Advanced military receivers using the sort of modern multi-channel, multi-constellation capabilities already available commercially, could enable the Air Force to focus its anti-jam efforts on the ground, simplifying future GPS satellites and lowering their cost. Moreover, experts told *Inside GNSS,* the cutting-edge receivers could be deployed years before the anti-jam capability planned for the new GPS III satellites would be fully available.

Military GPS Receiver Advances Could Help Trim Satellite Costs

DEE ANN DIVIS

"Space is going to be a contested place," explained one source, who, like several others experts, spoke on condition of anonymity to be able to discuss the issue. "If I have receivers that can receive [any GNSS signal], what does it matter that you take out my GPS? It doesn't matter if it's one (GPS satellite) . . . 10 . . . all of them. So, it's degraded for a period. Does that mean I can no longer operate? The answer is 'No.' I can still operate."

Lt. Col. Andrew Zinn, chief, GPS Plans and Requirements, for the GPS Directorate, says adding signals from other constellations to the military's mix of positioning, navigation and timing (PNT) data was being considered under Gen. Hyten's Space Enterprise Vision, a plan to improve the overall resiliency of the Defense Department's space assets.

"Although it was not yet clear how the overall GPS program might be incorporated into the Enterprise Vision," Zinn told the May meeting of the PNT Advisory Board, "one of the things that we are going to continue to improve our resiliency to jamming and spoofing."

Frequency diversity is critical for the future, the expert said, adding that there has been a push "for a long time to have multichannel user equipment to include M-code. The capability exists today."

"The Air Force is considering bringing Galileo into military-issue receivers," confirmed Todd Humphreys, a GPS spoofing expert and associate professor at the University of Texas at Austin. "They don't consider it for today, but they are looking several years out and saying 'Yes, we should be doing that.'"

However, the technology advances go well beyond just tapping other GNSS signals and include antennas with greater anti-jam protection and internal receiver processors that can compare signals and drop suspicious ones from calculations. The capabilities, of which some already have been demonstrated, would boost resistance to jamming and spoofing as well as overall resiliency and could be fielded in the near-term, several sources agreed.

Sooner, Not Later

"Let's run the math in terms of chronology," said another expert familiar with the tradeoffs. "The first of those satellites, where we are now, there will be none of those satellites launched before 2020 or 2022— even if they just go ahead and say, 'We're going to do it.' And if the first one is launched in 2022 — at the rate of two, or at the most three, say two and a half [satellites launched] a year — how long does it take to get to, let's just say, 20 [satellites]? That takes another 8 to 10 years. And then you have to field the user equipment, because there'll probably be some differences. In my opinion, there's no way you could get such a system fielded before about 2032."

The long lead time to fill out the constellation means the system will be out-of-date by the time it's completed around 2035, said the first expert. By the time the satellites are in place, he said, "the stuff that's on the ground is going to so far exceed that [capability] it doesn't matter."

You could take the money now planned for satellite-based anti-jam capabilities and invest it instead in further improving user equipment, suggested the second expert.

"If you really want jam resistance, we know how to do it," the source said. "You can start fielding it in probably three or four years and . . . it will work for all the signals you already have."

Dee Ann Divis has covered GNSS and the aerospace industry since the early 1990s, writing for *Jane's International Defense Review,* the *Los Angeles Times, AeroSpace Daily* and other publications. She was the science and technology editor at United Press International for five years, leaving for a year to attend the Massachusetts Institute of Technology as a Knight Science Journalism Fellow.

More Spoof-Proof

Approving the capability of U.S. military receivers to use other constellation's signals would also step up those devices' ability to defeat spoofing.

"There's always an anti-spoofing benefit to bringing in all the signals in the sky," said Humphreys. "With the latest Broadcom chips we can bring in GPS, Galileo, GLONASS and BDS (BeiDou). That makes a spoofer's job four times harder than if it was just GPS. . . . And crosschecking between all those constellations helps quite a bit."

Relying only on the encrypted M-code to thwart spoofers is ill advised, he said.

"I have a really dim view of M-code," Humphreys told *Inside GNSS*. "I think M-code is doubling down on an antiquated idea and brings with it a lot of the same challenges as the legacy PY code."

In fact, M-code is vulnerable to a replay attack, he said, one of the simplest of all of spoofing attacks.

"It doesn't matter that it's encrypted, it's still vulnerable," said Humphreys.

A replay attack, he explained, involves recording the encrypted signal and then sending it, delayed, to a military receiver, thereby distorting the timing, or sending it from a different location, throwing off the target receiver's positioning solution.

"I just find it marvelous that the military has chosen the most expensive defense, in terms of all the defenses you could put together for anti-spoofing, " Humphreys said, "and it's the one that's vulnerable to the least expensive attack."

A paper by Humphreys and Mark Psiaki, a Cornell University professor of mechanical and aerospace engineering, entitled "GNSS Spoofing and Detection," will be published in a forthcoming issue of *Proceedings of the IEEE*. The paper describes a variety of spoofing attack methods and defenses against them and includes an attack/defense matrix (see table on page 25) that documents which defense techniques are effective against the various attack techniques.

"There are many effective defenses for civil and military users to choose from," Humphreys says. "None of the defenses are water-tight, but by layering two or three defenses, you can have formidable resistance against spoofing. . . . So, they are, quite rightly in my view, exploring new waveforms and new techniques that will improve the security of civil and military GNSS alike."

Cutting Costs

But it is the anti-jamming capability of the new receivers that may have the most programmatic advantages.

"There's a whole group of people who say it's cheaper to put [anti-jam] on the satellite than it is to put it in user equipment. That's not a true statement anymore," said the first expert, who acknowledged that receivers had improved far faster than expected. "When I've got a $1.98 chip that can do all this stuff, why in the world would I want to spend millions of dollars to put it on orbit?"

If you can achieve anti-jam capability in the receivers, you can forego putting spot beams on the satellites, the experts agreed. Spot beams are directional antennas that boost the power of the signal on the ground. They have been planned for GPS III for some time as a way to surge signal power on a regional basis and help break through jamming. Zinn said that the GPS Directorate is now considering a new requirement for a successor to the spot beam approach called Regional Military Protection.

But the capability to boost the power of the signal from orbit comes at a cost

"For every watt that you put on the Earth you have to generate three watts in space," explained a third source familiar with the program. Batteries and solar panels will be required and the additional heat that will be generated must be dealt with.

Ditching the spot beams could "easily" save $10 million per satellite, the expert said.

If dropping the spot beams also means the satellites can be made smaller, potentially even more could be shaved off launch costs, perhaps with dual launches. That's when you get into real money. The cost of a launch on SpaceX is less than $100 million, according to a recent report in Space News. The cost of a launch on a rocket from the Boeing-Lockheed joint venture, United Launch Alliance, which has lofted the most recent GPS satellites, is more than $350 million.

The Air Force recently awarded Boeing, Lockheed Martin, and Northrop Phase 1 production readiness feasibility assessment contracts for GPS III satellite 11 and beyond. One of the GPS specialists who spoke to *Inside GNSS* said the receiver advances had triggered a re-examination of what those contractors may ultimately be asked to do.

"It (the spot beam antenna) will be dropped," said the first expert. "It's just a matter of time.

Congressional 'Help'

To tap the full potential of the new receivers, said one of the sources, it is essential that Congress not deny the U.S. military the ability to use other nation's signals or to require that it only use signals incorporating the M-code.

Although the view of the Senate Armed Services Committee about foreign PNT signals is unclear, as it has yet to publish the details of its version of the National Defense Authorization Act for Fiscal Year 2017 (NDAA), the House Armed Services Committee (HASC) has already weighed in. In fact, House lawmakers have proposed a trio of directives for Department of Defense (DoD) officials in the report it published to accompany its version of the NDAA, which, at press time, was going before the full House for a vote.

Among those instructions is a mandate for the secretary of defense to ensure that the Armed Forces and each element of the Department of Defense not use signals from a "non-allied positioning, navigation, and timing system or a service provided by such a system." This would certainly block utilization of signals from Russia's GLONASS satellites or the emerging Chinese BeiDou Navigation Satellite System (BeiDou) constellation.

Even so, the Pentagon would have more that just GPS and Europe's still incomplete Galileo network with which to work. For example, it could still tap the capabilities of Japan's QZSS (Quasi-Zenith Satellite System), which covers much of Asia.

The "non-allied" restriction is itself limited and sunsets on September 30, 2018. The defense secretary may also

TABLE I: Cost-Ranked Matrix of GNSS Spoofing Attack and Detection Techniques

Detection Techniques	Attack Techniques												
	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13
D1	X	X	X	X	X	X	X	X	X	X	X	X	X
D2	~	✓	X	X	~	X	X	X	X	X	X	X	X
D3	~	~	~	~	~	X	X	~	~	~	~	X	X
D4	~	✓	~	~	~	~	~	~	~	~	~	~	~
D5	✓	✓	✓	✓	✓	~	~	✓	✓	✓	✓	~	~
D6	X	✓	✓	X	X	✓	X	✓	✓	X	X	✓	X
D7	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D8	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D9	~	✓	✓	✓	~	✓	✓	✓	✓	✓	~	✓	✓
D10	✓	✓	✓	✓	✓	✓	✓	✓	~	~	~	~	~
D11	✓	✓	✓	✓	✓	✓	✓	X	~	~	~	~	~
D12	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~
D13	X	✓	✓	~	X	✓	~	✓	✓	~	X	✓	~

Detection probability matrix keys: ✓ – high, ~ – intermediate or case-dependent, X – low

	Detection Techniques Key		Attack Techniques Key
D1	Pseudorange-based RAIM	A1	Meaconing, single RX ant., single TX ant.
D2	Observables and RPM	A2	Open-loop signal simulator
D3	Correlation function distortion monitoring	A3	RX/SP, single TX ant., no SCER
D4	Drift monitoring (clock offset, IMU/position)	A4	RX/SP, single TX ant., SCER
D5	Observables, RPM, distortion, and drift monitoring	A5	Meaconing, multi. RX ants., single TX ant.
D6	NMA*	A6	Nulling RX/SP, single TX ant., no SCER
D7	NMA* and SCER detection	A7	Nulling RX/SP, single TX ant., SCER
D8	Delayed symmetric-key SSSC*	A8	RX/SP, single TX ant., sensing of victim ant. motion
D9	NMA*, SCER detection, RPM, and drift monitoring	A9	RX/SP, multi. TX ants., no SCER
D10	Multiple RX antennas	A10	RX/SP, multi. TX ants., SCER
D11	Moving RX antenna	A11	Meaconing, multi. RX ants., multi. TX ants.
D12	Dual-RX keyless correlation of unknown SSSC codes	A12	Nulling RX/SP, multi. TX ants., no SCER
D13	Symmetric-key SSSC* [e.g., P(Y) equiv.]	A13	Nulling RX/SP, multi. TX ants., SCER

* Detection techniques requiring changes to the Signal In Space (SIS); TX: Transmitter; RX: Receiver; RX/SP: Receiver-Spoofer

From "GNSS Spoofing and Detection," by Todd Humphreys and Mark Psiaki, *Proceedings of the IEEE,"* 2016

waive the prohibition before then if he or she determines it is in the national security interest of the United States and notifies Congress of this assessment.

Lawmakers also asked for more information on the use of non-allied systems, directing the secretary of defense, chairman of the Joint Chiefs of Staff, and the director of national intelligence to report on any risks to national security or to the operations and plans of the Department of Defense from using foreign PNT.

HASC also wants a separate report on the benefits of incorporating Galileo's PNT signals, particularly the encrypted Public Regulated Service (PRS), benefits that are being held in limbo. This effort is complicated by the fact that the Europeans have not issued a formal specifications document for PRS, according to sources familiar with proposal.

"The committee is aware, the House wrote, "that the National Space Policy of the United States of America directed the United States to 'engage with foreign GNSS [global navigation satellite system] providers to encourage compatibility and interoperability, promote transparency in civil service provision, and enable market access for U.S. industry.'"

Waiting for FCC Approval

Official use of a non-U.S. satellite navigation system in the United States, however, requires authorization from the Federal Communications Commission (FCC), which the European Commission (EC) requested in October 2013. Most of the steps for approval have been completed, but the process bogged down over a year ago. The EC is waiting for the FCC to post the application for public comment.

HASC wants a report from the secretary of defense, in coordination with the chairman of the Joint Chiefs of Staff, outlining the national security benefits that the DoD would expect from approval of the EU request and, interestingly, "any other matters they deem relevant."

Finally the House Armed Services Committee also expressed its concern about the potential for the U.S. Department of Defense to be come dependent on non-allied PNT systems and, much more broadly, on systems that use those PNT systems.

To prevent such dependence, the HASC included in its NDAA report a provision prohibiting the use of such systems beginning in fiscal year 2017 — that is, starting on October 1 of this calendar year. Lawmakers also want the secretary of Defense, chairman of the Joint Chiefs of Staff, and director of national intelligence to submit an assessment of the risks of using such systems.

The HASC also directed DoD's chief information officer to brief both the House and Senate Armed Services Committees on the extent to which the U.S. military uses "either the Russian Federation's Glonass or the People's Republic of China's Beidou Global Navigation Satellite System or telecommunications systems that rely on them, and potential impacts of prohibiting use of such systems."

Putting limits on the number and source of signals is a huge mistake, said one of the experts, who argued that having more signals is better, especially since spurious signals could be identified and ignored by the new receivers.

"Don't allow Congress to close the door on all of this other capability that is available to everybody but you," the source said. "Why is it you want your potential enemies in the future to have greater capability than you do?" IG