The Air Force's reach exceeded its grasp when it tried to take on the entire electromagnetic spectrum.

—Staff photo by Guy Aceto

How Electronic Countermeasures Went Wrong

BY JAMES W. CANAN
SENIOR EDITOR

EIGHT years ago, the Defense Department began thinking bigger than it ever had about electronic warfare (EW). Soviet tactical weapons, radars, and other sensors were becoming more sophisticated and harder to counter at every turn. They threatened to overwhelm the US EW systems then in service. So DoD set out to design and build new EW systems of unprecedented potency and versatility, systems capable of coping with the threats of the moment and for a long time to come.

The idea was sound, but the systems that sprang from it were not. The Air Force sank into an EW morass from which it is just now extricating itself. The story of how this happened goes back many years and is complicated. The stakes could hardly be higher.

To the Air Force, no task is more urgent than seeing its combat aircraft safely through or around enemy air and ground radar networks and enabling the planes to defend themselves against highly sophisticated, hard-to-jam SAMs, antiaircraft guns, and air-launched missiles. Airborne EW systems devised to detect and jam, or otherwise foil, such radars and missiles could well mean the difference between victory and defeat in the electromagnetic milieu of modern warfare.

Unfortunately for USAF, its development of EW systems through this decade has been, for the most part, dismal. Many new EW systems, most notoriously the defensive avionics suite aboard the B-1B bomber, fall short of performance expectations, cost too much, are taking far too long to get into operation—or suffer from all such faults.

Chronic problems with the B-1B's electronic countermeasures (ECM) have claimed the most attention, but are by no means the only ones besetting the Air Force's EW community. New ECM systems for other combat aircraft seem to have gone sour all over the place. Air Force leaders have taken to criticizing the service's EW scheme of things quite openly.

Not long ago, for example, Gen. Bernard P. Randolph, Commander of Air Force Systems Command, singled out the ECM scene for a tongue-lashing, calling it "a disas-

The B-1B's tail section houses the main elements of the bomber's chronically troublesome ALQ-161 defensive avionics system. Too many ambitious programs for developing such EW systems have turned sour for the Air Force in recent years.

ter." With everything to lose as a result of ECM deficiencies, Gen. Robert D. Russ, Commander of Tactical Air Command, has on occasion been just about as harsh.

Now the Air Force is moving to set things right. It seems determined to stick with several problem systems and make them work as well as possible. The B-1B defensive avionics system is one. There are signs of progress in USAF's program-by-program perseverance and signs of hope for the future in its adoption of a more realistic attitude toward EW across the board.

Less Ambitious, More Feasible

USAF is taking a wholly different approach to designing and developing EW systems, one that it sees as less ambitious than its approach of recent years, in which its reach often exceeded its grasp.

Brig. Gen. Noah E. Loy, the director of acquisition for electronic combat programs in the Office of the Secretary of the Air Force, explains. "The Air Force has decided to take an approach to EW that is more doable. We're in the process of refining our EW requirements. We want to make our systems simpler, not more complex. In the past, we have confused some of our goals and strategies with what we thought would be possible in terms of technical solutions. We had a tendency to think we needed a [EW] system in our aircraft that was capable of taking on everything in the electromagnetic environment. We are getting away from that."

The "think big" approach that USAF is turning away from originated in a well-intentioned directive that Richard D. DeLauer, then Under Secretary of Defense for Research and Engineering, sent to the military services in 1981.

In it, Dr. DeLauer noted that the services were in the habit of pursuing "only those EW programs designed against hostile equipment that is already deployed or is well along in development" and that "therefore we are well behind the emerging threat before we start."

He continued: "Using current practices, there is no possibility that we can field the EW capability needed—in time—to counter the changes in the Soviet threat during the next ten years." He advised the services, in planning for EW systems, to begin taking into account "the projected threat, approved by the Defense Intelligence Agency, of estimated future enemy capabilities based on intelligence, extrapolation of existing enemy weapon designs, and anticipated enemy technological advances."

To help do this, the Defense Department forthwith enlisted the services of experts in the US electronics industry. Given access to DIA "threat documents" on Soviet electronic combat capabilities and tendencies, fifty or so key executives of electronics companies joined with top military and civilian EW officials in the defense establishment to form the DoD Electronic Warfare Technical Study Committee.

Nice Try, Little Payoff

The EWTSC bent to analyzing and forecasting Soviet sensor and signal processing technologies and systems—with much emphasis on the radars and infrared guidance systems of Soviet SAMs and air-launched missiles. Meeting at least monthly, its several specialized subcommittees also studied US needs and prospects for EW technologies and systems to counter advances anticipated in Soviet electronic combat capabilities.

This was a highly unusual endeavor. It meant that each company represented on the committee was put in the position of sharing, by virtue of its contribution to the common cause, at least some information about its own electronics technologies. On the other side of the coin, all the companies stood to benefit from the boom times in EW contracting that could be anticipated—and that happened—as a result of the DoD effort.

No one disputes that the EWTSC made a nice try. To this day, industry executives who served on the committee claim that it served a useful purpose. For example, one such executive, Sanders Associates President John Krieck, says the committee's reports "did a great deal to broaden the perspective" of the US EW community on the threat and on the technological possibilities for countering it.

Dr. Krieck also recalls that the EWTSC's assessments of Soviet technology and systems trends were fairly accurate and that its conclusions and recommendations, all of which remain highly classified, were pretty much on the mark.

The committee's work helped to promote the concept of integrating all EW elements in future fighters around a common, high-speed signal processor, a concept that is expected to become reality in the integrated electronic warfare system (INEWS) of USAF's Advanced Tactical Fighter.

For all the committee's sound insights and suggestions, though, the actual payoff from its work has been, to all appearances, disappointing. Programs for new and upgraded jammers, radar-warning receivers, and chaff dispensers across the spectrum of combat aircraft have not panned out or have wound up well in arrears of existing threats by the time they go into the field.

As General Loy explains: "After we changed our way of doing business in 1981, we set a whole bunch of programs in motion. A lot of them were for developing new types of hardware we could build, such as antennas to increase our sensitivity, and expanding RF [radio frequency] bandwidths in the electromagnetic spectrum for detecting threats.

"We were also looking at microchips that could give us the signal-processing capability that we needed to move into a software-intensive environment—to design [digital computer] hardware with enough flexibility to handle the software changes that the threat would impose on us in the future."

It didn't work out. "We ran into troubles," General Loy recalls. The computer hardware developed for new and updated EW systems was not flexible enough, at first, to accommodate the required software. When the hardware began coming around, the software lagged.

"Our software-writing capability did not keep up with the development of the chips," explains General Loy. "The problem with software development basically was that we outpaced the capability of industry and society to produce software people to do the job."

He sums up: "So Dr. DeLauer's memo instituted a cultural change—away from taking specific approaches to countering particular

threats, to looking at the enemy on a broader scale and trying to develop a more generic systems-engineering approach to countering the threat on that scale.

"We were not able to accomplish that."

A major reason was the fallacy of an assumption that the Pentagon and industry made about the advances to be expected in Soviet signal processors. The expectation was that the Soviet military would sooner or later emulate the US military by switching altogether from analog signal processors to digital signal processors in their radars.

This mirror-imaging of projected Soviet systems led to conclusions that those systems would be susceptible to the same jamming techniques and technologies that US systems needed to be protected against.

It didn't turn out that way. The Soviets either were incapable of fully exploiting digital computer technologies or chose not to do so. Although they incorporated some digital technologies, they continued to rely mainly on analog processors, which lend themselves to the incorporation of robust counter-countermeasures.

The upshot was that the hardy analog electronics of Soviet signal processors and ECCM confounded US EW devices and "denied us access into the internal workings of those systems," General Loy explains.

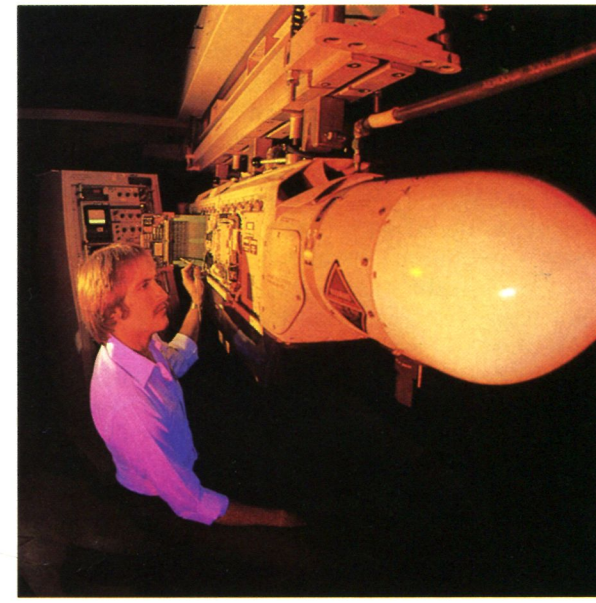
By staying the course with analog processors, the Soviet military also made it virtually impossible for the US electronics industry, which left off developing analog technologies a long time ago, to simulate Soviet systems. This was also a major setback for realism in the testing of US EW equipment and for confidence in validating such equipment as being truly capable of performing as advertised in combat.

Behind the Curve

Capabilities of individual systems aside, the central reason for difficulty in electronic warfare is the very nature of the beast.

Robert W. Selden, Chief Scientist of the Air Force, provides this perspective: "We're operating in a world where the amount of electromagnetic energy is increasing at just an unbelievable rate. In any of the standard scenarios of conflict in central Europe, for example, there are electromagnetic radiations from hundreds if not thousands of radars, thousands of communications systems—radios and other things, even lasers to some extent.

"The sophistication of these systems has increased dramatically. . . . If you want to interfere with any of them you have to build [electronic] machinery that listens, figures out what's going on, and decides what to do about it, all in real time. If anybody wonders why we have trouble today with electronic combat, that ought to explain it."



A Westinghouse ALQ-131 ECM pod is checked out by a company technician. The ALQ-131 is the jammer for a variety of combat aircraft and has been upgraded to meet the contemporary threat.

Dr. Selden adds, "The technology in computing and in the electronic systems that generate these signals and receive them is changing faster than we can put systems into production. . . . If we start today, we're going to have equipment in the field that is responding to a technical capability of a couple of generations ago, maybe more."

This behind-the-curve characteristic of EW equipment is exactly what the Defense Department tried to correct in the forward-looking approach that it adopted in 1981. The built-in resistance of Soviet systems to electronic invasion has been a major frustration for that approach.

A DoD top-priority goal was to design jammers that would be "smart" enough to disrupt electromagnetic emissions in the innards of enemy electronic systems—emissions from signal processors of the radars controlling the missiles, rather than the radio-frequency waves from the antennas of those radars.

In theory there was nothing wrong with that DoD aspiration to "jam behind the faceplates" of enemy weapon systems. Neutralizing a missile before it is launched by jamming its fire-control computer is safer than waiting until after it is launched to try jamming its target-homing seeker.

Says General Loy: "We were trying to deny missile launch, because we knew if the missile never came off the rail, it could never hit us. Now we're going back to the way we used to do it, manipulating the emissions that are radiated from the antenna. But that makes us do something else—create enough 'miss distance' between our aircraft and [enemy] missiles once they're launched. This requirement makes our ATF [Advanced Tactical Fighter] all the more important."

Overoptimism, System Deficiencies

Technical reasons for the woes of US EW systems through this decade are classified as to details. But other reasons abound.

A study conducted for AFSC's Aeronautical Systems Division a few years ago cited Air Force and industry overoptimism about technologies as probably the chief culprit. Among other problems detailed in the study were rampant deficiencies of system integration,

adversarial relations between the Air Force EW R&D community and its contractors, unrealistic cost ceilings, and debilitating cost/performance tradeoffs.

In one way or another, overoptimism may well have contributed to all the others. At any rate, the findings of the study apparently were a major reason for the subsequent reorganization of ASD's EW shop at Wright-Patterson AFB, Ohio, and the start of something new there.

Last year, the Air Force Electronic Combat Office went into business at Wright-Patterson. A prime goal of AFECO is consistency and balance in the business of developing and acquiring EW systems. Not long ago, an AFECO official was quoted as saying that the Air Force is "trying to do a better job of defining an executable program" in EW and that its previous inability to do so was "one of the common denominators of a failure we've seen in the past."

For whatever reason, all manner of Air Force EW programs fell by the wayside or limped along through this decade. Each was seen as necessary to counter the threat that now looms in the European theater, to say nothing of the threat that may be in store there. The threat is building elsewhere, too. Sophisticated radar and infrared weapons built by the US, the Soviet Union, and their respective allies have been on the rise in the Third World for quite some time. A recent example was Libya's purchase of late-model Soviet fighters with topnotch radars and ECM.

Among unclassified Air Force programs that were devised to meet the threat but that got the axe were those for an "advanced capability" jamming pod and a multipurpose EW Area Reprogramming Capability. Also canceled were the Precision Location Strike System (PLSS), the F/FB-111 internal jammer upgrade program, and directional receiver antenna signal processors for F-4G Wild Weasel aircraft.

Radar warning receivers for fighters and attack aircraft seem to have fared better, by and large, than jammers. New RWRs for the F-15 and the F-111 are finally looking good for production, their bugs having been worked out, but a new, much-coveted RWR for the F-16 is on hold.

Plagued by Delays

Delays have plagued two highly important EW endeavors: strengthening and broadening the EF-111A Raven's area-jamming system by means of a more powerful radar and communications jammer and bringing to fruition the long-coveted Airborne Self-Protection Jammer (ASPJ). One program made out better than the other.

The EF-111A update program fell two to three years off the pace and was finally called off. Its demise probably did as much as anything else to raise the ire of the Air Force leadership about the service's EW state of affairs. The reasons are that the ECCM systems of Warsaw Pact forces have become alarmingly powerful and that the radars of those forces now sport such jammer-daunting features as single-pulse, or "monopulse," radars operating at extremely dense pulse rates, or frequencies.

The possibility that the Raven's EW prowess won't be enough in the clutch is very worrisome. In combat, the Raven could be the franchise for US forces. It could be called on to screen US and allied penetrating attack aircraft by jamming enemy ground control intercept radars and SAM and AAA gun radars from standoff range; to penetrate alongside bombers and fighter-bombers and jam the early-warning and acquisition radars seeking them out; to fly near battlefronts and shield close air support aircraft from antiaircraft radars while the planes go after tanks; and to screen aircraft that are forming up or doing radar-surveillance missions in friendly—but potentially perilous—skies.

The ASPJ was once seen as jamming just about all things for all aircraft. But that was a while ago. The jammer has been so long in the making that it may be past its prime against today's threats even as it enters the field.

As far back as 1978, the Defense Department asked companies with expertise in electronic warfare to propose designs for the ASPJ. It will be yet another couple of years before the system goes operational in significant numbers.

Destined for deployment on Air Force and Navy fighters, the ASPJ was seen in the beginning as the first ECM system to take full advantage of the technological revolution in microelectronics. It was designed to embody multiple, programmable microprocessors to make it capable of countering an unprecedented variety of anticipated threats from SAMs and air-to-air missiles. Extra capacity was built into it to enable it to accommodate new technological features as time went by.

Compactness was a major aim. The ASPJ was designed to combine a number of ECM technologies into one miniaturized system of microprocessors, receiver, amplifier, and wide-band and narrow-band transmitters that would take up only 2.3 cubic feet inside an aircraft.

The Pentagon's high hopes for the ASPJ in the late 1970s as a first-rate now-and-future jammer marked the beginnings of the starry-eyed EW policy that DoD would put in place in 1981.

The Westinghouse-ITT team of prime contractors for the ASPJ has done a good job, by all accounts. But the jammer has been slow in coming for a number of reasons—some of them, such as funding fluctuations, beyond the control of its contractors—and is only now on the verge of low-rate production.

Given its long gestation and growing pains, will the ASPJ be capable of standing up to the Soviet ECCMs and jamming the Soviet weapons that have come into play since it was designed? "I think ASPJ will do the major things we need it to do against the threat it was designed against," says General Loy. "We're finding there are some shortcomings in the [ASPJ] system as the threat changes. However, we expect to fix the shortcomings through a product-improvement program."

B-1 Shortcomings

There are shortcomings galore in yet another major EW system that USAF seems stuck with—the defensive avionics suite on the B-1B bomber. The Air Force will do its best to bring that ALQ-161 system up to snuff, but admits that it will probably never be as good as it ought to be.

The ALQ-161 got off to an uncertain start in the mid-1970s, marked time after the original B-1 bomber program was called off in 1977, and was caught short on technology

when the bomber was revived as the B-1B in 1981. It was designed to meet the Soviet threat as sized up by DIA in 1974, and it was the first defensive avionics system ever designed to be totally integrated aboard an aircraft.

The ALQ-161's merits began to look dubious as the Soviet threat rapidly worsened and the integration of the system became ever more challenging. To make matters worse, the capability of the system was cut back to compensate for architectural problems and unexpectedly high development costs.

In 1981, the Air Force moved to upgrade the ALQ-161 to bring it abreast of the threat and orient it to future threats. The system's receiver architecture was revised to accommodate new techniques and hardware components that USAF decided it had to have. That decision was based on the results of USAF's manned bomber penetrativity evaluation of the late 1970s and 1980.

In the MBPE, pulsed-Doppler radar developed for USAF's F-15 fighter—and thought to be in the works for Soviet fighters, too—was "flown" against ALQ-161 architecture, which was found wanting. For this and other reasons, USAF drastically raised the "sensitivity requirements" of the system's receiver.

"So we added new [EW] techniques and the hardware needed to produce those techniques on top of the old architecture that had never been fully developed," General Loy explains.

"We felt we could do that, given new computer technology. We also added a new computer and put a new high-order software language into the system.

"The bottom line is that we added a lot of new stuff on top of an old system and tried to complete the development as a total system. We have not been able to develop that system to the full goal that we set down."

The computer-oriented system's major problem is one of hardware, not of software. Says General Loy, "Software cannot fix the hardware deficiencies and limitations built into the system from a previous design. The basic receiver was designed from 1974 through 1978, and we assumed it was good—even though we never had completely developed or tested its architecture—when we added the new capabilities that were required."

Problems brought on by such additions "plague all our systems in some ways, although not as much as they do that one [the ALQ-161]," General Loy says. The reason is that the other systems—for example, jammers on the F-15, F-111, and B-52—had been more thoroughly developed before undergoing modifications.

"All of them were designed to handle basically the same kinds of older threats dating back to 1970. What we tried to do was elevate them to meet the new threat capabilities," General Loy explains.

—Staff photo by Guy Aceto

An EF-111A Raven EW aircraft is groomed for an area-jamming mission. Failure of the vital Raven upgrade program has evoked harsh criticism of USAF's whole EW scene.

Avoiding or Defeating the Threat?

Notwithstanding arms-control measures and negotiations, those threats are getting worse all the time. In this decade alone, Warsaw Pact forces have put into the field ten new SAM systems. Those forces are now said to have deployed more than 700 EW aircraft, 10,000 intercept radars, 4,000 fighter/interceptor aircraft, 12,000 radar-controlled AAA systems, and 13,000 SAM systems.

Despite its disappointments in EW, the Air Force will keep working on new jammers and new weapons, such as antiradiation missiles and the Tacit Rainbow radar-homing drone and others, to defeat the threat. But defeating the threat may no longer be the name of the game in electronic warfare.

Right along, EW is becoming synonymous with avoiding the threat instead, through tactics and by means of such stealth technologies and platforms as the F-117A fighter now in service in limited numbers, the Advanced Cruise Missile, the B-2 bomber, and, later on, the ATF and USAF's variant of the Navy's stealthy A-12 attack aircraft.

"We've had a tendency to think that defeating the threat is the only capability we should be pursuing in electronic warfare," says General Loy. "There are other capabilities that will let us get in there. The avoidance capability, with stealth, is a major one. And once we get into stealth in numbers, we can never go back. We will have changed the playing field permanently."

As an admittedly disastrous decade in electronic warfare comes to a close, the biggest challenge before the Air Force may well be its urgent need to decide on the best blends of weapons and other systems for defeating, degrading, and avoiding the enemy threat. This, says General Loy, is "why it is so important for us now to get hold of our requirements process," wherein USAF makes just such decisions.

The heavy betting is that the Air Force will more and more come down in favor of stealthy systems, such as the ATF, that can do all those things to one degree or another. ■