Navy Forges New EW Strategy: Electromagnetic Maneuver Warfare

By SYDNEY J. FREEDBERG JR.on October 10, 2014 at 5:13 PM

WASHINGTON: The Navy is crafting a battle plan to retake control of the electromagnetic spectrum, which the Pentagon's chief of research says we've lost.

First of all, if adversaries can exploit rapid advances in commercial electronics to run circles around America's multi-billion dollar arsenal, our slow-moving procurement process needs to be more open to civilian innovation. But new technology is not enough.

What's really needed is a whole new concept of electronic warfare, officers told me this week. It's a concept in which jamming is not just an "enabler" for conventional attacks but a weapon in its own right. It's a concept in which electronic warfare is no longer largely relegated to specialized aircraft, like the Navy's venerable EA-6B Prowler and its replacement the EA-18G Growler. Instead, the Growler becomes the cornerstone of a network encompassing the entire force, from drones to surface forces and even submarines. Coordinated by a yet-to-be-developed "electromagnetic battle management" system, all of these individual platforms will collect data on enemy signals to inform the network while dialing up and down their own emissions to deceive or jam the adversary. The Navy calls this "electromagnetic maneuver warfare."

Today, "it's pretty much trench warfare," said Capt. Rob "Ice" Gamberg, a lead author of the Navy's implementation strategy for Electronic Maneuver Warfare, which will be briefed to Chief of Naval Operations Adm. Jonathan Greenert later this month.

"You've got your certain set of frequencies, you've got your certain power settings, and you've got your certain set of modulations and that's kind of what you use, day in and day out," he told an audience of EW professionals at the annual Association of Old Crows conference. "If you're going to change it, it's going to take you a long time" — and that can't keep up with adversaries using commercial technology.

So, I asked Gamberg after his remarks, if the counter to trench warfare and the Maginot Line was the highly mobile German *blitzkrieg* — the modern archetype of maneuver warfare — how do you go from trench warfare to "maneuver" when you're dealing with radio waves?

One model is how submariners deal with sound waves, Gamberg replied. "It translates really well [and] we're leveraging a lot of the thought process, he said. "That's why Adm. Greenert" — a submariner — "understands this stuff."

In both civilian and military networks today, the default is everyone's connected — and transmitting — all the time: A cellphone is constantly emitting electromagnetic signals, which is why airplane passengers used to have to turn them off. On submarines, by contrast, the default is that you're dark: you don't transmit, you're not connected, you emit as little as possible. Every time submariners do something that makes noise, let alone run up the periscope to see or a VLF radio buoy to communicate, they must make a conscious, tactical calculation about the risk involved.

That's the kind of mindset that surface and air combatants must now apply to electromagnetic emissions, Gamberg told me. "Even though I'm in an airplane and I may be *able* to transmit all day long, I'm not gonna," he said. Aircraft and ships need to take maximum advantage of passive sensors, "listening" to the emissions in their environment like a submariner. Even when they must go active — to transmit vital information to the rest of the force, to scan a target with radar, to jam an enemy signal — they need to do it in deliberately unpredictable ways. "I may not transmit in the same frequency, the same power level; I may not use the same modulation," Gamberg said. "I may jump out of the RF [radio frequency] spectrum and go into EO [electro-optical, e.g. visible light]."

"Within the limits of physics, I want to make choices" about what makes tactical sense to emit at any given moment, Gamberg went on. That may mean dropping off the network completely as does a diving submarine. "Maybe today's the day I'm moving in the physical domain and I don't want anybody to know about it, so, guess what, you're not going to hear from me. I'm not going to hear from you," he said. At other times, that might mean turning every emission up to 11 so a small decoy ship looms on enemy sensors like an aircraft carrier: "I may not be doing anything, but he thinks I'm doing something big."

"All warfare is based on deception," Sun Tzu wrote 2500 years ago. But what makes this deception possible in the electromagnetic realm is technologies largely developed in the last 25 years. Radios and radars used to be built with hardware that could only transmit in certain pre-defined ways. Military aircraft could carry a computerized "threat library" of what kinds of signals came from what enemy systems and automatically match newly detected emissions to this limited list. Today, radios and radars are controlled by software that can change how they emit from moment to moment, often using frequencies and waveforms most US systems aren't even designed to detect.

Retired Navy cryptologist Jim Kilgallen, now president of COMINT Consulting, recorded one burst transmission — he didn't say from whom — that changed modulation eight times in two seconds. "I think the environment has gotten away from us to a point that we don't understand," Kilgallen told the Association of Old Crows. "I think some of the things we face are so quick, so nimble, and so rapidly changing that.... there's no time for a human to be in the decision loop." At least part of the response must be controlled by a "cognitive" computer — in simple terms, artificial intelligence.

The strategic problem is that cutting-edge software — unlike nuclear weapons or stealth fighters — is not a monopoly of major powers: It's available to any state, organization, or even individual with the cash to buy it and the know-how to use it.

"Our adversaries really take advantage of these technologies and push them out sometime far faster than we ever imagine," said Frank Klemm, head of tactical electronic warfare at the Naval Research Laboratory (NRL). "We typically only react after we've seen the problem and we're constantly playing 'let's catch up.'"

Is there any area in EW where America does have an enduring advantage? If so, it's not technology. Instead, it may lie in leveraging our vast investment in all sorts of aircraft, ships, and submarines not originally envisioned as electronic warfare platforms.

The Navy's new EA-18G Growler electronic warfare aircraft during sea trials.

The Navy Vision: Beyond The Growler

The new appreciation of electronic warfare isn't limited to the Navy. But it's the Navy EW community that has the most money, equipment, and experience, ever since the Army and Air Force retired much of their EW arsenal after the Cold War and left the job to Navy and Marine Corps Prowler squadrons.

Now the Navy — though not the Marine Corps — is replacing the aging Prowler with Boeing's EA-18G Growler. But the new electronic warfare concept goes far beyond the Growler.

"Everyone looks at the EA-18G as 'the' electronic warfare platform," said Capt. Scott Farr, deputy commander of the Pacific Fleet's electronic attack wing on Whidbey Island, Washington. "Well, in naval aviation, we are interweaving electronic warfare into every platform." That includes the new P-8 Poseidon patrol plane, the upgraded E-2D Hawkeye radar plane, even the MH-60R helicopter, plus the soon-to-arrive F-35 Joint Strike Fighter, he told me in a phone call: "All of those platforms are going to have a lot more play in… electronic warfare."

Navy MH-60R helicopter

"The whole basis of electronic maneuver warfare is to bring all those capabilities to bear," agreed Gamberg at the AOC conference. "The EA-18G with the Next Generation Jammer is really the cornerstone capability," he said, but only by using every possible platform — even submarines — to collect intelligence can the Navy detect elusive, low-power and rapidly changing enemy signals.

Those other platforms hardly replace the Growler, however. To the contrary, they feed it more information on the enemy so it can attack more effectively. "The role that the EA-18G is going to be play is going to be *more* robust," Farr said. As so-called "anti-access/area denial" systems grow more sophisticated and long-ranged, he explained, the EA-18G will be essential to break the electronic links of the "kill chain" connecting enemy sensors to commanders and weapons.

"Instead of running away bravely like we used to do with the Prowler, now we have the

ability to fight and stay on station [with the Growler], said an appreciative Air Force officer, Lt. Col. Don "Buzz" Keen, currently assigned to a Navy EA-18G squadron on Whidbey Island. "As [enemy] radars get more and more powerful," he told the AOC conference, "we need to have a platform that can push in close and inject massive amounts of energy into enemy radar comms and links" — something only a dedicated jammer aircraft can do. "If we can quickly dispatch an air-to-air threat [using targeting radar], we can stay in position much longer to support the strike package."

EA-6B Prowler

In the past, EA-6B Prowlers operated in pairs supporting "strike packages" of other aircraft — Navy, Marine, and Air Force alike — in "scripted and preplanned" missions, Capt. Farr said. "What the EA-18G brings is an adaptability and a flexibility that we didn't have before."

Except for a small number of upgraded Prowlers, the older aircraft lacked the datalinks to exchange large amounts of information in real time as new threats emerged. That was acceptable against Soviet-style air defense systems, with their centralized command and outdated electronics — although even the Serbians learned to turn their radars on and off rapidly, taking quick glimpses instead of long looks to avoid being detected and destroyed. Against modern electronics that can change frequency, modulation and such in fractions of a second, the Navy needs a nimbler approach.

The new concept of operations relies heavily on *passive* detection. All kinds of aircraft, surface ships, and even submarines will have sensors to pick up electromagnetic emissions in their environment and datalinks to transmit what they find. At the receiving end are electronic warfare specialists on Navy flagships — where the battlegroup EW commander is being elevated to the same level as the carrier air wing commander, Farr said — and in the back seat of the EA-18G Growler.

Instead of flying in pairs as the Prowlers did, with both aircraft actively jamming, the Growlers will probably fly in trios, with one plane mostly in passive mode. "When you're jamming, the ability to receive threat emissions is degraded," said Farr. "It's like being able to talk when you've got the stereo turned up to ten." The third, quiet Growler will be better able to detect the enemy — both directly using its own sensors and indirectly using data relayed from other platforms — and then transmit detailed intelligence to the other two EA-18Gs.

EA-18G Growler

(Flying three Growlers at once instead of two requires increasing the number per carrier from five to seven or eight — a major reason the Navy wants to buy more EA-18Gs).

Moving all this data around requires a powerful network. The effort required will be similar to the creation of NIFC-CA, the long-awaited Naval Integrated Fire Control-Counter Air network for anti-aircraft defense, Capt. Gamberg said. "We need machines talking to each other [with] picosecond level timing, but it's going to take us a while," he said.

To create a single electronic warfare network linking everything from subs to drones, Gamberg told me, "the challenge… is bringing all that together, understanding it, controlling it, so you can actually use it. That's a lot of work left to be done."

Colin Clark also contributed to this story.