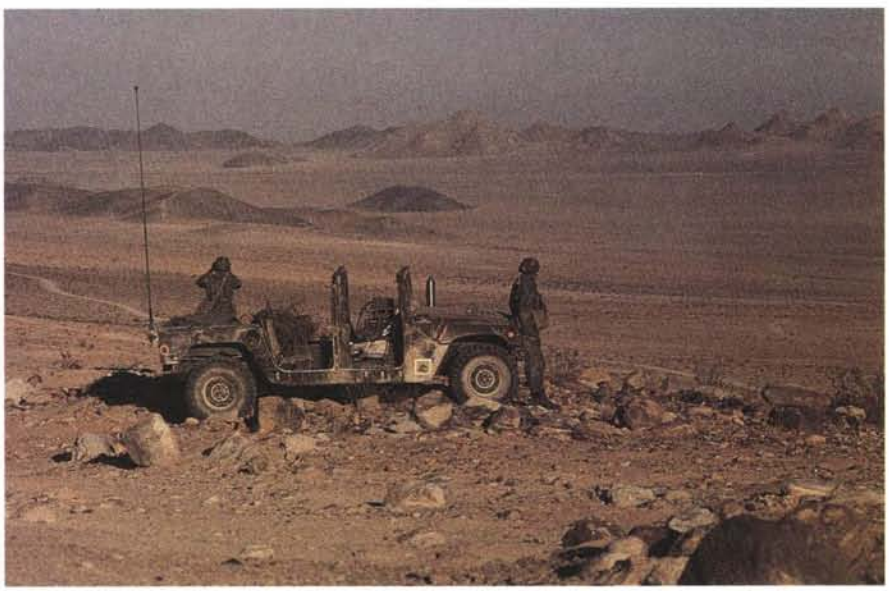
Global Positioning System technology was too phenomenal for the Air Force to keep a monopoly on it. In wartime, that will make an enormous difference.

GPS in Peace and War

By Peter Grier



Staff photo by Guy Aceto

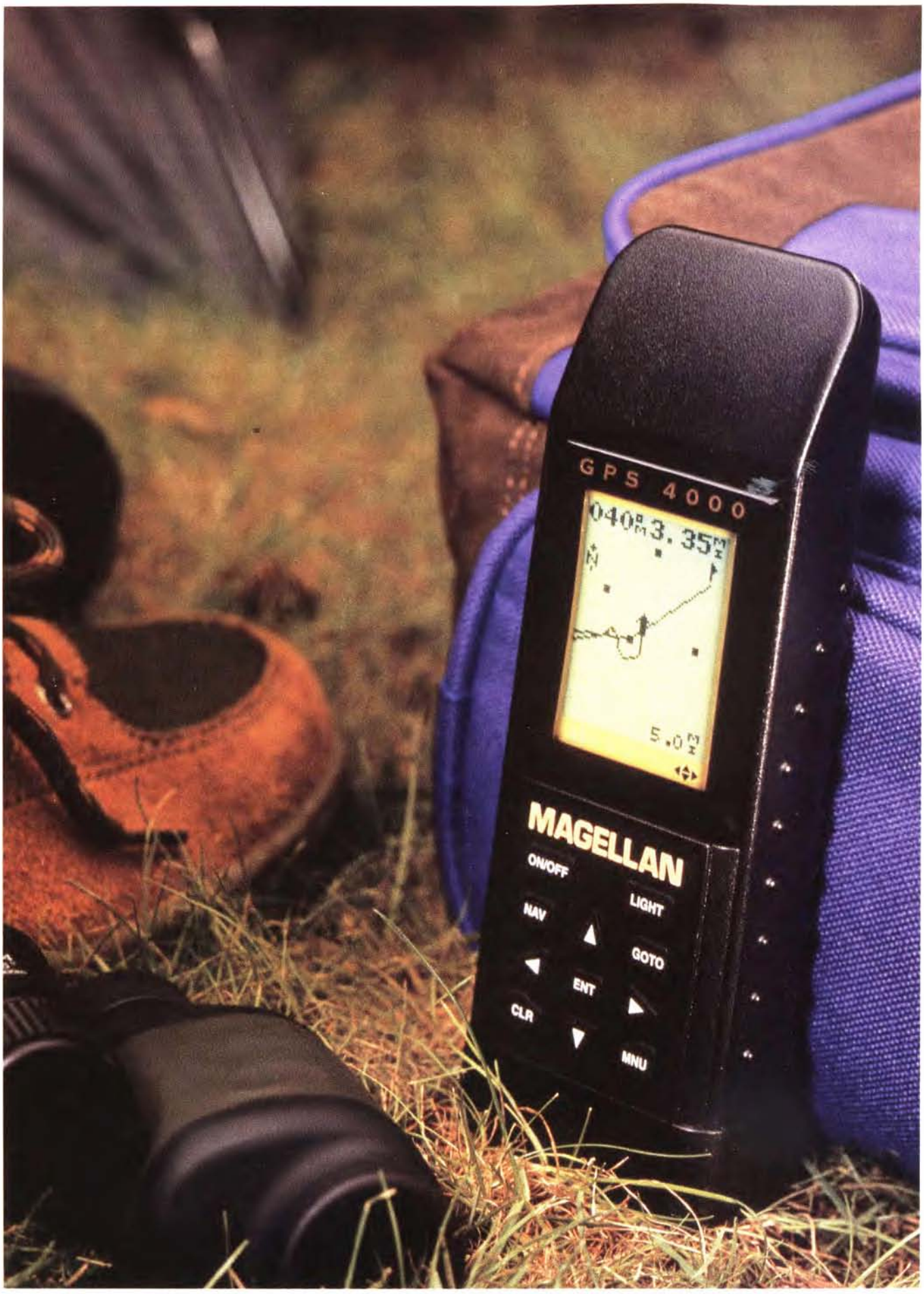
Both soldiers on maneuvers in the trackless desert and weekend hikers in the Adirondacks depend on GPS technology to tell them exactly where they are. The US must now find a way to ensure that its troops have the most accurate, secure, positioning information while denying such data to potential enemies.

THE USAF Global Positioning System is one of the most successful high-technology projects ever produced by the Defense Department. Signals from the twenty-four orbiting satellites that make up the GPS constellation now provide precise time and location data for all manner of US military forces—from troops creeping through unknown landscapes to precision guided munitions speeding toward their targets. Reliance on GPS will only increase in the years ahead. Congress has promised that after 2000 it will cancel production of any aircraft, ship, or armored vehicle not equipped with a GPS receiver.

To some extent, however, GPS now risks becoming a victim of its own success. The commercial market for its services has exploded faster than anyone had predicted—complicating national decisions about the system's control and use. Potential adversaries may be plotting to take advantage of global positioning data, having seen the power of GPS demonstrated by US forces during the Persian Gulf War.

Thus, it is no longer enough for the Pentagon simply to deny other users the most accurate signals produced by GPS satellites, according to a new RAND Corp. study. The Air Force and other services need to start thinking—now—about how they will handle the inevitable proliferation of global positioning information.

"The United States must begin preparing to operate in a world where access to GPS-type and augmented


GPS 4000
MAGELLAN
ON/OFF
LIGHT
NAV
GOTO
ENT
CLR
MNU

GPS services are the norm," says a new RAND study of GPS produced for the White House Office of Science and Technology Policy.

For one thing, that means planning defenses-in-depth against attacks by GPS-guided missiles. It also means devising ways to protect US global positioning assets. Attacks on such vital data providers could well be a facet of a coming age of information warfare.

"The overall magnitude of [the] threat appears manageable, provided that the United States proceeds prudently in preparing an array of defensive measures," concludes the RAND report.

Three Systems

Operated by the US Air Force, the Global Positioning System was developed over two decades at a cost of around $10 billion. It reached its formal initial operational capability on December 8, 1993, though its fledgling satellites had already been providing useful positioning information for years.

Technically speaking, the GPS is not one system but three.

The first is a constellation of twenty-four Navstar satellites orbiting Earth in six different planes, spaced so a user on the ground will typically have access to the signal from a minimum of five different "birds."

The second is ground control, consisting of a master control center at Falcon AFB, Colo., and unmanned monitoring stations in Colorado Springs, Hawaii, Ascension Island, Diego Garcia, and Kwajalein.

The third system consists of users, whose GPS receivers convert raw signals from the satellites into position information.

The GPS satellites are in essence extremely accurate clocks in the sky. They broadcast precise time information toward the ground via coded radio transmissions, which are picked up by equipment ranging from handheld receivers to units mounted in aircraft or on guided weapons. The receivers calculate how long it has taken them to receive the radio pulses from different GPS satellites—and use the barely perceptible differences in time to figure out their position on the face of the Earth.

In fact, GPS satellites broadcast two different kinds of time signals. The first is the Coarse Acquisition signal, or C/A-code. Designed for nonmilitary users, it provides position information accurate to about 100 meters. The second signal is the encrypted Precision signal, or P-code. Intended for US military or other authorized recipients, it is accurate to within twenty meters.

The Pentagon has long worried that the easily obtainable C/A-code might someday be picked up by adversaries and used against the US. Thus, GPS satellites already intentionally degrade the commercial signal, using a dithering technique called Selective Availability (S/A). Without S/A dilution, the C/A-code would be much more accurate than it is; during the Gulf War, however, the Pentagon turned S/A off so troops would be able to take full advantage of commercially bought receivers many brought with them or received from their families.

Tens of thousands of commercial receivers are undoubtedly still in use throughout the US military. They are small, readily available, and cheap. Given continued budget cuts, officials will undoubtedly be tempted to rely more heavily on off-the-shelf GPS equipment in the future.

A Bad Idea

RAND experts judge this to be a bad idea—for security reasons as well as accuracy. The more commercial equipment used by US military forces, the greater the internal pressure to turn S/A off permanently will be. More important, the less accurate and less sophisticated C/A-code could become a victim of future electronic warfare. "US forces relying on the C/A-code will be much more vulnerable to jamming than those using the P-code," says the RAND report.

Commercial considerations, however, will inevitably figure in GPS's future. Since its beginning as a solely military system, it has grown into perhaps the most successful dual-use technology program of its age, with GPS signals serving a wide array of civil and scientific purposes. GPS guides airliners and helps control the Internet; it keeps rental-car users from getting lost and helps farmers navigate their own fields. The market for civilian GPS use is about three times bigger than its military counterpart, and growing fast. An industry council predicts that by 2000, sales of commercial GPS equipment will generate $8.5 billion a year.

Striking a balance between national security and the needs of industry has thus become a prime problem for Air Force GPS officials. In the past, much of this debate has centered on S/A accuracy degradation. Civil aviation users, among others, have called for S/A to be scrapped, in the face of opposition from the military services. But the civil-military GPS debate may soon include another, equally contentious subject: commercial augmentation of the standard GPS signal.

Augmentation services can provide commercial users with greater accuracy than they can receive from GPS alone—in some cases, as precise as within five meters. A technique called local-area differential GPS (DGPS) is the most common such booster. It works by using a base station whose location is precisely known to beam an additional signal to GPS users.

Current DGPS services are limited to relatively small areas and are used for such purposes as marine navigation. Their augmentation signals are broadcast on the FM-subcarrier portion of the radio spectrum, or over phone lines, and are typically usable only by fee-paying subscribers.

Commercial access to DGPS is likely to expand greatly in the years ahead, raising real security issues for the Pentagon. The FAA, for instance, is planning a wide-area augmentation service that would include broadcasts from geostationary satellites. Eventually, these add-on systems may enable adversaries to have position information as accurate as that available to US forces using military-specification equipment.

The availability of local- and wide-area DGPS is beginning to erode the protections provided by S/A degradation, according to RAND. The US and its allies need to plan for the emergence of DGPS-guided weapons. The Pentagon might also work to discourage other US agencies or friendly nations from providing wide-area GPS augmentations beamed from space—at least for now.

"Time is needed both to develop electronic countermeasures and negotiate international agreements" on DGPS control, concludes RAND.

Hostile Exploitation

Hostile forces could exploit GPS signals in a number of ways. They could use location data for guidance of ground forces, as the US does. They could use the data to aid in warship location or aircraft navigation. The most threatening use of intercepted GPS signals, however, would probably be to increase the accuracy of air-delivered ordnance or ballistic and cruise missiles. "While such [uses] are currently out of reach for most Third World nations, their basic building blocks will be in the hands of several countries fairly soon," says the RAND study.

The notoriously inaccurate Scud missile, for instance, is one weapon system that could be made more deadly by an infusion of GPS technology. According to RAND calculations, adding basic GPS guidance to a Scud derivative or a version of North Korea's No Dong 1 could improve overall missile accuracy by twenty to twenty-five percent.

This figure would be little changed if the Pentagon turned off S/A and allowed easy access to the unaltered C/A-code, say RAND scientists. That is because so many other factors are involved in missile guidance that a more accurate GPS reading would make little difference.

The situation is the same for cruise missiles. A GPS-aided cruise missile could be a significant threat to US forces—particularly if outfitted with a warhead containing biological or chemical weapons. But it is the basic GPS signal itself, not its most accurate manifestation, that would provide aggressors with the greatest benefit.

Thus RAND judges GPS to be a facilitator, but not a driver, of missile proliferation. The military threat posed by the US GPS system must be seen in context, says RAND. Few nations have the potential to make real use of GPS in the near- to mid-term, and most of these are US allies. GPS-guided missiles are a real tactical threat, but not necessarily a strategic one, particularly if the US proceeds with upgrades to the Patriot missile defense system and other planned defensive moves.

Overall, the use of GPS guidance could help an adversary place US lives and property at risk. "However, these forces' ability to destroy critical national assets is marginal, and the likelihood that they will either prevent the United States from winning a [regional conflict] or threaten the survival of the United States itself is quite low," judges the RAND report.

One implication of the RAND findings is that S/A is becoming an increasingly questionable defense technique. Much of the benefit of GPS is realized simply through access to the basic signal. Meanwhile, more accurate augmentation services are spreading around the globe.

RAND does not go so far as to recommend that S/A be abandoned. A decision on whether to turn S/A off in the future should be made by US officials only after development of GPS countermeasures, says the think tank's report.

Electronic Defense

Offense is not the only way adversaries could wage GPS war. They could also play electronic defense by jamming GPS signals and preventing the system's use against them. Current GPS transmissions can be easily disrupted by both intentional and unintentional interference.

The vulnerability stems from the relative weakness of the GPS signal and the susceptibility of many receivers to electronic attack. Tests show that a one-watt jammer can drive a commercial GPS receiver haywire at a distance of twenty-two kilometers—and large numbers of small jammers can be hard to find and destroy. Even a 1,000-watt jammer can be miniature enough to be man-portable.

The first step in fighting GPS jamming may be to purge the military, as much as possible, of commercial receivers. The second is to increase the sophistication of milspec GPS equipment. Currently, military receivers work by first acquiring the C/A-code, then jumping over to the encrypted P-code. RAND recommends that they be designed to acquire the P-code directly, as it is much more difficult to block than its C/A counterpart.

Antenna improvements could provide an additional antijam margin. RAND also suggests equipping each advanced GPS receiver with its own inertial navigation system (INS), to provide some location data in case of loss of signal.

"It is clear that the use of GPS for military applications is extremely vulnerable to jamming without a design that includes additional antijam enhancements and an adequate INS to ensure graceful degradation after loss of GPS," says the RAND report.

Adding INS capability could be expensive, however. An aircraft-navigation-quality INS unit can cost upward of $100,000.

US forces also may need GPS jammers of their own. A future adversary could depend on commercial GPS receivers; therefore the Pentagon "should ensure it has adequate electronic countermeasures to selectively deny GPS, GPS augmentations, and [similar] signals to an adversary," recommends RAND.

In the end, Pentagon planners might wish that GPS had remained entirely under their control, without interference from commercial users or allies, but the time when GPS could be thought of as a purely military system is long past, concludes RAND. The commercial benefits are obvious, and the commercial market is too big. In addition, GPS is a strong example of US technical and scientific leadership at a time when the global economy is increasingly competitive.

The threats from relatively open access to GPS signals can be managed through cooperation with allies and appropriate international bodies, conclude RAND experts. The US government also needs to do a better job coordinating the views of the various bureaucratic stakeholders in the system, from the Department of Defense, to the FAA, to members of Congress. "The United States should issue a statement of national policy, perhaps a Presidential Decision Directive, on the Global Positioning System to provide a more stable framework for public- and private-sector decision-making," concludes the RAND report. ■

Peter Grier, Washington bureau chief of the Christian Science Monitor, *is a longtime defense correspondent and regular contributor to* Air Force *Magazine. His most recent article, "New World Vistas," appeared in the March 1996 issue.*