

## Lightening War

Unfettered digital battlefield combat opposed by intelligence

By David A. Fulghum, Washington

The Pentagon and intelligence agencies are at loggerheads about the rules that will control the unleashing of cyber-counterattack, a mission that could, with more investment, be conducted from aircraft against targets a half-world away.

But before airborne cyber-attack becomes a tactical weapon, resolution must be reached on the relationship between warfighters and intelligence and the authority to decide what is a valid target and what is not.

A unique characteristic of cyberwarfare—that weapons effects cannot be seen and often cannot be verified—means that the operator's location near the battlefield may well become more important. Those implications become increasingly relevant as Congress and the Obama administration are considering the buildup of the U.S. military's cyber-operations headquarters at Ft. Meade, Md.

Aircraft can create anti-electronic effects such as enforcing "cones of silence" on communications in a limited area or pre-detonation of certain types of buried explosive devices. Networks in other countries, or those employed by non-national irregular, criminal or terrorist organizations, can be monitored, tracked and exploited.

But the dividing line between tactical and strategic cyber- or network attack is a battleground between intelligence and warfighting organizations.

The active, electronically scanned array (AESA) developed for long-range, high-accuracy radar also brings radio frequency-injection (data streams of algorithms fired into an enemy antenna) to the battlefield as a weapon. The Radar in the F-22 and F-35 can be used for the task in limited frequency bands. But AESA antennas are being redesigned to cover a far greater frequency range and are expected to be a key element of the U.S. Navy's Next-Generation Jammer, an example of sophisticated electronic attack entering the tactical battlefield.

The heavy hitters in cyberwarfare, such as the National Security Agency, say that any cyber-network attack for the foreseeable future will have to be analyzed for secondary or cascading network effects and approved by Washington and the NSA.

However, such restrictions are often quickly ignored in wartime. During the North Vietnamese army (NVA) 1972 offensive in South Vietnam, the signals intelligence organization at Phu Bai cut a hole in the security fence so they could feed real-time information to an artillery unit next door. They soon were cutting off intercepted NVA command-and-control signals in mid-sentence. That kind of intelligence-tactical cooperation has improved over the years, but it is still spotty.

Now the weapon of interest is cyber-attack instead of artillery fire.

"There is a lot of contractor hype," says a longtime U.S. Air Force airborne electronic attack specialist. "Most of what is described as combining jamming and cyber-attack is nothing more than the subtleties of smart jamming.

"Technology enhancement efforts have been ongoing for many years with retrofits into existing systems and application to the [U.S. Navy's] nascent Next-Generation Jammer program," he says. "The challenge is providing 'mission management' of the multitude of collectors and jammers on the battlefield to avoid electronic fratricide," he says. "Someone has to decide whether it makes more sense to exploit, spoof, jam or kill the signal."

There's another complicating factor: Fewer and fewer airmen, specialized in electronic attack, will be flying over the battlefield.

Aircrews in tactical electronic attack aircraft have dropped from four members in the EA-6B Prowler to two in the EA-18G Growler. Soon the number will drop to one in the F-35 and then to none in unmanned air vehicles and unmanned combat aircraft with an electronic attack (EA) payloads.

"So who is going to be controlling the EA activity?" says Dennis Hayden, director for information operations and electronic attack at Northrop Grumman. The F-35 will be "almost an unmanned [airborne electronic attack] platform. For a pilot [-only aircrew], an expendable [EA] weapon or a UAV, you need some type of coordinated battle management approach. Of course [automated decision aids can be used] from the ground, back home or from a flying platform that are automated [onboard], offboard or a combination."

It is a given that when conducting cyber-attack or exploitation, the best access is through an Internet connection, say advocates of the intelligence-first approach.

"If this nation does Internet attack, the majority of it will be done from Washington and [NSA at Ft. Meade]," says a senior industry executive and former NSA official. "The only time you need to involve the [military] services is when you need RF injection."

That means that a radio frequency signal—specially modified to exploit or damage an enemy network—is packaged in a data stream that is fired into an antenna that is connected to the target network.

"There are some cases where you will need it, but I don't think it will be a major player [except at the] tactical level," he says. "If you are going to attack a computer, it's probably part of a command-and-control system. At least for the short and medium term, that will be engineered from Washington because of the need to deconflict all of those types of attacks [and] understand the effects. While I think the jammer capabilities that the services are developing will potentially be useful [for cyber-operations], I don't think it will be used a lot now."

"The first step in getting to that organizational structure is to decide who's in charge," says Vice Adm. Steve Stanley, director of force structures, resources and assessment for the Joint Chiefs of Staff. "That's what Cyber Command does. We will then take direction from that commander, through the combatant commander, in this case Strategic Command, to define the way ahead."