OVERVIEW OF GPS INTERFERENCE ISSUES

Statement Delivered
to the
Conference on GPS Interference and Mitigation Techniques
at the
John A. Volpe
National Transportation Systems Center

Cambridge, MA

27 August 1998

by: Langhorne Bond
Pittsboro, NC
(919) 542-6614

I. "THIS CHANGES EVERYTHING"
Andrew Lloyd Webber

What a difference a year makes.

Last August we got the first picture and sales brochure for the Moscow GPS Jammer. For $3,500 and 5 watts of power you could jam the civil and military GPS signal for 200 kilometers. A very useful device if you have a little advance notice. Now we know why the counter terrorist cruise missiles in the Middle East were timed to arrive at exactly the same instant.

I'm not interested in learning the DOD's innermost secrets about jamming and counter-jamming. That's classified, and, as I have said before, properly so. But I am concerned about GPS and its role in civil aviation, ocean shipping, and other civil transportation control applications such as railway train control.

The recent use of GPS as a counter-terrorism strategy has confirmed what many of us have been saying lately—GPS and world terrorism are inextricably related.

The GPS technology is so pervasive, and so beneficial and lethal all at once, that we in the civil world have scarcely understood its implications. Its significance, for good and evil, is so great that the existing legal and managerial structures are obsolete.

What's more, the world's political leadership has not addressed this problem. And make no mistake, this vastly important matter is not going to be solved by career technicians. In the US, President Clinton, Secretary Albright, Secretary Cohen, and Secretary Slater must become involved. There's plenty of energy and vision on the US team, but it has been focused elsewhere.

II. RETHINKING THE PROBLEM

We in the US are showing modest signs of a growing awareness of the problem. We have realized that GPS can reach back and bite us.

The current DOD/DOT Federal Radionavigation Plan calls for the deactivation and scrapping of all—repeat, all—secure ground based radionavigation aids in the very near future. If you think the word "scrapping" is too dramatic, consider this: the US Coast Guard dynamited the LORAN tower on Hawaii recently. From a radionavigation perspective, US shipping and aviation is already "sole means" in the Central Pacific.

Today's conference at the Volpe Center, together with the RTCA/Applied Physics Lab study under the supervision of Bob Baker of American Airlines and Monte Belger of FAA, are initial attempts to study the issue of GPS vulnerability in a systematic, partially public, way. The effort is praiseworthy, and will lay the groundwork for solving one aspect of the total GPS conundrum, namely protecting the United States from a catastrophic loss of GPS signal.

III. DEFINING THE PROBLEM

The current Federal Radionavigation Plan calls for the abandonment of all ground based radionavaids in the very near future. The US policy, unless amended, commits US aircraft to flying with only GPS for navigation and landing guidance. To actually implement this policy, two questions must be answered satisfactorily.

A. Is it Single Thread?

In the aviation world, and I suspect in the marine world, we love redundancy. Our safety policies are based on the hard-won knowledge that nearly everything, sooner or later, will fail. If some element of an aircraft—a piece of structure, or a radio, or a fuel pump, or a hydraulic pump—or some element of a navigation

system, or of a surveillance radar system, fails, we want it to fail safe. We love redundancy. We love a back-up.

Navigation by GPS as a sole means is the ultimate single thread system. And it affects every aircraft in the sky, not just one. If the GPS signal is lost for any reason on a night when the ground is obscured by weather, the result will be multiple catastrophes.

The DOD figured this out long ago. Every US combat aircraft and guided munition carries, or will carry, an independent inertial navigation system.

Navigation by GPS is, by definition, single thread navigation. With the possible exception of flight over remote areas where there is no radionavigation now, and VFR flight, GPS sole means navigation is unacceptable. This conclusion is entirely independent of any findings on GPS vulnerability.

B. Is GPS Vulnerable?

By now everyone knows that the GPS signal is vulnerable. We all know about the Moscow jammer, and the French jammer, and the Sandia jammer, and the Rome, NY jammer, and solar interruptions, and so on. For the latest update you can dial up the US Air Force's advisory to its pilots on GPS outages.

The problem, oversimply stated, is that the GPS signal is extremely weak because it comes from a solar energized satellite 11,000 miles away. By analogy, the GPS signal received on or above earth, is equivalent to the light received from a 25 watt bulb 11,000 miles away. Modern receivers work fine with this signal. But it is so weak that it can be blotted out by a low powered transmitter which is, itself, hard to locate. It needn't be jammed for long: in three hours all arriving aircraft will have run out of fuel.

The DOD is hard at work in its NavWar program to reduce GPS vulnerability. Antenna design, and filters, should provide partial protection. In response, some enemy navwar expert will counter the counter. As with all military technology,

this process will go on without end. But it will never be foolproof for the user. If it were, the DOD would not be installing inertial back-ups.

It is even harder to imagine FAA requiring the installation of the latest anti-jamming technology in civil aircraft. The ARAC process now takes seven years from initiation to implementation.

In addition to jamming, interference from solar activity is another threat. This will be discussed today. I will be interested in the outcome because the estimates of the seriousness of the solar max range from meltdown of the birds to trivial non-event.

There is an additional failure mode which will not be covered today. Two years ago at the ATCA convention, I called it "Stealing the Switch." The GPS birds are controlled by radio signals from five ground stations in Colorado, Hawaii, Diego Garcia, Kwajalein, and Ascension Island. These signals change the orbits, turn off the signal, improve and degrade the signal accuracy, and very likely, spoof the signal in ways that are not public. The signal can be turned off over selected regions. The "switch" signal is uplinked in encrypted form.

The code is secret but the signal is not: it has been picked off by the satellites and ground stations of curious nations and non-governmental organizations, not all friendly to the US. If the code can be broken, and control of the birds stolen, we have a problem.

This spring a group calling themselves Masters of Downloading announced on the Internet that they had cracked the DOD code that controls the GPS birds. The fragment of the code they released was confirmed by DOD. DOD said it wasn't serious. Who knows?

Finally, there is the problem of unknown failure modes. In the design of life-critical electronic systems, this is very important. You can bet on this: DOD

knows a whole lot more about this than we civilians do. Which leads me to my concluding section.

IV. WHAT WE DON'T KNOW

There are so many dimensions to GPS policy. We all know when the GPS signal is lost: that is widely reported. But we have no idea exactly why. We know, for example, that DOD is developing counter jamming techniques. But we don't know the latest techniques, and I doubt FAA will be given them to put in the Federal Register.

We also know that DOD is developing its own jamming systems that are more sophisticated than the Moscow Jammer, several of which DOD purchased. Jamming our own GPS signal to deny it to the enemy is a perfectly sensible battlefield strategy. Could a military jammer be designed to deny the enemy but not our receivers? I hope so. But I don't see this going into our civilian planes and vessels any time soon.

So my expectations for this conference, and for the RTCA/APL study, are very limited. The data we need to assure aviation and marine safety is just too critical to the defense of the free world to declassify.

That is why the press release summarizing the Presidential Decision Directive (PDD) on GPS policy said, cryptically, 'The GPS signal will remain responsive to the National Command Authority.'

The full text of the PDD was not released.