AVIATION WEEK
INTELLIGENCE NETWORK

Electronic Warfare

Experts Urge U.S. To Link EW And Cyber Plans

Aviation Week & Space Technology Mar 17, 2014 , p. 56

David C. Walsh
Washington

Is the U.S. lagging when it comes to electronic-warfare planning?

Printed headline: Keeping Pace

Advancements in the Chinese air force, along with a proliferation of technologies that could be converted into electronic weapons, have analysts and officials warning that the U.S. may not be keeping pace.

In November 2011, the Government Accountability Office issued a scathing review of the Pentagon's management of electronic warfare (EW), charging that it had ill-defined coordination practices. The following February, then-Defense Advanced Research Projects Agency Deputy Director Kaigham Gabriel testified to Congress that the U.S. had lost preeminence over the electromagnetic spectrum since “about 1997.”

In the electronic domain, the goal is to exploit the spectrum by jamming, altering, misdirecting, mimicking or destroying an adversary's operations—while safeguarding one's own. The spectrum is already facing an increasing barrage from radiated electromagnetic or directed energy.

Chief of Naval Operations Adm. Jonathan Greenert is an advocate for harnessing the spectrum for EW. “We are using the electromagnetic spectrum as a domain and as a means, and we understand and grasp it,” he says. “We have to figure out how we can beat things electronically first. Why do we spend all this money kinetically if we can jam, spoof or do otherwise?”

The EA-18G Growler specializes in electronic attack and enemy air defense suppression. *Credit: U.S. Navy*

The first step in becoming more adept at EW is to cultivate more awareness of the electromagnetic and cyberwarfare environment, Greenert says. “We need to know what 'normal' is,” he expounds. “We've brought all these networks in, and we know when there is a change, but is the status quo the normal? The [next step] is finding out what our electronic signature is on all our units.”

The Navy needs to develop radars that can use alternate frequencies, and to assemble cyberteams. “We have got to evolve this paradigm,” Greenert says. “We need to prepare the fleet to enact an electronic warfare plan the same way they think of a communications or surface warfare plan.”

Kevin Pollpeter is the deputy director for the study of innovation and technology in China, at the University of California-San Diego. Like Greenert, he advocates the convergence of EW and cyber.

In his book “China's Emergence as a Defense Technological Power,” Pollpeter notes the relative ease of inserting malicious algorithms in any antenna—with benefits well outweighing costs.

China's e-threat matrix, he says, comprises space, cyber and EW. And it is here—versus conventional arms, where it is definitively outclassed—that China hopes to seize the initiative.

Pollpeter explains that China appears well prepared to employ melded EW and cyberattack; the U.S. is not. That fusion will be “a major part of any operation involving an advanced military power,” he says.

Should the Pentagon fail to engage similarly, “systems not protected against such [tandem] attacks will be vulnerable,” Pollpeter notes. E-assaults would be worse in light of vulnerabilities with active, electronically scanned array (AESA) radar, which are used on many advanced U.S. aircraft.

Otherwise highly competent, AESA provides “an easy pathway for malware insertion and other cyberattack.” Another AESA counter, Pollpeter says, citing Chinese defense industry boasts, is the KG300G jammer pod, using “digital radio-frequency memory.”

China's anti-access/area-denial (A2/AD) strategy is gaining favor, too, according to Pollpeter. A2/AD refers to Beijing's increasing demarcation of contested territory as “I dare you” zones, the maneuvering toward which could be construed as a casus belli.

The response would be resisted, he believes, as much or more via EW/cyberwarfare ops such as jamming radars as through traditional kinetic means, including capable anti-radiation missiles. Even limited spectrum/cyberwar/kinetic successes might “greatly complicate U.S. Air Force operations.”

Targeted in this “quick war, quick resolution, preemption and surprise,” war scenarios would be “centers of gravity,” specific U.S. command and control networks, and other nodes.

Significantly, Chinese writings propose not widespread extirpation of the enemy or “victory” in the usual sense, but localized, time-specific information dominance. “The goal is to paralyze, not annihilate the enemy, but merely render him deaf, dumb and blind,” he says.

Another development may be a speed-up in program maturation. Gabriel and others describe a “democratization” of EW, pointing to the avalanche of easily reverse-engineered mobile consumer electronics, i.e. tablets and smartphones. These help enable adversarial nation-states like China (and its plausibly deniable “patriot hackers”) to jam frequencies and otherwise imperil the U.S. defense establishment's encrypted communications. Likewise, “lone wolves,” industrial spies and anarchist groups can employ these methods. The core technology was previously closely guarded but is now within the reach of millions of people.

And newer, smaller devices are not less powerful, but more numerous, offering access to more frequencies for malevolent aims, Gabriel testified. Relatively crude, the devices are cheap and easily manufactured. Concentrated on the same target and launched in numbers, they become an asymmetric force multiplier.

Other experts are more measured in their comments about a gap between Chinese and U.S. capabilities.
U.S. Air Force Col. (ret.) Wayne Shaw is a longtime EW officer who flew missions over Bosnia-Herzegovina, Iraq and Afghanistan. He now presides over the Association of Old Crows—an influential EW advocacy organization.

Shaw has a professional's concern about Chinese EW/command and control and similar capabilities, but leavens it with can-do optimism and a tally of America's e-warfare assets.

About the airborne warning and control system (AWACS), a platform that can control 100-plus other aircraft at once, he says, “China has only a handful” of KJ-200/2000 AWACS. “That hardly makes for a robust capability.” The U.S. owns about 70 E-3 Sentry AWACS brimming with advanced EW and electronic intelligence exotica, offensive and defensive.

The People's Liberation Army Air Force (Plaaf) KJ-200 maxes out at about 20,000-ft. orbiting altitude, limiting line of sight, versus the much higher orbiting E-3; “an operational disadvantage,” he quips, “for orchestrating air wars over hundreds of miles of airspace.”

The KJ-2000, based on the Soviet IL-76 airframe, is “not exactly new technology. And they have only about four of them.” It should be capable of orbiting higher, but Shaw believes there are too few to make “a really viable fleet.”

U.S. E-3 AWACS significantly outclass the Plaaf's. The Chinese, Shaw concludes, “will be closing the gap for a long time to come.”

In addition, the U.S. maintains its fleet of EA-18G Growlers, which specialize in electronic attack and enemy air defense suppression. Shaw, who has viewed crews in an EA-18G simulator during a high-threat scenario, notes that “it is an incredible capability.”

Other serious U.S. EW tools include the MALD-J (Miniature Air Launched Decoy-Jammer), which can be launched from B-52s, 16 at a time, and the Next Generation Jammer (NGJ), reportedly soon to replace the legacy ALQ-99 jamming pods.

Concludes Shaw: “Don't lose the faith.”