Protect Critical Infrastructure - A Resilient Navigation & Timing P3
November 2013

"Reliance on satellite navigation and timing systems has become a single point of failure for much of America and is our largest, unaddressed critical infrastructure problem."
Dr. Brad Parkinson, "The father of GPS"

Executive Summary

The Department of Homeland Security has determined that the GPS timing signal is essential for the operation of 11 of the nation's 16 critical infrastructure sectors; all sectors use GPS information in some form. The number of jamming and spoofing incidents in the US continues to grow each year and the threat to our national, homeland and economic security increases.

In 2008, the federal government decided to establish a high power terrestrial navigation and timing system that would complement GPS in the United States to improve resilience, prevent spoofing and deter jamming. Signals from the new terrestrial system would be usable underground, indoors, and underwater. The new system would also be compatible with terrestrial navigation and timing networks in other countries.

Because of a number of non-technical, non-security reasons, the U.S. federal effort has stalled. In the meantime, the nation's ability to easily establish a terrestrial system is diminishing as DHS dismantles and disposes of the existing infrastructure; this, in spite of recent studies and experiments that confirm it is the best and lowest- cost solution.

Meanwhile, the risk to the nation increases. Some users have resorted to a variety of precise clocks and local systems that will provide backup/carry over during short-term GPS outages. No existing methods used in the U.S. cover broad areas or extended outages. Many users have no backup at all.

Establishing a public-private-partnership to create and operate a low-cost, hard- to-disrupt terrestrial navigation and timing system will:

- **help protect critical infrastructure;**
- **provide new services and;**
- **create a new IT industry segment.**

A public-private-partnership would combine the government's unused infrastructure and desire to protect the public interest with private sector investment and innovation. A terrestrial system could be built in the continental US for about $40M, operated for about $16M/yr, and need not be taxpayer funded. Demand for such services is high, reuse and upgrades of existing infrastructure will keep costs low, and numerous revenue streams are available. In our preferred business model, we propose to establish an endowment to help fund the enterprise in perpetuity.

The Vulnerability

Global Navigation Satellite Systems (GNSS), like America's GPS, are tremendous economic and technology enablers. They are highly precise and are free for use by anyone with an inexpensive receiver. As a result, their navigation and timing signals have been incorporated into nearly every aspect of modern life, from synchronizing power grids, to financial systems, telecommunications, and transportation. The signals are used by all 16 of our critical national infrastructure sectors. The Department of Homeland Security has said that the timing signal alone is essential for 11 of them.

When these faint, far-away signals can't be received, people start to feel the impact immediately. Usually these outages have minimal impact because they are localized and short lived. Often they occur because the user is temporarily in an area without a good view of the sky. More and more often, though, they are due to the presence of one of a growing number of people with jamming devices (many of which also block cell phone frequencies). Inexpensive, easy to obtain, and illegal, use of jammers is increasing[1] as people become more concerned about privacy and being tracked by their employer, spouse, NSA, and others. Although the government tries to collect information on jamming incidents, no widespread detection system has been established, and few verbal reports are received. For the calls that do come in, it is often impossible to determine which are because of user error (being in a bad location for reception, not understanding their equipment, etc.), and which are purposeful interference. For those cases where jamming is discovered, locating and identifying the perpetrator is difficult and often impossible. As one example, in spite of near daily interference with a landing system at Newark International Airport, it took the FAA and FCC over two years of concerted effort to identify the perpetrator.

If a navigation satellite outage became widespread and lasted more than a few hours because of a major solar flare, software problem, hacker or cyber-attack, most authorities agree that the impacts would quickly become catastrophic. While much of the information is classified, we do know that transportation would immediately become much less efficient and more dangerous (even traffic lights are coordinated using satellite timing). Telecommunications, financial, energy and other systems would also soon begin to fail as their back-up timing systems lost synchronization with each other. Power grids would lose synchronizations and outages may occur as transmission points became overloaded. More than speculation, these problems have been documented in academic papers, proven in government tests in the US and UK, and the early stages of such impacts have been observed in localized and short term outages in the United States. Most dramatically, they were observed during North Korea's intentional jamming of its neighbor to the south.

[1] http://www.fcc.gov/encyclopedia/jamming-cell-phones-and-gps-equipment-against-law

Of equal concern is the problem of spoofing. The world's pre-eminent spoofer of satellite navigation receivers, Professor Todd Humphries of the University of Texas, Austin, has demonstrated how easy it is to take control of unmanned aircraft and ships on autopilot by sending just a slightly stronger navigation signal, making the receiver think it is somewhere other than where it really is (Iran claims to have done something similar, capturing a US military drone in 2010). Professor Humphreys has also shown (on paper) how time stamps on automated financial transactions could be altered through spoofing. This could do things like reverse the buy-sell equation at a stock exchange, allowing someone to sell at a higher price before buying at a lower one.

Some navigation and timing users have resorted to a variety of methods such as sophisticated clocks and local systems to tide them over during interference events and other outages. Telecommunications companies, for example, typically place cesium timekeepers in cell towers for just such eventualities. Many captains of cargo ships still carry sextants so they can navigate by the stars, if need be. Aircraft can still navigate from point to point using 1960's era radio beacons. But even the best backup clocks lose synchronization with each other eventually, and older forms of navigation can't meet the needs of modern transportation systems. And that's for users who have made provisions for outages. Many have no plans or capability at all.

Of greatest concern though, is that so many users unquestioningly rely on satellite navigation and timing signals. Ships have run aground, aircraft have overshot their landing sites, and drivers have been led astray. The high availability and perceived accuracy of the signal and receivers make many unable to detect spoofing, jamming or a malfunction before it results in an accident. The most valuable feature of having a second, independent signal, is that it could alert users when something might be wrong and that they should start paying closer attention.

The Government-Approved Solution

So what is to be done? As it turns out, these challenges have been extensively documented and discussed since at least the 1990s. In 2004, President Bush, issued the National Space Policy (NSPD-39) that addressed the problem. Although portions of it are still classified, contained within the publically releasable section was direction for the Department of Transportation to, in coordination with the Department Homeland Security:

> "….develop, acquire, operate, and maintain backup position, navigation, and timing capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the United States, in the event of a disruption of … space-based positioning, navigation, and timing services…"[2]

[2] https://www.fas.org/irp/offdocs/nspd/nspd-39.htm

In response, the two departments consulted numerous experts and commissioned a study by the Institute for Defense Analysis (IDA) to determine what system or systems should be procured. The IDA study team, which included Dr. Brad Parkinson, widely recognized as "the father of GPS," unanimously recommended that an existing and outdated nation-wide navigation system called "Loran-C" be greatly updated and modernized to "eLoran." Such a system would provide a navigation and timing signal comparable with and complementary to GPS. They concluded that:

> "eLoran is the only cost-effective backup for national needs; it is completely interoperable with and independent of GPS, with different propagation and failure mechanisms, plus significantly superior robustness to radio frequency interference and jamming. It is a seamless backup, and its use will deter threats to US national and economic security by disrupting (jamming) GPS reception."[3]

What the IDA did not find, but that has since become evident, is that establishing a terrestrial system, in addition to deterring those who might want to jam or spoof satellite signals, could be an important part of a network to identify and locate jamming and spoofing attempts. With integrated receivers using both eLoran and GNSS (GPS) signals, the system could quickly detect and report differences in the two systems that might indicate deliberate interference. This could be especially valuable in sparsely populated areas where other detection networks, if established, might not reach.

The body in charge of coordinating navigation and timing issues for the federal government is the National Space-Based Position Navigation and Timing Executive Committee (NPEC). It is chaired by the Deputy Secretaries of Transportation and Defense. Responding to early briefings on the IDA report (which was not formally published until 2009), the Departments of Transportation and Homeland Security in 2007 told the NPEC that they had decided eLoran was the right answer. After further federal deliberations over how to create the system, 2008 saw:

- A press release by DHS saying that the department would be implementing eLoran, using the old Loran-C infrastructure (7 February 2008)

- The DHS "2009 Budget in Brief" document (February 2008) propose transferring the legacy Loran-C systems and $34.5M/yr from Coast Guard to NPPD, stating:

[3] The IDA effort called upon a comprehensive array of pre-existing work and consulted with numerous experts and government officials. The report consolidated the professional judgments and analyses of a very broad segment of those in the field. The report was published by DOT at: http://ntl.bts.gov/lib/31000/31300/31359/24_2009_IAT_Summary_of_Initial_Findings_on_eLoran.pdf

"The FY 2009 budget transfers the budget authority for the LORAN C system from the United Sates Coast Guard to the NPPD. The Department, acting as Executive Agent, will begin development of enhanced eLORAN as a backup for the Global Positioning System (GPS) in the homeland."

- The National PNT Executive Committee endorse the above decisions (March 2008)

Failure to Launch

Unfortunately, DHS funding for 2009 came as part of a continuing resolution, and the Congress did not approve the transfer of funds from Coast Guard to NPPD. This was because influential members of Congress wanted the eLoran capability, but were concerned about the lack of a documented transition plan for the move from one agency to the other. A year later, though, no plan had been presented, and the President's request (and enacted legislation) for 2010 contained no mention of upgrading the system. In fact, it contained provisions for shutting down and defunding the old Loran-C system without providing funds for NPPD or any other agency to establish the new eLoran capability.

What happened between one budget year and the next to take the nation from "solution-in-hand" to "no solution at all" is not a matter of public record. Internal administration budget deliberations are not generally released to the public. It does appear, though, that this disconnect between policy, requirements and budget was due to a number of factors, many of which showed bureaucracy at its worst. A new administration, putting together its first real budget, quite rightly wanted to shut down an antiquated system, but did not understand the importance of the new one. OMB's long corporate memory that the original budgets for the expensive GPS program included a promise that all other navigation systems would be redundant and hence eliminated, and OMB apparently desired to finally see that through. Lack of support from other knowledgeable government agencies was also a factor. Concerned that, if they showed too much interest in the issue, OMB might assign the responsibility of fixing the problem to them, their input as to the severity of the problem and the need for a solution was tepid, at best. And within DHS a lack of understanding and enthusiasm at the still relatively new NPPD that was consumed with other and seemingly more immediate issues prevented them from being a good advocate. All of these, and probably others, unquestionably played a role.

Movement Backward

Without any funding, DHS has conducted several studies and experiments since 2009, but has done little to address this critical infrastructure issue. While officials at the Department of Defense talk about the need for resilience, experts throughout government and industry decry the lack of action, and the Department of Transportation still has acquiring "backup position, navigation, and timing capabilities" on its to-do list – neither department has seen fit to move forward on their own.

DHS has reduced the nation's ability to create a terrestrial system, prevent spoofing, and create a wide area interference detection and mitigation system. An on-going effort to fell towers and dispose of equipment from the legacy Loran-C system, will significantly increase the cost and time-to-operation of the new system the nation needs.

The Way Forward

Yet awareness and understanding of the problem within government, and the general public has continued to grow. The U.S. National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board published a seminal white paper in 2010 on the topic strongly recommending the establishment of an eLoran system. Todd Humphries, the UK navigation authority, and others have provided numerous graphic demonstrations of the folly of relying upon just one electronic navigation system, and how things can go horribly wrong. Some of these have been well publicized. Other incidents are highly classified and known only to a few.

There are also signs that the U.S. intelligence, cyber and defense communities are becoming more and more concerned. North Korea's repeated jamming of satellite navigation and timing signals has been a particularly powerful lesson. South Korea has reacted by committing to establishment of a robust eLoran system. Russia and China already have their own versions of Loran-C, and Russia has announced it is working with the UK to upgrade its system, called Chayka, to eChayka to support navigation resilience in the Arctic. China is undoubtedly not far behind in upgrading its system. India also has funded a plan for an eLoran system, as have others. Small wonder that the Defense Department CIO has expressed interest in eLoran as part of DOD's pivot to the Pacific. But providing a system at home is not in Defense's job description, nor should it be.

Fortunately, respected leaders at the Departments of Transportation and Homeland Security still see this as an important issue that needs to be addressed. The question for them now is not one of technology. The technology decision made in 2008 has since been revalidated by a plethora of academic papers, risk estimates, and white papers. The terrestrial eLoran system still appears to be the most effective and least expensive solution available. What DOT and DHS must resolve are questions of governance and how to fund the system in one of the most difficult federal budgetary climates in decades.

The answer may lie in a public-private partnership (P3). In such an arrangement, the government would bring its interests and the infrastructure it owns to the table. An entity in the non-profit sector or industry would provide investment to refurbish the infrastructure, stand up and operate the system. Such a P3 enterprise could not only pay for itself, but be an on-going source of revenue for both the government and the private entity.

The Business Model - Demand

A well configured eLoran system is able to provide navigation accuracy to within 8 to 10 meters and timing accuracy to within 30 nanoseconds.[4] This meets the needs of an estimated 95% of users in the United States. And while eLoran does not offer the sub-meter precision of a high end, augmented GPS/GNSS system, it has its own advantages. In addition to being very difficult to disrupt, its high power (typically 400 kW transmitters), low frequency (100 kHz) signal easily penetrates and is usable underground, inside buildings, and underwater. Places that much weaker and much higher frequency satellite and cell phone signals are unable to reach.

The UK experience with eLoran and private surveys in the US have shown high commercial demand for a ubiquitous, wireless, precise, and resilient time and navigation service. Power companies want to be able to synchronize grids with a signal that can't be disrupted by a delivery driver trying to avoid being tracked by his boss. Cell phone companies would be happy to replace expensive cesium clocks in their towers with an inexpensive eLoran sensor. Owners and operators of autonomous vehicles want a way for them to navigate that is highly resilient to spoofing. And research has shown that many users who rely upon GPS/GNSS time for mission critical applications have no secondary source to fall back on in the event of a disruption.

Since eLoran typically penetrates inside buildings, underground, and underwater, it can be used for timing and navigation in many places where no other navigation and timing sources are available. For example, it has been used for underground and underwater navigation. When paired with an accurate satellite signal before going underground or submerging, eLoran could allow a navigation receiver to maintain a comparable level of precision for several hours. Even after that, it would provide the navigator an accurate underground/underwater compass, and a good position.

Spoofing and interfering with eLoran is very difficult. This makes it very attractive for transportation, especially for owners and operators of autonomous vehicles. The average received eLoran signal is 1,300,000 times stronger than a GPS/GNSS signal. Interfering with it requires large, powerful equipment that would be very easy to detect and locate. And, for a vehicle that has both eLoran and GPS/GNSS, a spoofer would have to deceive both systems in exactly the same way, at exactly the same time in order to be successful. A difficult and unlikely achievement at best.

The eLoran navigation and timing system now in operation in the United Kingdom is also generating revenue by transmitting data. While the full potential of this "third-party data

[4] This accuracy is based upon already demonstrated capability. When the GPS system was first implemented, accuracy was about 65 nanoseconds for timing and 65ft for navigation. Since then, more PHD's have been granted for research on GPS than any other field of study, and augmented GPS signals are now able to guide machinery with a precision of millimeters. While that level may never be achieved for eLoran because of its low frequency, additional university and commercial research, once the system is in operation, will undoubtedly improve its already good performance.

channel" capability is still being explored, the ability to assure delivery of data to, and possibly communicate with such areas is very appealing to many commercial and government organizations. The potential benefits to first responders and commercial interests are almost limitless.

The Business Model - Costs

The cost for the P3 to standup and operate an eLoran system in the Continental United States would be exceptionally low. Most of the needed infrastructure is already owned by the federal government in the form of the sites for the shuttered Loran-C system. Many of these still have transmission towers and other equipment that could be repurposed Re-using this infrastructure and equipment would greatly reduce both the time and expense need, compared to standing up the new system from scratch[5].

Operating and maintenance costs would also be low. Solid state equipment, remote monitoring, and other advances in technology make the process of re-establishing a transmitting station fairly inexpensive. Today's eLoran station is a tower, a small telecom shelter, a fence, and a backup generator in case of power outages. And with only a modest investment needed to refurbish existing infrastructure, regular outlays needed to service capital debt would be minimal, at best.

Some estimates are that a terrestrial precise navigation and timing system, such as the one established in the United Kingdom and the one up for contract by South Korea, could be established in the continental United States within three years and for approximately $40M, if the existing infrastructure were repurposed. Operating costs are estimated at approximately $16M per year. Usable signals could be available well within the first year of operation.

Business Model – Revenues

Significant National and Homeland Security concerns. High demand. And low cost (especially compared to any space program). It is clear that, but for a series of bad bureaucratic reasons, eLoran would have been established in the US, probably as a government owned and operated system, long ago.

But high demand and low cost are also excellent ingredients for a business enterprise, provided there are sources of revenue. An eLoran P3 could have multiple sources of revenue. Depending upon the type of partnership and business model(s) the government selected, surplus revenue might also be generated. Some of the possibilities include:

- **Guaranteed delivery data transmission** – As mentioned earlier, eLoran's high power and low frequency mean that the signal penetrates where few others will. In addition to

[5] Of course, the more DHS continues with its program to fell these towers and dispose of the real property, the more expensive establishing the new system will become, and the more time it will take.

navigation and timing information, which are inherent in the basic signal, data can also be included on intermingled or additional pulses. The highest demonstrated data transfer rate to date has been 1,300bps. Many believe that, with a modicum of research, that rate can be much higher. Although 1,300 BPS is considerably slower than "internet" speeds, it is adequate for high-priority, critical texting. As the owner of the high power transmitter network, the P3 would generate revenue the same as any telecommunications provider - by charging per message or for time on the network. Applications could include:

- Assured wireless control of remote equipment and vehicles, including indoors, underground and underwater.
- Information delivery to first responders and other crews regardless of location. This would be especially good for pre-programmed emergency and operational commands to evacuate, use another procedure, etc.
- Immediate device updates and reprogramming. The ability to reach all of the enabled devices on a given network at the speed of light and virtually simultaneously has unlimited potential.

- **PNT Interference Detection and Monitoring** – One of the biggest challenges to countering jamming satellite navigation and timing signals is the lack of a detection network. The eLoran transmitter and receiver network will continuously synchronize with GPS/GNSS signals and instantly detect when differences between the two dissimilar systems occur. Instant reports could be generated to inform federal, state, and local authorities of the anomalies and assist in finding their locations. Mobile disruptors could even be tracked as they drove down the highway, sailed through the port, or flew across the sky. The P3 could generate revenue by contracting to provide such information to private parties and government agencies concerned about interference incidents.

- **Licensing Receivers** – One of the simplest ways to generate revenue and endow the P3 would be for the government to assess a small fee on every standalone or integrated eLoran and satellite navigation receiver sold in the United States. A one dollar fee per unit could generate over $20M/yr and fund operation of the entire system. Such a fee could be discontinued as other sources of revenue from the system made it unnecessary.

- **Broad-based User Fees** – Since navigation and timing signals are essential to so much US critical infrastructure, a case could be made that the cost to endow the P3 should be spread as broadly as possible across the technologies it supports. For example, a temporary 8 cent fee on every monthly US cell phone and electric bill could, in one year, provide enough funding to endow the P3 in perpetuity.

- **Value-Added Services For "High End Users"** – More than 90% of the users of precise time in the United States require it at the microsecond (1,000 nanoseconds) level of accuracy. eLoran can provide a signal accurate to 30 nanoseconds. To achieve that level of precision, the eLoran network transmits data that compensates for small differences in the received signal due to the terrain in a given area. This correction data could be encrypted. Most users would access the signal at the microsecond level of accuracy for free. Revenue could be generated by charging those who desire the higher level of precision a fee for the encrypted portion of the signal.

The above list of potential revenue sources is just a sampling of the many ways a P3 could be funded. It shows that financing the enterprise need not come from tax dollars, and should not be an obstacle to its creation.

The Public-Private-Partnership

The US government has had some great successes solving previously intractable problems through public-private-partnerships. Probably the best known of these are the P3s formed for housing on military bases. Establishing a business model that has private partners constructing and managing on-base housing has resulted in more, and higher quality, housing for our troops. Such arrangements must be carefully established and managed, however. Both the Congressional Budget Office (CBO) and the Office of Management and Budget (OMB) are understandably concerned that public-private partnerships may get a project going but soon the costs may fall entirely on the government.

Success in any endeavor depends upon its execution. The type of partnership the government selects and creates will be key. While, at its heart, a P3 is just a contract, the nature and provisions of government contracts are endlessly varied. Issues that need to be addressed will include how the infrastructure is provided, if it is to be retained in perpetuity by the government or will be conveyed to the private party, what length of contract will allow the private partner to recoup its initial investment, and the business model(s) to be pursued.

The type of governance will also be important. Models vary from establishment of a self-funded independent government corporation that would oversee operations on a daily basis, to an agency-supervised, performance-based contract that only requires regular reports on system availability and performance.

And, of course, the concerns of CBO and OMB will need to be met. Fortunately, the federal government is not without experience with P3s. Also, there are many supporting resources available, such as the National Council for Public Private Partnerships (www.ncppp.org).

We Have to Do It

Establishing a public-private partnership will bring together the best of both the government and the private sector. For its part, the government will bring the legacy infrastructure and its interest in safeguarding the public good to the table. The private sector will bring financing, technical know-how and innovation. A better system for America will result than would have been possible if either were to act alone.

It is unquestionably in our urgent national interest to address the problem now, before jamming and spoofing become more widespread, or we have a larger, more damaging event.

The need is clear. The technology exists and works great. Financing is not a problem. All that remains is for dedicated leaders within government and the private sector to work together and implement the solution.

Mr. Dana A. Goward is the President and Executive Director of the Resilient Navigation and Timing Foundation, a U.S. 501(c)(3) non-profit. The RNT Foundation is devoted to helping protect critical infrastructure by educating people about the need for and encouraging resilient “navigation and timing ecosystems” with services that complement each other and have different failure modes. www.RNTFnd.org