

Breaking Defense

INTEL & CYBER

US Has Lost ‘Dominance In Electromagnetic Spectrum’: Shaffer

By SYDNEY J. FREEDBERG JR.
on September 03, 2014 at 3:49 PM
40 Comments

533
SHARES



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

533
SHARES



NATIONAL PRESS CLUB: “We have lost the electromagnetic spectrum,” said [Alan Shaffer](#), the [Pentagon’s research and engineering chief](#), this morning. “That’s a huge deal when you think about fielding [advanced systems](#) that can be [countered] by a very, very cheap digital jammer.”

We’ve heard senior Pentagon officials fret about electronic warfare before, most prominently the Chief of Naval Operations, [Adm. Jonathan Greenert](#), but this is the bluntest and most alarming statement yet.

“We have got to, in my opinion, regain some dominance in the electromagnetic spectrum, or at least parity, so things that we buy continue to operate as we intended them to,” Shaffer said. For example, the Pentagon’s biggest program ever, [the F-35 Joint Strike Fighter](#), has much-touted

information technology built-in, but, he told reporters cryptically after his public remarks, “if we don’t really pay attention to the EM spectrum, it is not a good news story for the F-35.”

So what the hell happened? “There is no single answer,” Shaffer said when I asked him at the annual Common Defense (ComDef) conference here. Part of the problem is that the US government has sold off many of radio frequencies it used to own, “for good economic reasons,” he told the audience.

But by far the bigger factor is the global shift from analog to digital technologies, with a proliferation of high-powered, low-cost, commercially available equipment driven by Moore’s Law. The kind of electronic eavesdropping and jamming that used to require a nation-state’s resources are now available to small countries and even guerrillas (as well as to innovators inside the Defense Department). “People are able to create very agile, capable systems for very little money, and those agile, capable systems — if we don’t develop counters — can impact the performance of some of our high-end platforms,” Shaffer said.

What Shaffer didn’t say is that the US military neglected electronic warfare for at least the decade after the Soviet Union fell. After 9/11, radio-detonated roadside bombs triggered a rush to get EW gear to ground troops in Afghanistan and Iraq, but outside that narrow area, investments still lagged. While the Air Force has high hopes for the F-35, it has only a handful of dedicated electronic warfare aircraft left, the EC-130H Compass Calls. The Navy has spent heavily to replace the geriatric EA-6B Prowler with the sleek EA-18G Growler — but to date it’s putting a lot of old electronics in that new airplane: A new Next-Generation Jammer (NGJ) to go on the Growler is still in development.

533

SHARES

Nor has the military taken full advantage of new sensor and communications technology. “We ~~have~~ stayed largely in our standard radar and communication bands,” such as X-band radar, Shaffer said, “while the rest of the world has moved to higher and lower frequency....They’ve gone to broader bandwidth and more agile systems.”

G+

As a result, we have cases where Iraqi insurgents could watch video feeds from Predator drones in because no one bothered to encrypt the signal. While the guerrillas seem not to have made much of the jittery, out-of-context images, a more sophisticated opponent could have mined them for intelligence, jammed the link between the drones and their human operators, or even hacked into the US network.

A leading independent expert on future warfare agreed with this grim picture.

“Shaffer is absolutely correct,” said [Ben Fitzgerald](#) of the Center for a New American Security when I showed him a transcript of the remarks. “Many of the technologies the U.S. uses, GPS for example, don’t use especially strong signals and are susceptible to denial from other systems that are increasingly affordable.”

GPS is arguably the most glaring single vulnerability. While civilians worldwide have come to take the Global Positioning System for granted as part of daily life, the US Air Force still runs GPS, and all branches of the military depend on it for everything from foot patrols in Afghanistan to [smart-bomb strikes in Iraq](#). But GPS jammers are getting cheaper.

“I’d love to give GPS to the Department of Transportation and do precision navigation and timing [PNT] terrestrially,” i.e. without using satellites. “I can’t do that yet,” Shaffer told reporters after his formal remarks, “[but] we’re getting pretty close.” DARPA is leading research on using atomic clocks and other technologies to let military units know exactly where and when they are without having to depend on a [satellite signal](#).

DARPA is doing “good work,” said CNAS’s Fitzgerald, but the technology is not yet mature, let alone ready to affordably retrofit to a host of existing systems.

So, as the civilian world relies ever more on [networks and mobile devices](#), the military is now wrestling with how to keep fighting if the enemy pulls the plug.

533
SHARES

   

533
SHARES

Topics: air force, Alan Shaffer, Ben Fitzgerald, Center for a New American Security, CNAS, ComDef 2014, cybersecurity, drones, EA-18G, electromagnetic spectrum, electronic warfare, Global Positioning System, GPS, navy, networks, next-generation jammer, UAVs



EDITORIAL STAFF

G+

in



Colin Clark
Editor



Sydney J. Freedberg, Jr.
Deputy Editor