National PNT Advisory Board comments on

Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures

November 4, 2010

***Summary*: The United States is now critically dependent on GPS. For example, cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System (NEXGEN) cannot function without it. Yet we find increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations.**

Most alarming, the very recent web availability of small GPS-Jammers suggests the problem will get worse. These so-called *personal protection devices* (PPDs) as well as other, readily available, more powerful devices can deliberately jam the Global Positioning System (GPS) signal over tens of square miles. They also can be devastating to the other, new foreign satellite navigation systems being deployed worldwide.

PPDs are illegal to operate, but many versions are available (for as little as $30) from foreign manufacturers over the Internet. The simplest models plug in to a cigarette lighter and prevent all GPS reception within a line of sight range of 5 to 10 miles. Current penalty for operation is simply that the device is confiscated.

We currently lack sufficient capabilities to locate and mitigate GPS jamming. It literally took months to locate such a device that was interfering with a new GPS based landing system being installed at Newark Airport, NJ.

This paper provides background on satellite navigation and describes the impact of these dangerous PPDs and other disruptive radio frequency interference (Jamming). It also suggests needed action and discusses technical measures needed to harden GPS receivers against PPDs. The PNT Advisory Board believes that countermeasures and actions must be urgently developed.

We strongly believe that the Executive Branch should formally declare GPS a “Critical Infrastructure. But that is clearly only the first action and is by no means sufficient. A multiple agency approach must be urgently developed and executed

We must quickly develop and field systems that will rapidly locate, mitigate and shutdown the interference. In addition, laws are needed with the power to arrest and prosecute deliberate offenders. [This would be similar to legal action in response to the recent spate of laser attacks on pilots in flight].

Finally, we discuss the need for alternate navigation systems such as eLoran or a backup system currently being configured by the Federal Aviation Administration (FAA). While the foreign GPS-equivalent systems may offer some help against accidental interference, web sites are already offering devices that will effectively shut down ***all*** satellite-based radio navigation signals.

Note that all of these actions and jamming countermeasures tend to ***deter*** those who would deliberately interfere with the signals.

Specific Recommendations:

1. **National Focus**.

***GPS should be formally declared critical infrastructure by Executive Branch and managed as such by DHS*.**

2. **National Alerting and Pinpointing Interference Locations.**

The National Executive Committee should establish and sponsor a National GPS Interference Locating, Reporting, and Elimination System ; coordinating and expanding on the resources of several Departments.

3. **Shutting Down and Prosecuting Interferers –**

Legal and Law Enforcement actions. The National Executive Committee should examine whether or not they should sponsor Legislation in Congress that addresses interference to GPS that provides substantial fines and jail time for both possession and use of GPS jammers.

4. **Hardening GPS Receivers and Antennas.**

Government should foster and help to stimulate Manufacturers to speed up the development and offering of interference resistant GPS receivers, especially for safety-of-life applications such as commercial air and maritime.

5. **Fund a National back-up capability to insure continuity of PNT Operations.**

We strongly recommend that the previously announced decision (to deploy eLoran as the primary Alternate PNT) should be reconfirmed and quickly implemented.

We support the FAA's efforts to provide Alternate PNT options that can provide a robust backup to GPS and deter malicious interference.

Justification and Rationale

Background

The utility of GPS continues to increase with an ever-broadening set of applications including military use, aircraft guidance, harbor navigation, car navigation, emergency response and personal navigation. It is now estimated there are close to one billion users.

GPS is a one-way system; it broadcasts line-of-sight signals from a set of satellites in medium earth orbit (MEO) to the earth-bound users carrying GPS receivers. The satellites are approximately 12,000 miles above the receivers. These satellites are placed at this altitude, so that the coverage of an individual satellite is over one third of the Earth's surface. With 30 satellites carefully arranged in MEO, all earthbound users of GPS (with a clear view of the sky) can see at least the prerequisite four satellites to determine user location instantaneously. MEO is used so that a reasonably sized constellation can aid navigation worldwide. Lower orbits would require much larger constellations for worldwide instantaneous coverage.

For the reason described above, all GNSS satellites are placed in medium earth orbit (MEO). However, because the journey from MEO to the surface of the earth is 12,000 miles long, the GNSS signals are weak. They have a received power of only 10^{-16} Watts (*equivalent to a Los Angeles user receiving the light from 60 watt lightbulb in New York*), and can be easily overwhelmed by earth-sourced interfering transmissions at the GPS frequency. As described below, this radio frequency interference (RFI) can be: *scheduled*, *accidental*, or *malevolent*.

Critical Dependency on GPS

Much of our infrastructure is critically dependent on Positioning and Time from GPS. Two such dependencies illustrate this.

First, ***most telephone cell towers*** require GPS time to insure they are synchronized and cooperate. Recent instances of jamming in New York have rendered whole neighborhoods without cell service **including Emergency Service Providers.**

A Second example is the use of GPS for Aircraft Approach to Landing Fields. These GPS-based systems are being deployed and are particularly useful at airports where good alternatives are not available such as at Aspen, CO and Juneau, AK. There are now more FAA-sanctioned GPS approaches than the older beam-steering type. (Over 2000 GPS approaches). The value of these systems is enormous but the vulnerability is not universally appreciated: it took over a month to locate the deliberate small Jammer that was periodically driven by Newark airport. This example is particularly pertinent because the FAA's NextGen Air Traffic Control System is critically dependent on GPS. Proliferated Jammers would cripple the new system which is expected to greatly reduce aircraft delays.

Other Applications: GPS as a "Stealth" Utility. GPS has been aptly called the Stealth Utility. There are *literally 100s of additional application examples*. Some are safety-of-life (e.g. air and marine), some are startling productivity improvements (e.g. agriculture) and some are simply convenience or recreation (e.g. car navigation). It is now estimated that there are close to 1 ***Billion*** GPS receivers worldwide.

The GPS Jamming Threat

Scheduled RFI is probably the largest cause of GPS outages today. The military testing of GPS jamming causes these outages. The events are localized (usually in the Southwestern US), scheduled (during periods of light air traffic), and approved/coordinated by the Federal Aviation Administration. The FAA announces all upcoming events in Notices to Airmen. Because of the ever-greater Airway-Dependency on GPS, the FAA is increasingly reluctant to grant permission for these tests.

Accidental RFI has certainly interfered with GPS countless times, both domestically and internationally. Most events are probably not reported. The user who is denied service may not even know to whom it should be reported. These disruptive events include unintentional interference due to harmonics from broadcast television, and improperly designed wireless data communication systems.

Deliberate interference, called **jamming**, is the looming threat. Many of the billion GPS users have become extremely dependent on GPS accuracy, 24 hour availability, and outstanding integrity. This dependency makes GPS a very appealing target for sabotage or malicious mischief.

This white paper is a plea that the National Decision Makers address this situation.

Deliberate Jamming: the so-called "Personal Privacy Devices"

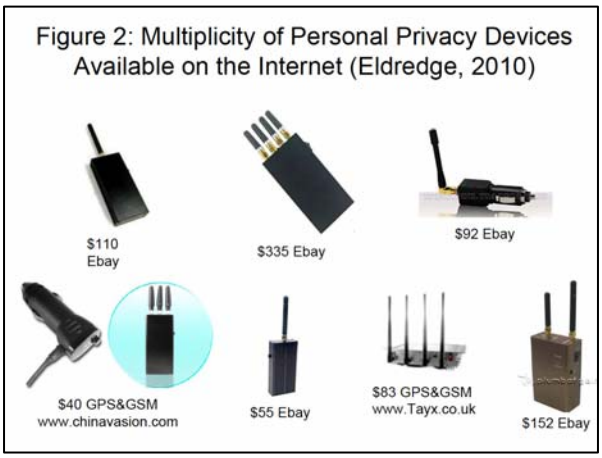
In the past year, so-called personal privacy devices (PPDs) have become widely available on the Internet. A simple example of such products is shown in Figure 1. The most inexpensive PPDs are single antenna devices that jam the one GPS signal frequency (L1) that is used by most users. More expensive units have multiple antennas and attack all three GPS signal frequencies (L1, L2 and L5). As such, these attackers anticipate the next generation of GPS user equipment that would continue to function if only one or two of the three frequencies were jammed. Others PPDs jam cell phone frequencies at the same time, shutting down all calls. They are preferred by car thieves that wish to prevent an on-car warning systems to report the location of a stolen car to the authorities using a GPS receiver connected to a cell phone link.

Figure 1: Commercially Available GPS Jammer ("Personal Privacy Device")

As shown in Figure 2 (Eldredge, 2010), PPDs range in price from $30 to over $300 based on the number of frequencies under attack and the transmitted power. Some radiate only a few milli-watts and other broadcast several watts. The former knock out GPS receivers for hundreds of yards, and the latter can have dangerous effects for many miles.

As their name suggests, PPDs are marketed to individuals that fear for their privacy. This sales strategy seems to be effective. An investigation recently initiated by the FAA revealed that trucks traveling on the New Jersey Turnpike were carrying these devices. Perhaps, these drivers worry that the company dispatcher was

Figure 2: Multiplicity of Personal Privacy Devices Available on the Internet (Eldredge, 2010)

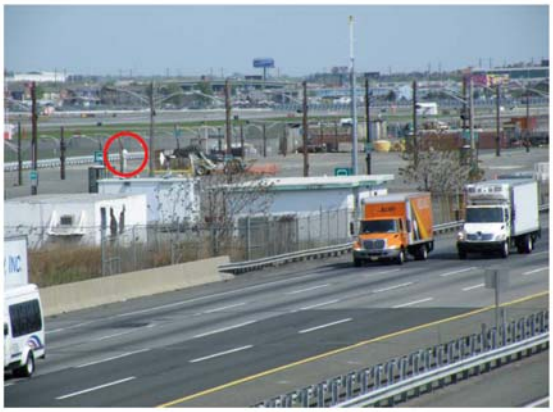


monitoring their locations. Ironically, the attention of the dispatcher must be drawn to the truck that never provides location reports.

Jamming Examples – the threat is real and getting worse.

Newark Airport. In any event, a PPD can cause collateral damage much greater than any privacy protection the user may possible enjoy. The above-mentioned FAA investigation was sparked while the FAA was installing a new GPS-based landing system for aircraft at Newark International Airport. This new system uses GPS receivers on the ground to aid GPS receivers in the approaching aircraft. This technique allows the use of all runways during restricted visibility conditions. The antennas for the FAA's ground receivers are shown in Figure 3 (Eldredge, 2010), which also shows the proximity to the New Jersey Turnpike. During system test, the FAA noticed that the GPS ground receivers suffered one or two breaks in reception on many days. PDDs were identified as the cause of the continuity breaks after an investigation that lasted several months. If PPDs gain notoriety, they could gain the interest of hackers. These people may not be particularly worried about their location privacy, but may simply enjoy the notion of jamming GPS over wide areas.

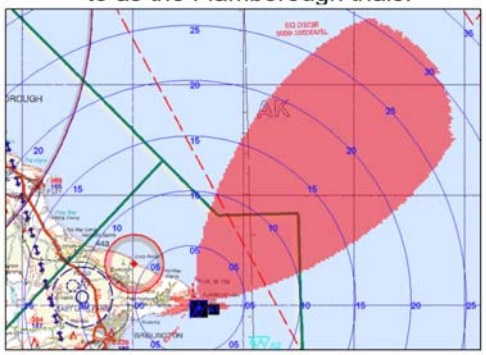
Figure 3: Proximity of Impacted GPS Ground Antenna to Highway



Military – North Korean Incident. Malevolent RFI is known as *jamming*. Enemy Jammers were deployed in Iraq to interfere with US weapons systems during Operation Dessert Storm. Most recently, military analysts have expressed concern about recent GPS jammers tested by the North Koreans. (Telematics, 2010). On August 23 and 25 of this year, jamming signals emanating from the North Korean city of Kaesong. These attacks interfered with South Korean GPS military and civilian receivers on land and at sea. Officials say the jammers were repeatedly switched on for 10-minute periods over a number of hours during the three days. South Korea's defense minister, Kim Tae-young, voiced concern to members of the National Assembly. He correctly observed that the North Koreans can mount transmitters on vehicles that can jam GPS signals within a 50 to 100 kilometer radius. Professor Park Young-wook, with Kwangwoon University's Defense Industry Research Institute, states that such jamming must be considered a serious threat if it reoccurs because GPS is an integral part of the infrastructure, not only for the military but for many other industries.

We certainly share the concerns voiced by Minister Tae-young and Professor Young-wook. However, we feel that the greater danger is posed by the propagation of GPS jamming technology to the wider public through devices sold on the Internet. These threats were described earlier

Figure 4: Jamming Zone During Trials Conducted by the General Lighthouse Authorities (GLA) of the U.K. and Ireland (Last, 2010). These are referred to as the Flamborough trials.

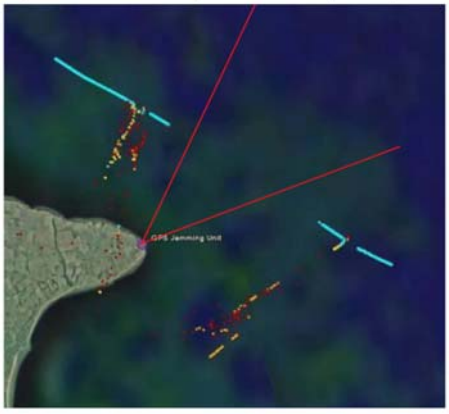


Maritime Controlled-Jamming Experiments. Until recently, GPS receivers for non-aviation purposes have not enjoyed the scrutiny or extensive testing used by the aviation community. Because of their

designs and clear line-of sight exposure, Maritime receivers can certainly be more vulnerable then aviation receivers. The following figures (Last, 2010) depict some disquieting results from recent trials conducted by the General Lighthouse Authorities (GLA) of the United Kingdom and Ireland.

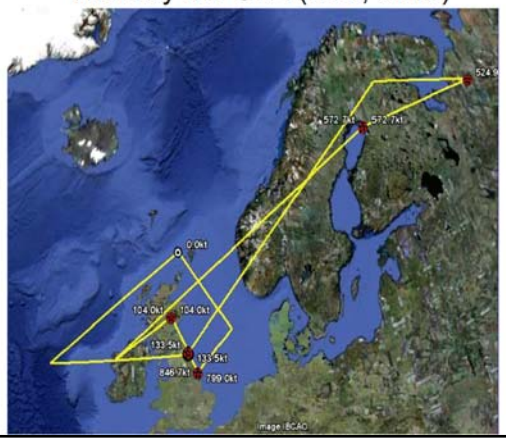
During these trials, a jammer was deployed in Flamborough, and the zone of impact is the wedge shown in Figure 4. As shown in Figure 5, this jammer had a devastating effect on the shipborne GPS receiver carried through the jamming zone. The receiver reports a faithful position track (in light blue) when the ship is far to the Northwest or far to the Southeast of the jamming wedge.

Figure 5: Position Fixes Reported by GPS Receiver Within Experimental Jamming Zone (red lines) Generated by the GLA (Last, 2010)



Within the wedge, the receiver is overwhelmed and reports no position fix – the jammer breaks GPS continuity. GPS shows no solution. **As the receiver approaches or has just departed the wedge, an extremely hazardous result occurs. The receiver suffers large position errors without an accompanying warning – integrity is broken. This is shown as the string of dots to the south and to the southeast of the actual blue track.** These last results are most troubling, because the bridge personnel would not be warned that the navigation system was degraded.

Figure 6: Position Fixes Induced by a Low Power Jammer Placed on Board the THV Galatea During Trials by the GLA (Last, 2010)



In another set of trials, the GLA placed a low power jammer on board the Trinity House Vessel Galatea. As shown in Figure 6, this jammer induced position reports that skipped across Scandinavia and Ireland while the ship sat steadfastly in the English Channel (the yellow track). Among the systems affected by the interference were the ship's radar and gyrocompass, key reversionary systems when GPS fails.

The worrisome results shown in Figures 5 and 6 would not affect an aviation receiver, because aviation standards insist on an internal set of tests (algorithms) for RFI. We later recommend that these algorithms or equivalents become part of the standards for receivers used in any safety-of-life applications.

Recommended Actions to Counter the Threat of GPS Interference

There is not any practical way to *completely* eliminate GPS interference. But steps can be taken to greatly reduce the frequency and impacts of such interference. Further, actions can be taken to insure that GPS receivers do not give false indications of position or time. Our recommendations are:.

1. **National Focus**. GPS is absolutely critical US National Infrastructure. This has not been formally recognized. ***GPS should be formally declared critical infrastructure by Executive Branch and managed as such by DHS.*** This is necessary to elevate the importance of GPS to our critical infrastructure and bring the needed attention to the interference problem. The various existing national interference programs must be coordinated and gaps must be filled with additional funded efforts (see later recommendations). Senior leadership must recognize the vulnerabilities of the current critical infrastructure and give high priority to budgets and solutions.

2. **National Alerting and Pinpointing Interference Locations.** ***The NATIONAL EXECUTIVE COMMITTEE should establish and sponsor a National GPS Interference Locating , Reporting, and Elimination System ; coordinating and expanding on the resources of several Departments*****.** It took several months to locate the PPD that shut down the Newark landing system. Technology exists to locate such sources much more quickly. To rapidly alert and pinpoint interference, two elements are required: 1. sensing of the interference and 2. a communications channel to report the problem in real-time. For example, every cell phone tower could be configured to expand the functionality of their GPS timing receiver by promptly recognizing and reporting interference, including pertinent characteristics. The incremental cost would be extremely small. Another example: many toll booths routinely videotape vehicles including license plates. A properly configured GPS receiver at the booth could identify vehicles that are broadcasting interference. There are many more national reference receivers that could be so configured. Cell phones that include GPS receivers can be configured to sense and automatically report suspected interference. This would constitute a near instantaneous reporting channel, worldwide. Of course a central data-gathering location is needed; it could be collocated with preexisting civil/military resources such as WAAS, NGPS or the Air Force's 2SOPS. In turn, the located sources must be reported for appropriate action. **No such National (or International) Real-Time System exists today or is even currently planned.**

3. **Shutting Down and Prosecuting Interferers – Legal and Law Enforcement actions.** When the mobile jammer was finally located at Newark, the only punitive action for the deliberate interference was to confiscate the Jammer. The coordination of FAA, FCC, FBI, and DOD was commendable, but ad hoc and very tardy. ***The PNT Executive Board should sponsor Legislation in Congress that addresses interference to GPS with laws that provide substantial fines and jail time for both possession and use of GPS jammers.*** Precedents have already been established with the laws enacted to prevent and deter lasers being aimed at Pilots as they attempt to land airplanes. Australia, which is also very reliant on GPS for Air Traffic control, has a law that fines the possessor of a GPS jammer $100,000. In addition, operational procedures for rapid interdepartmental reaction and mitigation of interference must be established. A reasonable goal is to locate and shut down any jammer in a matter of hours.

4. **Hardening GPS Receivers and Antennas.** In addition to legal action, we wish to galvanize a technical effort to strengthen all GPS receivers. GPS receivers should never give the Hazardous and Misleading Information (HMI) that is shown in figure 6. The techniques to avoid this are well known and specified for all FAA certified equipment. **All GPS safety-of-**

life receivers should include the integrity algorithms specified by the FAA. There are also well-known design techniques to greatly reduce outages of GPS receivers due to interference. Examples include: special antennas that null interference, coasting thorough interference by using inertial components and/or small atomic clocks, as well as physical shielding in the direction of presumed jamming. Some would add significant cost but may be warranted for safety-of life and other critical applications. New supplementary devices can make GPS receivers more robust and are becoming more affordable. (e.g. miniature accelerometers, chip scale atomic clocks etc.)

Some actions are being taken. For example, the FAA is already hardening the GPS receivers and antennas placed on the ground at Newark International Airport. Changes include: GPS antennas that are less vulnerable to radio frequency interference; improved practices for placement of GPS antennas on the airport (farther from public roadways); and receiver algorithms that more quickly recover when the PPD moves away from the GPS antenna. ***Manufacturers should speed up the offering of interference resistant GPS receivers, especially for safety-of-life applications such as commercial maritime. These receivers should use FAA techniques to insure they do not display Hazardous and Misleading Information during periods of interference.***

5. **Establishing GPS Backups to insure continuity of PNT Operations.**

As described above, GPS receivers should certainly be made more robust against jamming. In addition, we feel that the nation should vigorously support efforts to provide Alternate Position, Navigation and Time (APNT). In this final section, we first describe the role of planned foreign satellite systems (GNSS) that are similar to GPS. Unfortunately they have the same susceptibility to interference as GPS. Next we describe two alternate techniques to determine PNT (APNT) that are more jam-resistant and could be readily made operational.

GNSS. GPS is now recognized worldwide, and other nations are responding with satellite navigation systems of their own. The Russians are reinvigorating their satellite navigation system called GLONASS, and new systems are being developed in China, Europe, Japan and India. Taken together, GPS and these other systems are called Global Navigation Satellite Systems (GNSS).

These other systems are valuable for improved accuracy and integrity. In addition they will offer frequency diversity. Therefore they will be helpful in countering *unintentional* interference at a single frequency. **The new PFD (Jammers) being sold on the web will also prevent use of these foreign GPS-like systems as well as cell phones. Thus these new foreign systems will not be helpful in operating during deliberate jamming radiated by the better devices currently available.**

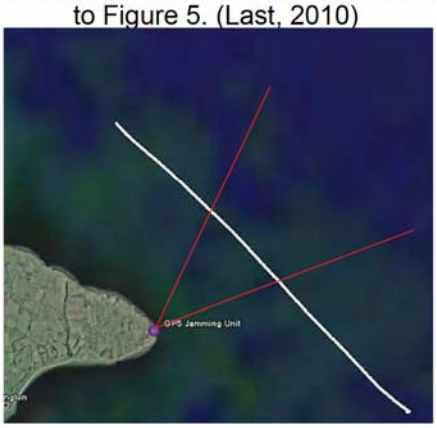
While a number of backup PNT systems have be considered, there are two major alternatives for APNT that have emerged as being particularly useful:

1. e-Loran: Loran is a ground-based radio-navigation system that preceded satellite navigation. It finds its origins in World War II, and enjoyed wide spread adoption after the grounding of the Argo Merchant on Georges Bank. At that time, the U.S. Coast Guard began to require Loran carriage by ships over a certain tonnage in the Coastal Confluence Zone of the United States. Importantly, Loran is based on the broadcast of *extremely high power signals* in the low frequency portion of the radio spectrum. The

frequency of transmission is 10,000 lower than the GPS frequencies in the microwave band, and the power of the transmission is 1000 times greater than the GPS transmission power. An updated version of called eLoran has now been developed and tested. It is very robust, resistant to interference and has two dimensional accuracies of about 20 meters in critical areas. It is not nearly as accurate as the best GPS, and the lack of the vertical dimension reduces eLoran's effectiveness, yet it is a very robust APNT system.

In December 2006, an Independent Assessment Team was appointed, reporting to DOT and DHS. It was under the administration of the Institute for Defense Analysis (IDA). After careful review over many weeks, they unanimously recommended that the eLoran deployment be completed as a backup for GPS. Yearly cost to maintain this in the US was about 20 $M. This is about 1/10th the cost of a single GPS satellite. The DHS then made an announcement that eLoran was the official APNT system for the US. The Schlesinger-chaired PNT Advisory Board has also unanimously recommended that eLoran be deployed and maintained as a GPS backup.

Figure 7: Faithful Position Track Produced by eLoran During the Flamborough Trials. Compare to Figure 5. (Last, 2010)



For these reasons, the *international* navigation community has also strongly supported the upgrade and sustainment of the Loran system in any number of forums. This recommendation has been heeded in Europe. Indeed, Figure 7 shows the faithful position track provided by enhanced Loran (e-Loran) as the ship traverses the jamming wedge generated by the General Lighthouse Authorities from Flamborough. Figure 7 provides a stark contrast to the GPS-based results in Figure 5. Unfortunately, DHS has not followed through with their announcement: the Loran system in the United States has been turned off.

We strongly recommend that the previously announced decision (to deploy eLoran as the primary APNT) should be reconfirmed and quickly implemented. The reasons for this are clearly stated in the IDA white paper. It is the most viable and robust backup to GPS and can be implemented in a way that is virtually seamless to the user.

2. Alternate Navigation for the Next Generation Air Transportation System: Today, the FAA uses an extensive network of terrestrial navigation aides to mitigate GPS outages. This backup navigation capability is based on ground-based navigation aids that precede GPS. All of these extant systems support point-to-point navigation. Even though these transmissions are reasonably robust against RFI, this point-to-point capability may not be suitable for the Next Generation Air Transportation System (NextGen). NextGen anticipates an increase in air operations by a factor of two or more by 2025, and will enable a host of operational improvements needed to smoothly support this traffic increase. NextGen is based on GPS, satellite-based augmentation systems (SBAS), and ground-based augmentation systems (GBAS). All of these systems provide so-called area navigation

(RNAV). In other words, they provide guidance over a volume, and the alternate navigation system of 2025 also needs to provide a volumetric aid to navigation.

Thus, the FAA is actively exploring alternate position, navigation time (APNT) as part of their NextGen effort, because the airspace should not revert to inefficient point-to-point navigation should RFI interrupt GPS-based operations in the 2025 timeframe. This APNT capability would be based on a reconfiguration of existing or planned FAA ground facilities (Eldredge, 2010), and Figure 8 shows part of the ground infrastructure that can be utilized to provide this APNT area navigation capability.

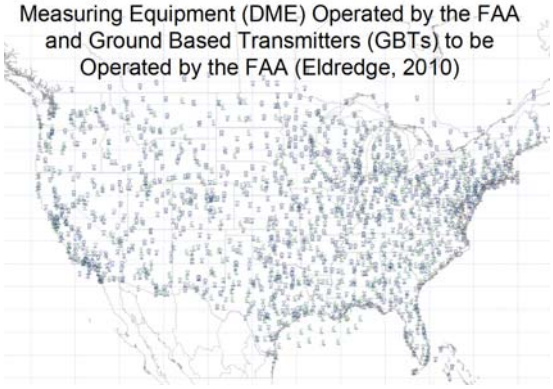


Figure 8: Combined Network of Distance Measuring Equipment (DME) Operated by the FAA and Ground Based Transmitters (GBTs) to be Operated by the FAA (Eldredge, 2010)

Time Synchronization: As part of their APNT effort, the FAA has identified three architectures that may be suitable for alternate area navigation in 2025. These straw men are based on the sites shown in Figure 8, but two of these APNT architectures require time synchronization of neighboring ground sites. To this end, the FAA has investigated time transfer based on hardened GPS receivers and low earth orbiting satellites (LEOs). In the former case, jammers are attenuated by so-called controlled radiation pattern antennas. In the latter case, the needed processing gain derives from the proximity of the LEOs. Indeed, the altitude of the LEOs is approximately twenty times less than the GNSS altitude. Thus LEOs have small earth footprints and cannot provide the navigation performance associated with GNSS. However, the signal received from this nearby source is approximately 400 times greater than the power received from GNSS. Thus, LEOs could provide the robust time transfer capability needed to support APNT, because time transfer only requires one satellite to be in the common view of the ground stations to be synchronized.

We encourage the FAA to continue efforts and to provide an APNT that is a robust backup to GPS and deterrent to malicious interference.

Summary and Conclusions:

The interference threats to GPS are very real and promise to get worse. These threats potentially imperil much of the US infrastructure. It will take some time to field a full set of countermeasures and systems. Failure to act will be a serious abdication of our national responsibility.

References:

1. Telematics, 2010, http://www.defence.pk/forums/military-forum/76068-north-korea-appears-capable-jamming-gps-receivers.html
2. L. Eldredge, 2010, “Alternative Position, Navigation and Time,” briefing to the FACA on Space Based Position, Navigation and Time, October 2010
3. D. Last, 2010, “Effect of Jammers on GPS in a Maritime Environment,” briefing to the FACA on Space Based Position, Navigation and Time, October 2010