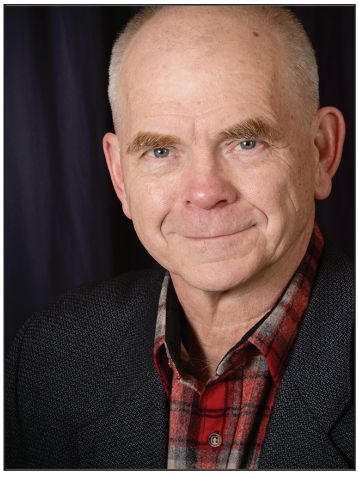
Ensuring PNT for All



Today's headlines frame my thoughts about securing GNSS assets, which one expert has characterized as our "least visible and most vulnerable infrastructure."

In the Columbia River Gorge, a National Scenic Area spanning the Washington-Oregon border, a 15-year-old boy has been accused of intentionally tossing fireworks into tinder-dry grass thereby starting a (thus far) 33,000-acre forest fire that has devastated a natural treasure. Meanwhile, in the latest incident of large-scale identity theft, credit-rating agency Equifax has belatedly acknowledged a months-long breach of its database in which 143 million personal records were reportedly accessed.

In one case, an individual — obliviously or purposefully — creates outsized havoc, in the other, a skilled team of professional thieves disrupt a global enterprise and endanger the financial well-being of millions.

Of course, we have headlines closer to the point, such as "Reports of Mass GPS Spoofing Attack in the Black Sea," or "South Korea developing eLoran Network to Protect Ships" from North Korean GPS jamming.

These latter incidents, of course, arise from state-sponsored or –enabled actions. But, as with the Columbia gorge fire, personal behaviors — often harder to detect and prevent — can similarly afflict GNSS capabilities. In recent years, considerable attention has focused on the use of small GNSS jammers, also known as "personal privacy devices." Perhaps the best-known case is that of a trucker trying to jam his vehicle's own receiver who interrupted GPS-aided landing operations at Newark International Airport.

As the articles on jamming and spoofing mitigation in this issue of *Inside GNSS* reflect, the motives and methods of perpetrators vary. But, given the natural progression of information-sharing and widening expertise in GNSS — along with our cultural soft spot for making heroes out of rebels and outlaws — we can probably assume that the trend toward disruption will only get worse.

Some GNSS user groups have struck out on their own to ensure the security of their constituencies and their particular needs. Military users benefit from a variety of alternative PNT technologies such as geomagnetic mapping, vision- and image-based navigation, and chip-scale atomic clocks and inertial measurement units. The U.S. Federal Aviation Administration has decided to retain, for the time being, a minimum operational network of VHF omnidirectional range (VOR) facilities originally planned to be phased out with the introduction of GNSS.

We can probably assume that the trend toward GNSS disruption will only get worse.

Over time, some of these alternatives may migrate into the commercial and professional space — then again, they may not. And the vast majority of individual GNSS consumers have no organizations to advocate for their needs.

So, what is to be done? How can we ensure that the positioning, navigation, and timing (PNT) utility is available to all users, and not just those sectors with the resources to develop solutions for themselves? The future of location-based applications and enterprise — and the associated economic benefits — depend on a satisfactory answer to that question.

Multi-level threats clearly require multi-tiered responses that fit the corresponding scope and scale of different domains. At the system level, GNSS providers are exploring such measures as encryption, signal authentication, stronger signal power, and advanced signal designs.

National and international legal/initiatives include such efforts as regulating the sale and use of GNSS jammers and spoofers. Alternative PNT systems — for example, enhanced Loran (eLoran) — represent a potential multinational approach to the problem.

At the level of user equipment, several GNSS manufacturers are incorporating interference detection and mitigation (IDM) and antispoofing capabilities into proprietary products.

The variety of these initiatives and their advocates illustrates the breadth of concern about assured PNT, but also reflect the fractured nature of responses to the threats to GNSS. The situation calls for leadership with the expertise and stature to bring comprehensive solutions before the wider GNSS community.

The International Committee on GNSS has the membership and forum, if not yet the clear mandate, to impose such solutions globally. At the national level, the U.S. Space-Based PNT Executive Committee assisted by its expert advisory panel seems the most likely candidate for this role.

GLEN GIBBONS, JR.
Editor