MAGTF EW.

The General Atomics Aeronautical Systems Predator B/MQ-9 Reaper's new electronic attack capability, using the Northrop Grumman Pandora EW system, is a major part of the Marine Corps future EW effort. The system could advance the Reaper from its existing role as a counter-insurgency ISR/hunter-killer aircraft to a broader spectrum of EW missions, says GA-ASI President Frank W. Pace.

Pandora is a pod-based, multi-function, wideband system providing electronic attack, such as jamming, support and protection. Demonstrations at Yuma Marine Corps Air Station, Ariz., were designed to evaluate the ability of Pandora-equipped aircraft to conduct coordinated EW missions in a multi-node approach against a more capable integrated air defense system.

"Pandora brings optimal size, weight and power to current and future high-endurance platforms, opening up a new world of electronic attack capabilities," says Janine Nyre, vice president of radio frequency combat information systems at Northrop Grumman.

"We demonstrated operational concepts using a layered approach to electronic warfare with Reaper, EA-6B Prowlers, and other Group 3 UAVs," adds Brig. Gen. Matthew G. Glavy, assistant deputy commandant for Marine aviation. "By conducting multiple events, we were able to evaluate the viability of UAVs to conduct EW missions against enemy air defenses in support of tactical strike aircraft."

The 2013 Marine Corps Operating Concept for Information Operations termed information operations (IO) as a complex box of tools the Corps must incorporate and exploit within the context of its overall maneuver warfare philosophy and expeditionary culture to operate "effectively against a myriad of potential adversaries and perform multiple, diverse and simultaneous tasks across the ROMO [range of military operations]".

"In the Marine Corps, IO is not a warfighting function in its own right; it is an integrating function which facilitates the six warfighting functions of C2, fires, maneuver, logistics, intelligence and force protection. This distinction between warfighting and integrating function is key to the Marine Corps' belief IO does not—and will not—replace any of the time-tested warfighting functions. It will

enable each of them," says the OCIC.

"IO is not a discrete, stand-alone capability, but is the integrated, coordinated and synchronized operational application of all information-related capabilities (IRCs), organic and non-organic, to affect decision-making by adversaries and potential adversaries, thereby creating an operational advantage. Integration is accomplished under the purview of the operations section, based upon commander's guidance, and supports achievement of the commander's end state. "IO is not synonymous with individual discrete capabilities or activities, much like fire support is not synonymous with artillery or aviation. More art than science, IO is focused on the human mind and seeks to influence behaviors to produce operational advantages."

EW in the air

While emphasizing they "do not generally comment on EW requirements, specific technologies or capabilities of our or others' systems", the Acquisition, Science, Technology and Engineering Directorate within the office of the Secretary of the Air Force (SAF/AQRM) did provide the following statement: "The Air Force recognizes that increased budgetary constraints, coupled with widespread availability of modern electronics, requires new technology and acquisition approaches for EW. The Air Force is tackling the problem along five fronts: 1) enabling fundamental components, 2) new techniques, 3) new adaptive modular approaches, 4) early prototyping and rapid reaction developments and 5) early in-the-loop testing.

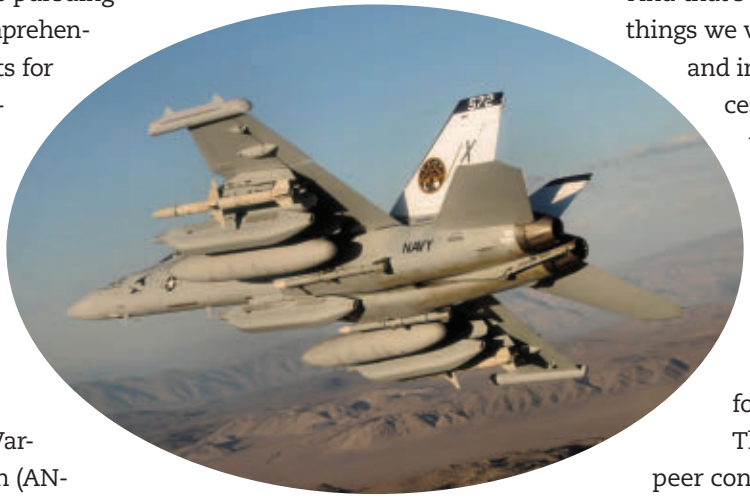
"Today's EW, Communications, Navigation, Sensing and Cyber

technologies require a more integrated use of the electromagnetic spectrum than ever before. The Air Force Research Laboratory (AFRL) is working on full spectrum science and technology, which includes: radio frequency EW; avionics protection; position, navigation and timing [PNT] in contested/denied environments; electro-optical/infrared threat warning and countermeasures; protected communications and robust cyber."

In its "Strategy for Spectrum Warfare", SAF/AQRM noted it is pursuing those goals through a comprehensive Advanced Components for EW (ACE) program and developing cognitive and distributed techniques, adaptive modular approaches and rapid prototyping.

AFRL issued a broad agency announcement (BAA) last fall for the Advanced Novel Spectrum Warfare Environment Research (ANSWER) program to develop adaptive spectrum warfare technologies to maintain warfighting capabilities in contested and denied environments consistent with A2/AD scenarios. AFRL encouraged industry to employ unconventional thinking on the use of advanced computing power, signals processing, modeling and simulation, anti-tamper and software protection technologies, GPS alternatives with comparable accuracies for warfighters in A2/AD environments, vision and laser-based navigation and electro-optics countermeasures.

"With an ever-changing environment between red and blue forces, the ability to control the electromagnetic spectrum is a key requirement to achieving success in warfighter operations. This is a daunting task under benign conditions and becomes even more of a challenge as adversaries are able to employ various denial capabilities," the BAA noted. "If one can conduct electromagnetic spectrum operations under A2/AD conditions, then successful operations in other less challenging environments should be achievable as well. To accomplish this, the warfighter needs to be able to control adversary use of electromagnetic spectrum, ensure friendly access to/use of electromagnetic spectrum, protect sensor/avionics end nodes, establish/maintain secure communications/data links in dense electromagnetic spectrum environments and assure the availability of accurate PNT information. The ANSWER program is designed to address these challenges."



The Navy Boeing E/A-18G Growler combat jet is the nation's primary airborne electronic warfare platform, and should see land- and carrier-based use well into the 21st century.

The Post-OEF/OIF EW Environment

"When it comes to EW, it doesn't have to be a near-peer or even a known rival. Electronics that can be made to be a problem are ubiquitous throughout the world," says the Army Cyber Center's Murray. "You can find a thousand types of cell phones in Afghanistan, which I certainly wouldn't call the modern world. So a lot of technology is out there, worldwide, that, in the wrong hands, can be a very severe problem, no matter what kind of advanced weapons or armor we have.

"Technology changes so fast that what is considered SOTA today may not be in another year," Murray says. "And that's one of the challenges on things we would like to have now and in the future. But the processes we must go through to acquire the equipment we would like to have and need to have are not as agile as we need them to be. They're OK now, but if we get into a new fight, you can't wait for what you need."

The possibility of near-peer conflict is growing as the U.S. puts a greater focus on the Asia/Pacific region and Eastern Europe once again feels threatened by Russia, even as the Middle East continues increasingly tech-based rounds of ancient conflicts. In addition, the vast distances involved and the lack of U.S. land bases in the Asia/Pacific—outside of South Korea and Okinawa in the north—will mean a greater focus on the Navy and Marine Corps, especially with respect to EW.

There was a sharp reduction in the Pentagon's EW research and development budget from 2013 to 2015—a cut from $3.5 billion to $2.1 billion—more than half from the Navy and Marine Corps. Of course, an unknown—but suspected

substantial—part of EW research falls under classified "black" budgets.

"Although EW is declining through 2015, we expect to start seeing a resumption of spending from 2016 on," says John Hernandez, a senior aerospace and defense industry analyst at market researcher Frost and Sullivan. "That is an area that is being underdeveloped right now, but with the potential new adversaries in the coming years, it will need to be reinvigorated. Some analysts are predicting an increase in small, even hand-held jammers, but our analysts expect to see more modularity, especially for ship-board systems.

"There was a move for a while to make the F-35 the new EW platform, but I don't think the expense was worth it, given the fine job the Growler is doing. But in the future, I can see unmanned systems doing more EW, whether that is a single platform or a flock of UAVs doing jamming or AD missions. Personally, I suspect protecting our own systems is and will continue to be a priority over offensive technologies."

Defense industry adapts

The new environment and focus on naval assets also has been reflected in industry. In February 2014, for example, Raytheon Space and Airborne Systems combined several EW efforts into a new mission area called Electronic Warfare Systems, based at the company's El Segundo, CA, campus. The new unit will focus on the Navy's Next-Generation Jammer (NGJ);; EW self-protection systems; EW communications systems; advanced EW programs; and airborne information operations.

At the Northrop Grumman Integrated Systems sector, meanwhile, airborne early warning and electronic warfare systems have seen a similar growth in importance, including the June 2014 award of a joint service (Army/Navy) contract for 18 APR-39D(V)2 radar warning receiver (RWR)/EW management system (EWMS) pre-production units.

"Our APR-39D(V)2 merges the baseline capability of previous systems with the Northrop Grumman digital receiver technology to provide advanced capability for today's and tomorrow's threat

environment," says Northrop Grumman's Nyre. "This lightweight system maintains interfaces with legacy systems and includes flexibility for future growth enhancements."

The company is to deliver the systems in late 2014 preparatory to hardware-software and platform integration testing in 2015.

Also next year, Northrop Grumman is scheduled to complete equipping the Navy's MQ-8C Fire Scout rotary UAV with a new external Multi-Capability Pod, providing it with "multiple EW sensors for employment in the littorals", says a DOD announcement in May 2014.

BAE Systems is leveraging advances in signals processing and machine learning under a DARPA-funded program called Adaptive Radar Countermeasures (ARC). The goal is a next-generation EW algorithm suite as a software upgrade existing EW hardware to can use to operate against emerging radar threats and help achieve and maintain U.S. air dominance in future battlespaces. Special emphasis will be on countering never-before-seen threats with unknown waveform characteristics and behaviors.

"This technology will provide a revolutionary capability to EW systems on U.S. military airborne platforms to counter adaptive radar threats and significantly improve survivability," says Joshua Niedzwiecki, BAE's director of strategic development. ARC is projected to be ready for live demonstration flight tests by 2018.

Mercury Systems in Chelmsford, Mass., has been predominantly involved with air-to-air/surface-to-air systems, but Chief Technology Officer Chris Lewis says the current SOTA for them "has been the transition from classic denial—jamming—to more deceiving your adversary".

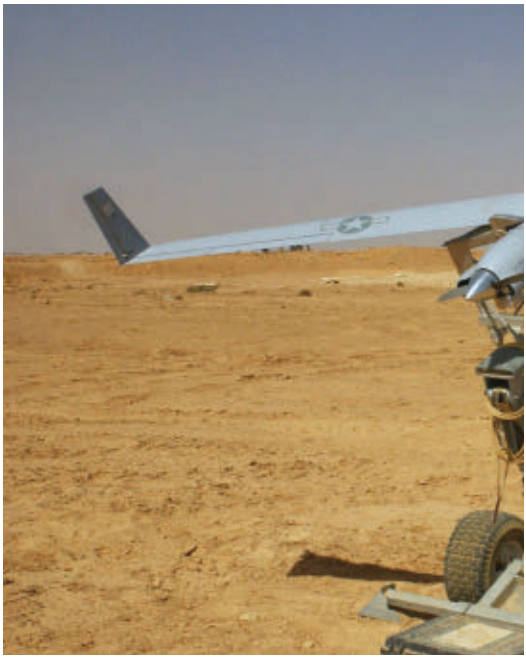
"The world today is less bifurcated between EW and Cyber, which I consider part of the same continuum," he says. "The kinds of things we're seeing starting to come on line are systems that are much tighter in their response. Where conventional systems saw a new waveform that then was captured and technology to deal with it developed in the lab, today's system is tighter, with techniques being developed in days rather than months. And the goal is be instantaneous.

"Enabling technologies for future EW include continuing improvement in the performance of FPGAs and microprocessors, the continued drive in communications and great improvement in solid state amplifiers due to gallium nitride. Further down the line is photonics for very wide bandwidth and high dynamic range. Another, not a technology so much as capability, is the adaptive learning system. Some of the SOTA things being done today are just scratching that surface and I see more of that coming online in the next few years."

Lewis sees the largest EW market for the foreseeable future being retrofits for legacy platforms DOD cannot afford to replace: "As the U.S. goes forward, there will be more and more demand to do things with less and less. And the leverage of doing that in terms of retrofits will have a lot of benefits for the country as a whole."

Spectrum warfare

Rapid advances in technology have complicated the definition of EW. The Air Force uses spectrum warfare to bring together all elements of EW with cyber warfare, information operations and essential capabilities to enable a full range of electromagnetic operations—offensive and defensive—in A2/AD environments against all levels of adversaries.



Unmanned aerial vehicles (UAVs) of various sizes, including the lightweight ScanEagle shown above, are taking on increasing roles in offensive and defense electronic warfare.

The Army prefers cyber electromagnetic activities. According to recently revised Army Doctrine for Unified Land Operations, CEMA involves "activities leveraged to seize, retain and exploit an advantage over adversaries and enemies in cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system". Implementation is achieved through synchronization and integration of cyberspace operations, EW and electromagnetic spectrum operations (electromagnetic spectrum).

Terminology aside, nearly every aspect of command, control,

communications, computers, intelligence, surveillance and reconnaissance (C4ISR) has (or is) a component of or dependent on 21st century EW.

Frequency-hopping radios and radar soon may be replaced by "cognitive" systems that don't rely on a set list of frequencies, but look for available "holes" throughout the full spectrum, jumping from one to the next on the fly. A primitive version of that is a smartphone that uses the best available way to connect, from nearby WiFi to 4G.

But control and unchallenged access to battlespace spectrum also is critical for navigation—from precision-guided munitions to logistics—semi-autonomous combat robots, field and battlespace medicine and more. And as spectrum becomes ever-more crucial to military and commercial communications and data transfer, two long-standing "laws" of technology continue to converge.

The more widely known Moore's Law, named for Intel co-founder Gordon Moore, states that CPU speeds double every two years (although purists note it is more accurate to say the number of transistors on an affordable CPU is what doubles).

The lesser known Cooper's Law, formulated by the inventor of the cell phone Martin Cooper, notes the number of conversations, whether voice or data, that theoretically can be conducted using a specific piece of useful radio spectrum has doubled every 30 months for more than a century. As a result, total spectrum allocation for personal communications alone has increased more than one trillion-fold in the last 90 years.

Increasingly competitive, congested and contested cyberspace and electromagnetic spectrum will be even more important as the U.S. faces potential conflict with a near-peer adversary for the first time since World War II—and as CEMA capabilities spread and grow down to the level of individual terrorist cells, criminal organizations and Third World nations, none of whom could ever hope to survive a traditional engagement with the U.S.

The services' differing views of the involved technologies are more than semantic, they also are operational. The Navy sees EW as modern warfighting, the Air Force considers it an essential and integrated component to the success of A2/AD and air dominance, but the Army continues to view it as a support component, not warfighting.

"When you talk about maneuver commanders, the objective is to seize and secure terrain. The EW mission is to support that, but EW and cyber have separate roles to play. Cyber can and is moving into a major combat role; the EW role is to control the spectrum to allow the maneuver commander to achieve his goals," says the Army Cyber Center's Cantrell.

CEMA's Cullen agrees, adding those in combat are only interested in what works: "From a maneuver commander's perspective—infantry or armor—they don't care if it is EW or cyber or whatever. There are advantages and disadvantages to both EW effects, cyber effects and kinetic effects. The requirement is to figure out which is best in a given situation."

In April 2014, the Naval Air Warfare Center Weapons Division and the Association of Old Crows held the 43rd Electronic Warfare Symposium at Point Mugu, Calif., with the theme "Enabling Collaborative EW Through Innovation and Invention."

"Staying up-to-date in EW technology is essential to supporting the warfighter, said Dr. Ron Smiley, director of the EW/Combat Systems and Avionics departments at the Naval Air Systems Command at Patuxent River Naval Air Station, Md., told the conference. "Electronic warfare is changing, becoming more challenging and has continued to become a lot more esoteric, particularly with the convergence of EW and Cyber Warfare."

Rear Adm. Mark Darrah, commander of the Naval Air Warfare Center Aircraft Division, summarized the conference discussions with a view to potential enemy developments and the changing nature of U.S. technology development. "Unlike 20 years ago, our advisories are developing similar technologies that we are—and are doing it right now," he says. "The only way we will stay ahead of the threat of our enemies is to take paper ideas and give it to our people for trial-and-error until we succeed."