3. Critical Infrastructure & Timing

Overview

"There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Presidential Decision Directive 21 (PDD 21) identifies those sectors and the policies and federal responsibilities associated with their protection. Further, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, states that "It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure [as defined in section 5195c(e) of title 42, United States Code] (critical infrastructure entities), as appropriate."

GPS and the PNT services it provides is not a critical infrastructure, but it is ubiquitous in daily life and in all critical infrastructure that rely on highly precise geolocation and timing services. GPS signals are exceptionally weak, line of sight signals. They are easily jammed, spoofed, or disrupted. Similar to cyber vulnerabilities they represent a single point of failure for the U.S.' critical infrastructure.

Utilization and Benefits

GPS and the PNT are ubiquitous in daily life and underpin all networks and virtually all critical infrastructure. Disruptions to GPS signals can deny service to end use devices, disable information pathways, and provide users and databases hazardously misleading information.

Disruptions

- Natural – Some terrain features and urban canyons can degrade GPS reception for some users. Solar flares in 2007 and 2014 disrupted GPS services for users in some parts of the world for about 15 minutes. Major solar flares could cause longer term disruptions.
- Purposeful -
    - International – Multiple open source reports have identified Russia, China, North Korea, Iran, and terrorist forces in the Middle East as repeat sources of GPS jamming and spoofing
    - Domestic – "Personal privacy devices" are illegal to use, but easily obtained via the internet. Anecdotal reports indicate that use is widespread and that the devices are popular with criminal organizations. The U.S. has no systematic way of monitoring or even surveying to estimate the rate of use. Sampling in Europe has detected over 240,000 unique electronic signatures and an increase over time in use and sophistication. Devices designed to deny service to areas up to 20 miles in diameter are also easily available on the internet.
    - Licensed – The FCC is considering licensing a service in a frequency adjacent to the GPS band. The PNTAB believes this will degrade and disrupt GPS service for many users. See separate paper.
- Accidental – Improper installation and use of electrical and electronic devices of many kinds has been found to interfere with reception of GPS signals. This includes installing GPS antennae in close proximity.
- Systematic – Equipment failure and operational errors have caused problems. Two examples:
    - A GPS system error caused navigation errors of about 16 km (10 miles) for three hours on 1 January 2004
    - On 25 January 2016 a 13.7 microsecond timing error migrated to 15 GPS satellites. This caused scattered faults and failures for 12 hours across infrastructures and around the world. Systems included the U.S. aviation safety ADS-B network and most all the first responder radio systems in North America.[5]

[5] http://rntfnd.org/wp-content/uploads/3.-Fault-Reports.pdf

Challenges to Reducing Risk

Users are typically unaware of GPS vulnerabilities. Even when they are, they are not willing to invest in more expensive equipment to reduce their threat of disruption. This lack of consumer demand has kept the cost of better equipment relatively high.

Recommended Actions

- Protect:

  The Nation must adopt and maintain spectrum regulations and allocations that protect critical infrastructure timing receivers from interference due to legal transmitters in the RNSS frequency bands and excessive power from transmitters in adjacent frequency bands. The PNTAB has made a recommendation on this separately.

  Significant sources of jamming and spoofing need to be promptly located and removed, not merely defended against. Nationwide capabilities for GPS Interference detection and mitigation should be implemented. The PNTAB has not made specific recommendations for how this should or could be accomplished.

- Toughen:

  Encourage manufacturers to develop more variety and less expensive receivers and antennae with improved resilience. Critical infrastructure owner/operators need to evaluate and, as appropriate, acquire, properly install and maintain such equipment. Recommended practices to achieve improved competency have been published by the NCC[6].

- Augment:

  Use of Multiple Satellite Constellations - Using selected signals from foreign satnav systems as well as GPS can improve receiver performance and resilience. The PNTAB has recommended separately that the FCC waive its requirement for licensing of non-Federal use of signals from Galileo as requested and recommended by key stakeholder agencies of the Administration.

  Backup System – Ensure backup capabilities for GPS-derived PNT are available and used to protect the nation's critical infrastructure and public-safety applications. Dependence on GPS signals and increasing instances of jamming and spoofing have created a single point of failure for U.S. Critical Infrastructure. In 2015, the PNTAB recommended an initial deployment of four eLoran transmitter sites, assuming cost of US$ 10 Million per site through refurbishment of existing Loran sites. Annual maintenance cost per site was assumed at US$ 1 Million. The PNTAB stated it is essential to verify these cost and performance assumptions. The PNTAB recommends prompt implementation of back-up capabilities for GPS per NSPD-39. Implement eLoran as a back-up for GPS timing in the continental United States, subject to verification of cost and performance. Further, agencies should be strongly encouraged to continue development of other capabilities that heighten resiliency.

  The PNTAB recommends prompt completion of civil agency deliberations on back-up capabilities, and prompt actions to implement the resulting decisions.

Summary

GPS timing is an asset to many aspects of critical infrastructure, but the fragility of many current implementations has created significant national vulnerabilities. Additional work needs to be done to make the use of GPS and other satnav systems' signals more resilient against existing and evolving threats, both intentional and unintentional. Modern GPS-derived timing, properly supported by cost-effective backup and complementary technologies, can help ensure the health of the nation's critical infrastructures. The first step is recognition of the extent to which GPS is present in all aspects of American life.

[6] https://ics-cert.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf)