McClatchy DC

Previous Story
Next Story

Advances in electronic warfare fly under the public's radar

By W.J. HENNIGAN

Los Angeles TimesMarch 17, 2014

LOS ANGELES — As the Pentagon moves beyond the relatively low-tech wars in the Middle East and turns its attention to future national security challenges, it has doubled down on sophisticated new radar-jamming devices that aim to render adversaries' air defenses useless.

Although the U.S. faced limited resistance in the skies above Iraq and Afghanistan, that would not be the case in Asia, where the Obama administration plans to shift its diplomatic focus and strengthen its defense strategy in the coming decade.

China and North Korea, for example, have quietly invested in advanced sophisticated radar systems, surface-to-air missile batteries and power-projection capabilities.

So when the Pentagon revealed its fiscal 2015 budget proposal two weeks ago, much of the attention was given to a boost in spending on drones and cybersecurity. Less heralded, but vital to U.S. strategic success, experts say, was the high-dollar investment in radar-jamming technology and other electronic warfare.

Much of this shadowy world is top secret, but the military's goal is to have complete control over the range of wireless frequencies at the heart of all aspects of war: satellites, radio and radar.

Jammers, for instance, are designed to identify enemy radar installations, then spew radio waves and beams of electromagnetic noise to electronically disable and destroy them. Though the technology does not result in the sort of fiery blasts produced by heat-seeking missiles or laser-guided bombs, the effect is the same.

"We are so used to dominating at sea and in the air, we don't spend anywhere near the money we should on enablers like electronic warfare and deception and other things like that," acting Deputy Defense Secretary Christine H. Fox said this month. "That can make a huge difference. And in this budget environment, we can actually afford things like that."

The hardware used to wage this brand of battle is rarely publicly discussed, but it's being built at locations throughout the Los Angeles area.

Travis Slocumb, head of Raytheon Co.'s electronic warfare systems programs centered in El Segundo, said work on next-generation electronic warfare will bring together all the advancements in computer, wireless and communications technology in recent decades.

Engineers are working on it inside the pristine clean rooms and laboratories at Raytheon's sprawling facility.

"I don't think they'll ever make a 'Top Gun'-type movie on the work we do," Slocumb said. "If our technology works, it isn't going to make the nightly news. Everything we do is behind the scenes. We like it that way."

The capabilities of jamming technology are shrouded in secrecy to stay ahead of adversaries.

What is known is that the equipment is strategic and has been used with great success in recent years. The U.S. Navy used EA-18 Growler jets in 2011 to jam Libyan dictator Moammar Gadhafi's ground radar, enabling NATO fighters and bombers to strike tanks, communication depots and other targets with complete freedom. The jet's "EA" stands for "electronic attack."

The Growlers look like imposing fighters armed to the hilt with big bombs slung under their wings. That's because the plane is a modified version of the F/A-18 Super Hornet. But a closer look reveals that instead of bombs, the Growler carries an array of radars, antennas and high-tech gear.

Each device hanging from the Growlers' wings performs a different function, including pinpointing the location of enemy radar sites, intercepting and jamming radio signals and following the changing enemy radar tactics.

The Navy has placed such a high value on the planes that last week it confirmed it placed an order for 22 more on its unfunded 2015 request submission. If approved by the Defense secretary and Joint Chiefs of Staff, the order would be a boon for Northrop Grumman Corp.'s El Segundo facility, which makes the plane's fuselage sections.

Although the Growlers' jamming system has been repeatedly upgraded over the years, it has been in service since the Vietnam War. The goal is to begin installing the Navy's new jamming devices on the carrier-based EA-18 Growler jet by 2020. They might also be put on the F-35 Joint Strike Fighter and remotely piloted drones.

Under the 2015 budget proposal, the jammer would receive $247 million in funding - 56 percent more than in 2014. With follow-on contracts, the Navy said the program could be worth more than $7 billion in the years to come.

The promise of money like that - at a time when defense spending on weapons is expected to shrink - set off a heated competition among four aerospace giants: Boeing Co., BAE Systems, Raytheon and a team of Northrop Grumman and Exelis Inc.

The contest dragged on nearly three years before Raytheon - and its electronic warfare unit in El Segundo - was named the winner.

Last year, the Pentagon said it would deploy a majority of its warships and submarines to the Pacific by 2020, leaving a 60-40 split with the Atlantic fleet. It also will add more advanced weapons systems and boost training exercises to enhance regional security.

The Chinese People's Liberation Army is known to have poured money into electronic warfare and has publicly acknowledged conducting training exercises. Such exercises are such a concern for the Air Force that it has been training fighter and bomber pilots to fly without GPS, data links, communications and radar.

"Our adversaries have taken careful note and have been investing in asymmetric ways to deny us these systems," Gen. Mike Hostage, commander of Air Combat Command, said in September. "Our adversaries should know that such asymmetric attacks will not stop us; they will only make us mad."

The Pentagon requested more than $500 million for electronic warfare programs, but much of the funding for the work is in a classified portion of the budget.

Even as the U.S. is trying to enhance its electronic weapon prowess, there are increasing fears within every branch of the military about its ability to protect against an electronic attack that could shut down those frequencies and render billions of dollars' worth of cutting-edge aircraft and munitions useless.

It has been shown in the Internet age that interfering with the spectrum doesn't take tremendous wealth, as it does with other modern-day weapon systems. Iraqi insurgents seem to have proved this when they reportedly hacked into live video feeds from MQ-1 Predator drones using off-the-shelf software. They couldn't take control of the aircraft, just see the video that was streaming back to military personnel.

What's more, electronic warfare and cyberwarfare are converging. The military has the capability to launch

cyberattacks by slipping viruses into enemy computer networks from ships floating at sea or aircraft flying thousands of feet above.

In 2012, a research team at the University of Texas at Austin used a technique called "spoofing" when it commandeered a small drone by sending false GPS signals to trick the aircraft's receiver, proving the technology is vulnerable to attacks.

Electronic warfare may not be new, but its growing importance cannot be underestimated, said Peter W. Singer, a fellow at the Brookings Institution and co-author of "Cybersecurity and Cyberwar."

"Going back to the first use of little strips of aluminum tossed out of bomber planes in World War II, electronic warfare has traditionally been about disrupting the enemy's systems through some kind of jamming or other forms of blocking signals," he said. "The new era is more sophisticated about getting inside their networks and not just disrupting or tricking them, but even co-opting them."

Join The Conversation

McClatchy Washington Bureau is pleased to provide this opportunity to share information, experiences and observations about what's in the news. Some of the comments may be reprinted elsewhere in the site or in the newspaper. We encourage lively, open debate on the issues of the day, and ask that you refrain from profanity, hate speech, personal comments and remarks that are off point. Thank you for taking the time to offer your thoughts.