Here is what was posted recently on this subject:

https://www.gpsworld.com/research-roundup-soft-information-for-iot-positioning/

https://www.nojitter.com/security/understanding-gps-data-spoofing

DOT Lagging on GPS Backup Demo:

https://www.linkedin.com/pulse/chairman-defazio-letter-questions-dot-secretary-lagging-goward/

https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf

https://www.congress.gov/bill/115th-congress/senate-bill/140/text#toc-id89e563a8d5524c5a84cacf66865f7ba1

Year in Review: Big Problems in 2019!

https://www.linkedin.com/pulse/grounded-flights-lost-drones-crop-circles-year-gnss-guy-buesnel/

https://www.linkedin.com/pulse/gps-week-rollover-telescopes-weather-balloons-traffic-guy-buesnel/

New:

https://www.linkedin.com/pulse/how-fight-jamming-gps-world-editorial-advisory-board-dana-a-goward/?trackingId=LaHKVqxuvqwWsEzGBCUueA%3D%3D

https://www.gpsworld.com/editorial-advisory-board-pnt-qa-policy-on-jamming/

Grounded flights, lost drones and ‘crop circles’: the year in GNSS vulnerabilities

- Published on December 10, 2019

Guy Buesnel

PNT Security Technologist - with expertise in testing system robustness against G... **See More**

44 articles Follow

In 2019, we saw massive worldwide disruption from GNSS jamming, spoofing and other vulnerabilities. Here’s a recap of the year’s most significant events.

If anyone still doubts the seriousness of the risks presented by GPS and GNSS vulnerabilities, the events of 2019 should put those doubts to rest.

I’ve spent most of my career identifying threats to GNSS-dependent systems, and I can categorically say I’ve never seen issues on the kind of scale we’ve seen this year.

Across the world we’ve seen flights grounded, shipping disrupted, drones lost, weather balloons downed, and vehicles of all kinds mysteriously lose their bearings. The causes range from state-sponsored electronic warfare and organized criminal activity to technical issues with the satellite systems and the receivers that rely on their signals.

Here’s a look back at some of the most significant events of 2019.

GPS week rollover disrupts flights, traffic lights, weather balloons, and more

At midnight on April 6th, the Global Positioning System rolled into its third epoch of existence. This entirely planned and predictable event nonetheless spelled trouble for many users of older GPS receivers.

The issue was with the way receivers interpret the week number element of the GPS time signal. To conserve bandwidth, the week number is encoded in a 10-bit format that resets to zero after 1,024 weeks (or one GPS epoch). Many receivers that hadn’t been patched to cope with this issue started to behave erratically as the rollover took effect, breaking the systems that rely on the data they output.

As I wrote at the time, systems affected on the 6th April included New York’s traffic lights, the weather balloons of the Australian Bureau of Meteorology and the tsunami warning buoys of the National Data Buoy Center.

But the GPS week rollover is actually an ongoing issue, because many receivers count the 1,024 weeks from the date their firmware was compiled, rather than from the start of the GPS epoch. So we’re still seeing new problems crop up – likely including this widespread grounding of flights in June, which the FAA attributed to a ‘GPS issue’ in one manufacturer’s avionics equipment.

Galileo goes down for a week – an unprecedented outage for a GNSS constellation

As if the GPS week rollover wasn’t enough, in July Europe’s Galileo system experienced a jaw-dropping week-long outage, during which it was unavailable for positioning, navigation or timing services.

The facts behind this huge and unprecedented GNSS system failure are only slowly coming to light, but one thing is certain: the world had a lucky escape. Today, almost all Galileo receivers also use GPS and sometimes other positioning systems, so they continued to work in Galileo’s absence. Most users wouldn’t have noticed anything amiss – although they may unknowingly have lost a certain amount of location accuracy and protection against interference.

But it does raise serious questions about what might happen in the event of a major outage of a system that single-constellation receivers rely on. As I wrote in July, it’s a wake-up call for GNSS users and developers to model the impact of a major outage and put backup measures in place.

State-sponsored GPS jamming and spoofing reach record levels

GPS signal jamming has long been a favoured method of electronic warfare (EW) by nation states, aimed at disrupting the enemy’s ability to navigate in geopolitically sensitive areas.

But 2019 saw unprecedented levels of jamming across huge geographical areas – particularly the Arctic Circle and the Middle East – with commercial shipping, aviation and emergency services all reporting significant disruption due to loss of GPS reception.

There are also signs that EW methods have advanced to include spoofing, in which fake GNSS signals are broadcast from a transmitter on the ground with the aim of throwing vehicles – notably drones – off course. Disruption reported in Russia since 2016 and in Libya this November suggests the use of powerful spoofing devices to capture drones or prevent drone attacks.

Drone threats increase, creating a dilemma for drone manufacturers

Methods for dealing with drones are becoming a concern in the civilian world, too. Last December, Gatwick was brought to a standstill when a rogue drone was spotted near the airport. In February, six drones were confiscated in Atlanta after breaking no-fly rules at the American Superbowl, and in August, a group of climate activists threatened to carry out drone incursions at Heathrow.

The problem creates a dilemma that will become acute in the next few years. Manufacturers want to protect their drones against jamming and spoofing, to ensure they work as intended in the presence of RF interference. At the same time, governments want to be able to safely disable any drone that's used as an offensive weapon – and RF interference is one of the most effective ways of doing that.

In short, the more robust its inbuilt protection against jamming and spoofing, the harder a rogue drone will be to disable. As I wrote in September, I wouldn't be surprised to see governments asking manufacturers to build 'back doors' into their drones' navigation systems – and the reaction to that request will be interesting to see.

ICAO flags GNSS interference as an 'urgent safety priority'

As commercial activity becomes more reliant on GNSS and the threats to GNSS increase, more organisations are starting to see signal interference as a critical risk – not just to business continuity, but to safety of life.

In October, the International Civil Aviation Organization (ICAO) for the first time identified GNSS disruption as an 'urgent safety priority', responding to concerns raised by a host of national and regional aviation bodies.

A horrifying near-miss incident at Friedman Memorial Airport in Hailey, Idaho, was one of the catalysts for ICAO's action. A write-up of the incident in NASA's June Callback newsletter notes that there was 'widespread jamming' and 'an abundance of smoke' in the area as 'Aircraft X' approached the airport. The pilot had reported a GPS outage prior to its descent, but said the problems had cleared up, so the local controller cleared the aircraft for a GPS-based approach.

Shortly thereafter, a controller some 250 miles away in Salt Lake City happened to notice that Aircraft X was straying off course. What's more, the plane was at 10,700 feet altitude and nearing a 10,900 feet mountain.

Thinking quickly, the controller contacted the local control tower in Hailey, which directed the aircraft back onto a safe flight path. The report concludes that "Had [the Radar Controller] not noticed, […] the flight crew and the passengers would be dead, I have no doubt".

This was an isolated incident, but data shows that GNSS interference poses a rapidly-growing threat to aviation. The chart below shows the number of instances of interference reported to NASA's Aviation Safety Reporting System every year since 1997. Bearing in mind the 60-day lag between an incident being reported and it being published, the 2019 data is significant indeed:

https://www.gpsworld.com/access-denied-anti-jam-technology-mitigates-navigation-warfare-threats/

https://www.gpsworld.com/septentrio-ppk-gets-a-boost-with-basefinder-function/

https://www.microwavejournal.com/articles/30994-beamforming-ics-simplify-phased-array-antenna-design?v=preview

https://www.linkedin.com/pulse/understanding-gps-data-spoofing-jitter-dana-a-goward/?trackingId=qsQkQQ1xAQmT7kcPFe5ozw%3D%3D

https://www.nojitter.com/security/understanding-gps-data-spoofing

https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/

https://www.yahoo.com/lifestyle/read-map-gps-fails-170214205.html

Emergency response providers participating in a workshop organized by the ResponDrone Project indicated that they would like to use drones to gather and distribute crucial information and provide communication networks in disaster areas. Check out more takeaways from the event:

https://www.gpsworld.com/first-responders-see-real-time-data-a-top-benefit-of-using-drones/

https://www.gpsworld.com/directions-2020-delivering-gps-capabilities/

"Aggressive GPS spoofing impacting shipping has been detected in over 20 Chinese coastal sites during 2019. These included the ports of Shanghai, Fuzhou (Huilutou), Qingdao, Quanzhou, Dalian, and Tianjin. AIS data courtesy Global Fishing Watch, ORBCOMM and Spire" - Thanks to The Maritime Executive and Dana A. Goward for using our collaborative data to break this amazing story on "Patterns of GPS Spoofing at Chinese Ports" today.

We create #newspace #bigdataanalytics built for #optimizing #weather & #maritimesecurity. Our goal is to power the #maritimeindustry with #emergingtech. Spire is a new kind of #satelliteimagery built for a new kind of #global #maritimesafety.

https://lnkd.in/dJtD4xf

https://maritime-executive.com/editorials/patterns-of-gps-spoofing-at-chinese-ports

https://www.gpsworld.com/staying-ahead-of-navwar-and-resilient-pnt-in-2020/

https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/gps-inventor-we-need-to-fix-gpss-jamming-problem/

https://www.scmp.com/news/china/society/article/3042991/china-flight-systems-jammed-pig-farms-african-swine-fever

https://www.gpsworld.com/launchpad-3d-data-ford-telematics/

Who moved my datum? In a few years, the US will replace its static spatial reference systems—NAD 83 and NAVD 88—with the new North American-Pacific Geopotential Datum of 2022 (NAPGD2022). Read more in ArcUser: **http://ow.ly/C2C650xEttu** https://www.eurekalert.org/pub_releases/2019-12/aiop-llt122319.php (Lasers accurately spot space junk)

https://www.linkedin.com/pulse/gps-spoofing-new-how-to-tutorial-youtube-dana-a-goward/

https://www.youtube.com/watch?v=3NWn5cQM7q4&feature=youtu.be

https://www.nasa.gov/image-feature/nasa-s-x-59-quesst-airplane-takes-shape-at-lockheed-martin-skunk-works