

Don Koulaouzos

Security in Outer Space: Planning for Compromised Positioning, Navigation and Timing

INTRODUCTION

More than a hundred different Global Navigation Satellites orbit the Earth providing Positioning, Navigation and Timing (PNT) services, with the latter capability being the least appreciated or understood.

PNT does more than guide motorists, aviators, sailors and hikers. Many industries such as construction, mining, surveying, package delivery, logistical supply chain management, farming, fixed and wireless communications networks, banking systems, defence, security and emergency services, financial markets, water utilities and power grids depend on the accuracy and availability of PNT.

How robust is this ‘invisible utility’, what are the consequences of compromised PNT on critical national infrastructure and what contingencies exist to protect it?

Most of the terrestrial-based PNT systems have been or are being progressively decommissioned leaving satellite-based PNT as a vulnerable single point of failure for many users.

Several natural and human threats can temporarily or permanently deny access to accurate satellite PNT. Low probability but high-impact risks to satellites can come from space weather or meteor showers, as well as space debris or anti-satellite attacks. Terrestrial threats such as jamming and spoofing are far more prevalent and insidious. These can come from unfriendly state actors, domestic military tests and even civilians using low-cost equipment to evade surveillance.

Mariners and aviators regularly report jamming and spoofing attacks that could have serious consequences. These attacks have also affected communications networks and financial services.

The financial impact on society from the loss of PNT has been estimated to be up to \$1 billion per day for some countries, but there are initiatives underway to improve the resilience or availability of PNT. This includes alternative capabilities in space as well as from terrestrial networks, self-contained inertial navigation and timing systems or diverse radio signals of opportunity on Earth.

Governments, society and industry should have a greater awareness of the risks and impact of compromised PNT so that further investments to protect this essential invisible utility can be considered.

A COMPROMISED PNT WORLD

While far out at sea in the middle of the night, the crew of a merchant vessel wakes the captain to tell him they have lost all control of the ship's steering and throttle.

A few hours later, an airline pilot aborts a landing after receiving warnings that there is an error in the approach guidance system and is forced to make a night landing in dangerous conditions.

Later, a young girl is sent home early when school is unexpectedly closed owing to a national incident disrupting all electricity, water and heating. She cannot call home because the cellular mobile phone networks are down. She tries to withdraw money from the nearest Automated Teller (cash) Machine (ATM) to pay for a taxi home, but the banking system is not working. Meanwhile, police cannot manage traffic gridlock in the city as their emergency services radio network is also out of action.

This is not an extract from a sci-fi or disaster movie. Each of these scenarios involving compromised Positioning, Navigation and Timing (PNT) from Global Navigation Satellite Systems (GNSS), such as the Global Positioning

System (GPS), are derived from actual events. The schoolgirl scenario is an amalgam of several separate occurrences, but compromised GNSS PNT is not rare.

In 2016, a timing error in the GPS network disrupted TV, radio, banking and emergency services communications for over half a day in different locations worldwide.¹ A large container ship lost control in the Mediterranean in 2017 after its navigation system was hacked,² while an airliner lost all GPS position information, forcing the pilots to make a hazardous pre-dawn landing in 2020 at El Paso International Airport without vertical guidance.³

These events provide a chilling reminder of our dependency on GNSS PNT.

This analysis will explore some of the risks and impacts of compromised GNSS PNT, while reviewing the adequacy of several existing, planned and proposed resilience initiatives.

PNT EVOLUTION AND GNSS DEPENDENCY

We cannot imagine life without the four essential public utilities that we take for granted: water, energy, communications and waste disposal. Yet in less than half a century, almost every aspect of our life has become reliant on an ‘invisible fifth utility’ – GNSS PNT. Positioning provides a two or three-dimensional location of the user. Navigation lets the user determine the current and desired relative or absolute position and apply corrections to course, speed and heading. Timing provides and maintains accurate time locally or globally from a standard reference such as Coordinated Universal Time (UTC).⁴ For many, the T (timing) in PNT is often overlooked and taken for granted as a hidden element embedded in this invisible utility. When GPS was initially established for the military, it was never envisaged that timing would become a critical service that many communities depend on globally.

¹ KOVACH et al. 2016.

² BLAKE 2017.

³ HARRIS 2021.

⁴ Ordnance Survey 2023.

GNSS PNT is not only used by motorists, hikers, mariners and aviators. Many industries, such as construction, mining, surveying, package delivery, logistical supply chain management, farming, fixed and wireless communications networks, banking systems, security and emergency services, defence, financial markets, water utilities and power grids, all depend on the global availability and accuracy of GNSS-based PNT.

LIFE IN A WORLD BEFORE GNSS PNT

In 1904, the first time signals were sent to ships by radio to allow navigators to check their chronometers. This was followed by the first radio navigation beacon installed in 1921.⁵ By the end of World War II, a global network of 72 high-power, Low Frequency (LF) radio transmitters provided Long Range Navigation (LORAN)⁶ services, including the U.K.'s Decca Navigator system. Radio nav aids for aviation and some maritime users progressively expanded after World War II. The number of Very High Frequency Omnidirectional Range (VOR) beacons peaked in 2000 when thousands of stations were operational in the United States⁷ along with other radio nav aids such as Distance Measuring Equipment (DME) and Non Directional Beacons (NDB).

All commercial airlines and aircraft flying in conditions without adequate outside visual references must fly under the Instrument Flight Rules (IFR). The Instrument Landing System (ILS), developed in the 1930s, provides precision radio navigation that allows suitably equipped IFR aircraft to approach and land at night and in bad weather by providing vertical (glide slope) and horizontal (localiser) guidance to and from the runway.

⁵ BOWDITCH 2022.

⁶ BARTLETT et al. 2015.

⁷ HARRIS 2021.

GNSS is progressively replacing radio navigation systems

The age of space-based navigation was launched in 1978 with the (then) \$12 billion investment in the US GPS operating in Medium Earth Orbit (MEO) of approximately 20,200 km.⁸

The business case for replacing radio navigation systems with their significantly higher installation and operational costs compared to GPS was compelling. The U.S. closed their last LORAN-C and Enhanced LORAN (eLORAN) stations in 2010, followed by Europe and the U.K. in 2015. LORAN-C and eLORAN services remain operational in several countries, including equivalent LF systems in Russia and China.⁹

The U.S. is also progressively decommissioning VOR stations, which will be reduced to 580 sites by 2030.¹⁰ The Australian Civil Aviation Safety Authority removed half of Australia's radio navigation network after mandating GNSS as the primary means of navigation for IFR aircraft from 2016.¹¹ In a similar cost-saving measure in 2018, the U.S. Federal Aviation Administration (FAA) approved IFR aircraft equipped with suitable avionics to make precision approach and landings using GNSS as an alternative to ILS at those airports that have installed Ground Based Augmentation Systems (GBAS).¹²

GNSS has also enabled the replacement of traditional navigation methods in the air. American Airlines achieved \$1.2 million annual fuel cost savings in 2013 by removing 16 kg of flight manuals and navigation charts from the flight deck, becoming the first airline to operate through all phases of flight with iPads.¹³

⁸ ESA 2021a.

⁹ BARTLETT et al. 2015.

¹⁰ ALWIN 2023.

¹¹ CASA 2016.

¹² FAA 2023.

¹³ HUGUELY 2013.

GNSS is an essential service for all mariners

In 2000, the International Maritime Organization amended regulations to allow Electronic Chart Display and Information Systems to replace paper nautical charts for seagoing vessels, eventually becoming mandatory for new and existing ships from January 2011.¹⁴ Plans to withdraw paper charts by 2026 and replace them with digital equivalents were announced by the U.K. Hydrographic Office in 2022. However, this deadline was subsequently extended to 2030.¹⁵ It is now common for pleasure yachts to be equipped with GNSS-enabled chart plotters that sailors often use as their primary means of passage planning, pilotage and en route navigation. The Automatic Identification System (AIS) uses Very High Frequency (VHF) radio to broadcast their GNSS-determined ship location, direction and identity automatically. AIS is compulsory for all vessels over 300 Gross Registered Tonnes and is also becoming more popular with pleasure yachts.¹⁶

Motorists and pedestrians rarely use paper maps for navigation today. To find their way to an unfamiliar address, almost all motorists and some pedestrians once carried a street directory, atlas or paper map. After Garmin launched the first portable Street Pilot GPS navigation system in 1998, drivers eventually became more dependent on this convenient technology.¹⁷

The growth of Satnav has reduced the demand for printed maps. For example, in 2017, the Map Shop stopped printing the once popular Fuller's Street Directory.¹⁸ The end of this once indispensable travel aid is representative of similar trends worldwide. More than one billion people use and rely on Google Maps every month.¹⁹

¹⁴ IMO 2011.

¹⁵ UKHO 2022.

¹⁶ NATO 2021.

¹⁷ LEITE 2018.

¹⁸ WHETHAM 2021.

¹⁹ MUKHERJEE-ZALANI 2024.

PNT will play an important role in autonomous vehicle operations

The International Standards Organization and the Society of Automotive Engineers International have jointly established performance and system requirements for autonomous vehicles. There are six defined levels of driving automation, ranging from no driving automation (Level 0) to full driving automation (Level 5).²⁰ These vehicles must achieve 95% confidence of horizontal position accuracy of around 20 cm with availability greater than 99.9%.²¹ They accomplish this by integrating multiple sensors and technologies, including GNSS, to accurately ascertain the vehicle's environment and maintain optimal real-time control.²²

Financial services globally depend on reliable precision timing. Almost all aspects of financial services utilise GNSS timing for compliance, operational analytics, market transparency, automated share trading algorithms and ATM operations. Regulators require mandatory timestamping of at least 100 microseconds accuracy for the Consolidated Audit Trail in the USA and Markets in Financial Instruments Directive II in Europe. These systems rely on atomic clocks synchronised between Earth and GNSS satellites, which provide accurate UTC down to the nanosecond.²³

GNSS is a key enabler for precision agriculture. Nearly 40% of large farms in the U.S. employ some form of Precision Agriculture (PA). Adoption of PA by large farms has reached 30% in Germany, 20% in Australia and almost 10% in Hungary.²⁴ PA relies on GNSS in 4 key areas: 1. guidance and steering systems; 2. land preparation; 3. yield monitoring and mapping; and 4. Variable Rate Application (VRA). Sensors, maps and GNSS are used in VRA to automate the application of irrigation, fertilisers, chemicals and seeds. Other PA

²⁰ ISO 2021.

²¹ PETOVELLO 2019.

²² GIANNAROS et al. 2023.

²³ HOPTRUFF 2023.

²⁴ TRIMBLE 2022.

applications reliant on GNSS include field planning, soil sampling, pest and crop monitoring, as well as farm vehicle and drone guidance.

Global and regional PNT systems

The military relies on assured GNSS PNT for everything from navigation and positioning of ground vehicles and dismounted ground forces to weapon guidance. It is used to synchronise elements of Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR) (C4ISR).²⁵ Consequently, adversaries now recognise the strategic value of GNSS PNT, making it a high-value target for Electronic Warfare.

GPS is often incorrectly used as a generic term for GNSS, which can also refer to augmentation systems used to improve the accuracy and stability of PNT. There are currently four operational GNSS and two Regional Navigation Satellite Systems (RNSS), which are listed in Table 1.

Galileo is the only civilian controlled GNSS, and it also currently offers the highest accuracy down to 20 cm horizontally and 40 cm vertically with its High Accuracy Service.²⁶

Each GNSS and RNSS transmits data on more than one dedicated frequency, some of which is encrypted, to enhance availability accuracy and mitigate Radio Frequency Interference.

GNSS plays a vital role in society, delivering (mostly) reliable, accurate and ubiquitous positioning, navigation and timing services worldwide for Critical National Infrastructure (CNI) and services that include:

- cellular, emergency services and defence telecommunications
- autonomous vehicles and drones
- air, sea, road and rail transportation
- power and water utilities
- financial services
- digital broadcast and land mobile radios

²⁵ ASCENCIO 2021.

²⁶ ESA 2023a.

Table 1
Global and regional navigation satellite systems

Name	FOC*	Constellation**	Control	Type
GPS (Global Positioning System)	1995	24 MEO	U.S. Government	GNSS
GLONASS (Globalnaya Navigazionnaya Sputnikovaya Sistema, or Global Navigation Satellite System)	2011	24 MEO	Russian Government	GNSS
BDS (BeiDo Navigation Satellite System)	2020	30 MEO, 5 GEO***	Chinese Government	GNSS
Galileo	2021	24 MEO	European Union	GNSS
NavIC (Navigation Indian Constellation)	2017	3 GEO, 4 IGSO****	Indian Government	RNSS (1,500 km around the Indian mainland)
QZSS (Quasi-Zenith Satellite System)	2018	1 GEO, 3 IGSO	Japanese Government	RNSS (East Asia and Oceania)

Notes: *Full Operating Capability; **Baseline constellation; ***Geostationary Earth Orbit; ****Inclined Geosynchronous Orbit

Source: ESA 2023

The dismantling of ground-based systems such as VOR, LORAN and other radio navigation systems further increases dependency on GNSS PNT, which, in some cases, has created a single point of failure for CNI.

There is no doubt that we now live in a world where all aspects of life are directly or indirectly dependent on GNSS PNT.

PNT RISKS AND IMPACT

Many human threats and some natural hazards could compromise GNSS PNT, affecting its accuracy, integrity, continuity and availability. Most of society and some industry segments are unaware of the fragility of this ubiquitous, free and ‘invisible utility’, expecting it always to be globally available.


Jamming, spoofing and cyberattack are threats to GNSS PNT. To illustrate one aspect of this vulnerability, consider that the strength of a GNSS signal is less than one billionth of a watt by the time it travels over 20,000 km to Earth. This is like trying to see a 20-watt light bulb in Lisbon from Moscow at midday. Therefore, it does not require a very strong or sophisticated source of interference to jam or spoof GNSS.

A direct Line of Sight (LOS) signal must be received from at least 4 GNSS satellites to obtain an accurate 3D fix (latitude, longitude and altitude). The user’s environment can impact LOS, where high terrain or buildings (known as Urban Canyons) can either block direct signals or generate reflected signals off these objects. These multipath reflections can degrade the accuracy of GNSS positions. Loss of primary LOS creates a vulnerability that can make it easier to inject false signals or jam them.

GNSS jammers are not only used by adversarial state actors. Construction of GNSS jammers with off-the-shelf components only requires a basic knowledge of radio and electronics. Jammers are illegal to use in most jurisdictions, but the production and sale of these devices are not universally regulated. Portable vehicle and fixed installation ‘chirp jammers’ are small devices that can be plugged into a car cigarette power socket. These units, known as Personal Privacy Devices (PPD), can be purchased online from around US \$10.00 an example of which is shown in Figure 1.²⁷

²⁷ DHgate 2024.

Motorcycles > Auto Electronics > Other Auto Electronics > 12V24V Car GPS Signal Interference...



12V24V Car GPS Signal Interference Blocker Shield Privacy Protection Positioning Anti Tracking Stalking for Auto Vehicles7954847

US \$6.01--9.75/Piece

USD	\$9.75	\$6.83	\$6.22	\$6.00
	2 Pieces+	10 Pieces+	49 Pieces+	167 Pieces+

Buy it Now Add to Cart

Figure 1
Low-cost in-vehicle GPS jammer
 Source: DHgate 2024

A common use of PPD jammers is taxi and Heavy Goods Vehicle drivers evading rules on maximum driving hours, toll payments or trying to stop employers from tracking them. PPDs block GNSS and can cause inadvertent interference to other users when operating near sites such as airports or even fixed GNSS PNT users. The London Stock Exchange was affected by repeated GNSS outages caused by passing PPDs that impacted the timestamping of financial transactions.²⁸

Jamming and spoofing represent the greatest immediate threat of all the risks that could compromise GNSS PNT. Unfriendly and friendly actors can affect GNSS PNT. The U.S. defence forces have been responsible for several compromised GPS events while developing countermeasures against jamming. In 2007, a U.S. Naval exercise testing GPS interference in San Diego harbour prevented residents from making ATM cash withdrawals, and doctors' emergency pagers stopped working – it took three days to identify their warships as the cause.²⁹

²⁸ CHAMPION 2020.

²⁹ CHAMPION 2020.

Aviation Safety Reporting System (ASRS) data released by the FAA, revealed that hundreds of aircraft lost GPS reception near military tests in 2017 and 2018. One day in March 2018, Los Angeles Air Traffic Control (ATC) received as many as 21 reports from aircraft experiencing GPS navigation problems, with some pilots requesting help to re-establish their correct course. Figure 2 shows a six month extract of aircraft types affected in 2017.³⁰

GNSS anomalies may impact some aircraft more than others because of the way complex automated flight control and navigation systems are integrated. In 2016, the FAA issued a Notice to Airman (NOTAM) warning pilots and operators of one of the best selling light jets, the Embraer EMB-505 Phenom 300, that in the event of GPS failure, the aircraft could enter a dangerous ‘Dutch Roll’ condition (unexpected rolling and yawing oscillations) at high airspeeds.³¹

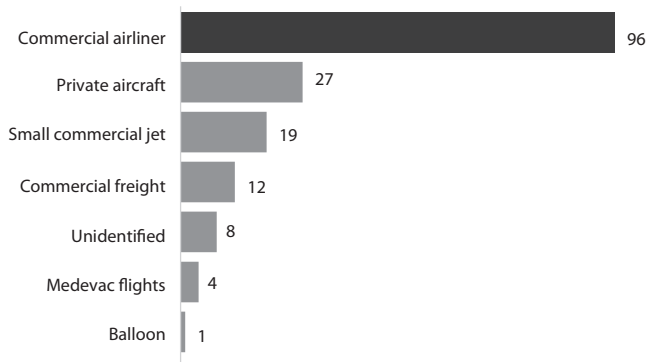


Figure 2
NASA ASRS GPS problems by Type of Aircraft Affected released by the FAA
(February to July 2017)
Source: HARRIS 2021; FAA 2016

³⁰ HARRIS 2021.

³¹ FAA 2016.

Since GNSS is so widespread, reliable and easy to use, an important human factor should also be considered. Aviators, mariners, motorists and hikers, to name just a few, may be more vulnerable to compromised GNSS if they lack basic traditional navigation proficiency. In 2019, a passenger airliner lost GPS near Salt Lake City. The pilot stated in his ASRS report: “To say that my raw data navigation skills were lacking is an understatement! I’ve never done it on the Airbus and can’t remember having done it in 25 years or more.”³²

Automatic Dependent Surveillance Broadcast (ADS-B) is an unencrypted surveillance and tracking technology required by all aircraft operating in IFR. It provides position, velocity, heading and identification data to ATC and other ADS-B users to maintain safe separation. Position is mainly determined automatically by GNSS.

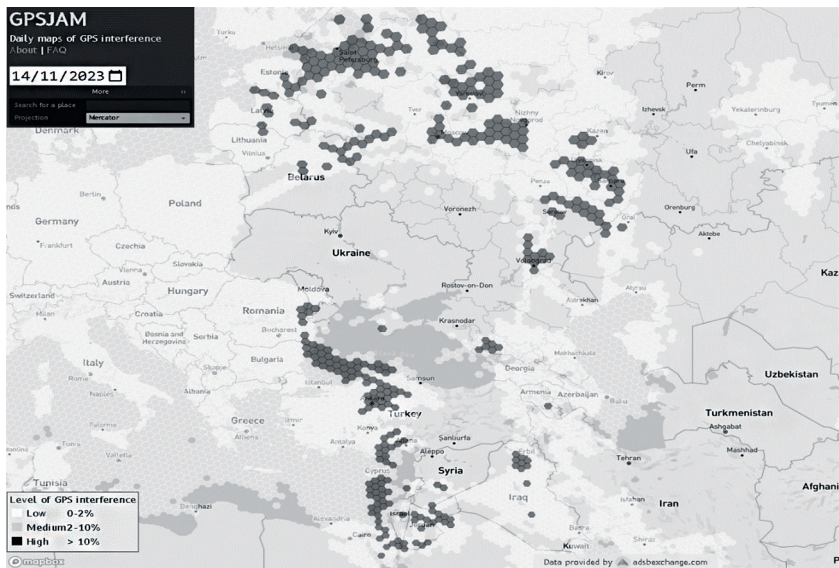


Figure 3
Screenshot with dark spots representing GPS interference >10%
 Source: gpsjam.org

³² HARRIS 2021.

The screenshot from gpsjam.org in Figure 3 uses data provided by ADS-B Exchange to generate maps of likely GPS interference based on aircraft reports of reduced navigation system accuracy without specifying the type of navigation system. It could be caused by GPS, another GNSS like GLONASS, or an Inertial Navigation System (INS) issue. Most navigation accuracy degradation occurs in the Middle East, especially in the eastern Mediterranean. Jamming activity is often observed in Iraq, Lebanon, Cyprus, Turkey and Armenia. In North Africa, Libya is also affected. Suspected jamming activity in Europe has occasionally been detected in Poland, Romania, Lithuania, Latvia and Finland.³³

Researchers analysed air traffic impacted by GPS interference over Eastern Europe between February and August 2022. On some days, this affected more than 1,000 flights or 60% of the daily traffic in the analysed area.³⁴ In February 2023, the European Union Aviation Safety Agency issued a Safety Information Bulletin warning pilots of degraded navigation or surveillance because of GNSS outages from jamming and possible spoofing.³⁵

GNSS jamming is harmful, but spoofing is a far more insidious threat. According to David Last, former president of the U.K.'s Royal Institute of Navigation: "Jamming just causes the receiver to die, spoofing causes the receiver to lie."³⁶

Malicious actors spoof or replicate satellite navigation signals by blocking the original transmission with a stronger, false, identical signal that the GNSS receivers then use. Meaconing is the most common form of spoofing attack, where GNSS signals are intercepted and rebroadcast on the same frequency, resulting in misleading location, velocity and heading.³⁷

GNSS are essential enablers for today's shipping which heavily relies on integrated IT networks and Industrial Control Systems (ICS). Many merchant

³³ WISEMAN 2022.

³⁴ FIGUET et al. 2022.

³⁵ EASA 2023.

³⁶ DAWSON 2018.

³⁷ LO 2019.

vessels' ICS will not even allow engines to start or leave port without receiving a valid GNSS signal.³⁸

Malicious state and non-state actors could use GNSS spoofing to create ship-to-ship or ship-to-shore collisions, diversion into hostile territories for military gains or terrorism purposes or be used by pirates to intercept and divert ships into vulnerable areas.

A maritime transport industry source reported that the captain of a Post-Panamax³⁹ class container ship en route from Cyprus to Djibouti in February 2017 could not manoeuvre when “the IT system of the vessel was completely hacked”. For 10 hours, pirates successfully remotely hacked the vessel's satellite navigation system to effectively control the throttle and steering to divert the vessel to an area where they planned to board and take over.⁴⁰

Students demonstrated how easy it was to ‘hijack’ and reroute an \$80 million superyacht 30 miles off the coast of Italy using a \$1,000 device they built to spoof GPS signals, without triggering an alarm or alert. In March 2016, GPS jamming signals along the North Korean border affected over 1,000 aircraft and 700 ships for over a week.⁴¹

Since February 2016, nearly 10,000 suspected instances of GNSS spoofing have been identified, affecting more than 1,300 commercial vessels. The disruptions appear to have originated from ten or more locations in Russia and Russian-controlled areas in Crimea and Syria.⁴² One of many examples of adversarial jamming occurred during the Ukraine war in October 2023. The Russians deployed their Pole-21 GNSS jammer (which also blocks GLONASS) to interfere with incoming drones and other precision-guided munitions. However, on this occasion, the Russian jammer became the target and was destroyed.⁴³ In October 2023, the U.S. Department of Transportation (DoT)

³⁸ AKPAN et al. 2022.

³⁹ A merchant vessel with 8,250 Twenty-Foot Equivalent Unit (TEU) container capacity, ~366 m long and 49 m wide.

⁴⁰ BLAKE 2017.

⁴¹ AKPAN et al. 2022.

⁴² Center for Advanced Defense Studies 2019.

⁴³ AXE 2023.

Maritime Administration issued a warning that “significant GPS interference has been reported worldwide” and that the unencrypted AIS can be spoofed.⁴⁴

On 25 September 2023, twenty civil aircraft in northern Iraq experienced a GNSS spoofing attack, creating false track positions of around 60 nautical miles. A Boeing 777 airliner was so far off course that the crew asked Baghdad Air Traffic Control: “What time is it, and where are we?” Two days later, the FAA issued a NOTAM warning of potential spoofing activities in Iraq and Azerbaijan that could pose a safety of flight risk, leading to potential accidents or loss of life.⁴⁵

According to reports from some of the affected pilots, the built-in safety systems, such as Receiver Autonomous Integrity Monitoring (RAIM), could not identify or discriminate between a legitimate and spoofed GNSS signal. Modern Flight Management Systems (FMS) use navigation inputs from Radionav and GNSS, with some also equipped with Inertial Measurement Units (IMU) or Inertial Navigation Systems (INS), which integrate an IMU with GNSS. Unless the flight crew is aware of a GNSS spoofing event and can disengage the GNSS inputs, the FMS will accept the invalid spoofed PNT data, affecting the entire system.

Space weather is a natural hazard that can affect GNSS. In 1859, a solar Coronal Mass Ejection (CME) caused the most intense geomagnetic storm facing Earth in recorded history. Known as the Carrington Event, it created havoc on telegraph communications networks worldwide in an era well before satellites and GNSS. The U.K. Government listed adverse space weather as one of the most serious natural hazards in its National Risk Register.⁴⁶ Apart from a Carrington scale CME, space weather is unlikely to cause satellite failure because of their robust, hardened design. However, GNSS errors can be caused by more frequent severe space weather events, which create scintillation in the ionosphere that adversely affects space-to-earth

⁴⁴ MARAD 2023.

⁴⁵ ZEE 2023.

⁴⁶ MAY et al. 2022.

signals. In December 2006, a major solar flare disrupted GPS and satellite communications for around 10 minutes.⁴⁷

The impact of Geomagnetic superstorms can be severe, but these are rare events. On average, there is a ~4% chance of at least one great storm and a ~28% chance of at least one severe storm per year, while there is only a 0.7% chance of a Carrington class superstorm per year.⁴⁸

Fifteen of the eighteen CNI sectors were found to be at risk of GNSS failure by the U.S. Department of Homeland Security. These included communications, emergency services, information technology, banking and finance, healthcare and public health, energy (electric, oil and gas), nuclear, dams, chemical, critical manufacturing, defence industrial base, postal and shipping, transportation, government facilities and commercial facilities.⁴⁹

*Inadvertent and hostile human activities
can compromise GNSS PNT*

The Kessler syndrome describes an uncontrolled growth of space debris (space junk) that could cause a catastrophic chain reaction of collisions with satellites and other space debris.

Space debris represents a relatively low direct threat risk to GNSS in MEO. However, the proliferation of space debris in other orbits may have indirect consequences for GNSS. In 2022, more satellites were launched than in any previous year, owing to the growth of megaconstellations⁵⁰ such as Starlink. In 2023, it was estimated that around 30,000 pieces of space debris greater than 10 cm remain in earth orbit from defunct satellites, launch vehicles, satellite collisions and other objects. Orbital debris has grown in number and total mass since the beginning of the space age, as shown in Figure 4.⁵¹ Almost 70%

⁴⁷ MALIK 2022.

⁴⁸ CHAPMAN et al. 2020.

⁴⁹ HOPTROFF–SUAREZ 2023.

⁵⁰ Constellations with hundreds or thousands of satellites.

⁵¹ COLVIN et al. 2023.

of space debris is concentrated in Low Earth Orbit (LEO), with debris below 650 km naturally deorbiting within 25 years owing to atmospheric drag.⁵²

Anti-satellite (ASAT) weapons, which can be launched from Earth or placed in orbit to destroy an adversary's spacecraft, may present a latent threat to GNSS. The USA, Russia, China and India have all developed and deployed these. In 2007, when China tested its ASAT capability in LEO, total space debris increased by 25%. In May 2013, China conducted another test that was suspected to be a kinetic kill vehicle that could potentially reach MEO and GEO orbits.⁵³

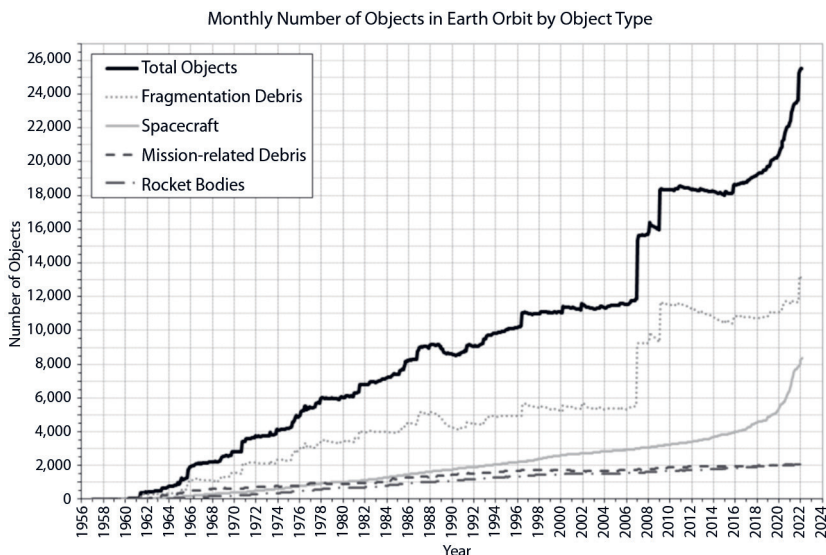


Figure 4
Chart showing the number of objects >10 cm in LEO
 Source: NASA ODPO

⁵² COLVIN et al. 2023.

⁵³ WEEDEN 2014.

Because of the serious repercussions, a direct ASAT attack from a peer adversary is improbable. However, the deployment of space weapons such as these and other provocative actions in space (and on Earth, which are harder to attribute) highlights the impotence or absence of effective international space law. These ‘Grey Zone’ hostile activities which exploit legal ambiguities in treaties are known as ‘Lawfare’.⁵⁴

The direct threat to GNSS from space debris is relatively low because MEO orbits, where most GNSS operate, are relatively clear. However, concern over this risk may rise as more PNT initiatives and capabilities are planned to be delivered from LEO. Launch and replenish missions for GNSS in MEO may be at greater risk while transiting space debris in LEO. An April 2023 study by the University of Malaga concluded that the human use of space “will disappear for both commercial and scientific activities if the current rate of space debris generation continues”.⁵⁵

Space is becoming increasingly congested and contested

Existing and proposed megaconstellations, such as ‘Starlink’ with plans for 12,000 and ‘Kuiper’ with 4,236 satellites, will be dwarfed by China’s ‘G60 Starlink’ with up to 12,000 and ‘Guo Wang’ with 12,992 satellites. The largest megaconstellation proposal comes from Rwanda, which filed its 337,320 satellite ‘Cinnamon-937’ programme with the International Telecommunications Union (ITU).⁵⁶ Up to 75,000 LEO satellites from 7 countries could operate between 328 and 2,000 km in the next ten years.⁵⁷ The scale of new LEO constellation growth can only increase the risk of collision with space debris, even if the estimated satellite population does not fully materialise. This should not present an immediate threat to MEO-based GNSS but may have implications for emerging LEO GNSS.

⁵⁴ ERWIN 2023.

⁵⁵ Innovation News Network 2023.

⁵⁶ KUTHUNUR 2023.

⁵⁷ HAINAUT 2020.

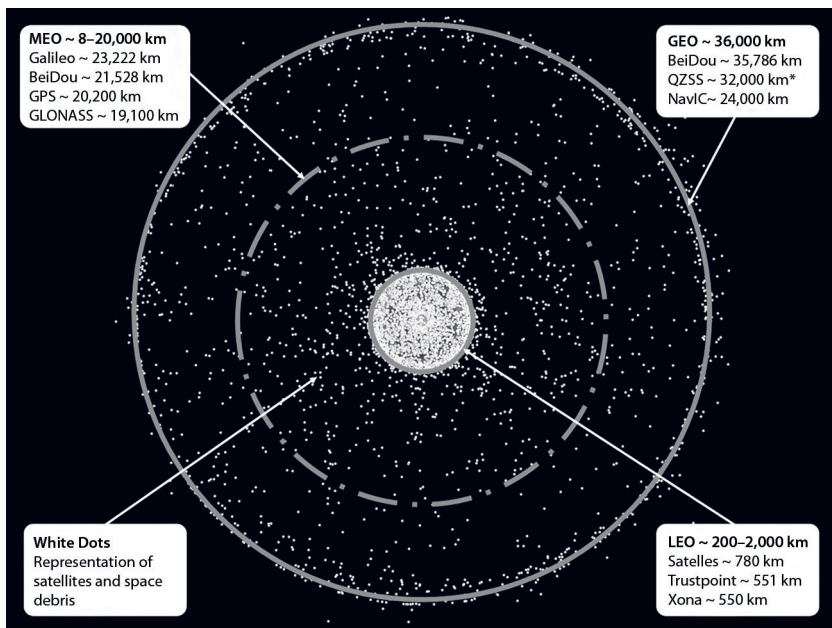


Figure 5

*LEO, MEO and GEO orbits with Satellite and Space Debris field overlay (*QZSS perigee)*

Source: Compiled by the author based on [Debris-GEO1280 p.jpg](#) and [Comparison satellite navigation orbits.svg](#)

The nominal altitudes of the LEO, MEO and GEO GNSS/RNSS orbits together with an overlay of current satellites and space debris fields are presented in Figure 5. The density of space debris is greatest in the LEO orbits where it exhibits the greatest risk to space operations, especially with the growth of emerging megaconstellations.

Radio Frequency Interference to GNSS can compromise PNT. GNSS operates in L-Band (1 to 2 GHz) because the propagation characteristics of these radio frequencies are ideal for all weather operations day and night as they can penetrate clouds, precipitation, fog and vegetation. The ITU has allocated separate L-Band frequencies between 1.1 GHz and 1.6 GHz for each

of the 4 GNSS and 2 RNSS operators.⁵⁸ However, national administrations are responsible for the local licensing and permitted use of frequencies within the ITU global and regional allocations.

In 2020, the U.S. Federal Communications Commission (FCC) approved using a portion of L-Band to Ligado, a 5G cellular phone operator, provided they separated their transmissions from GPS systems.⁵⁹ However, the U.S. Department of Defense (DoD) commissioned a study which confirmed that Ligado's planned 5G deployment would interfere with DoD GPS receivers. The DoD report rejected the FCC's suggested mitigation and replacement plans as unfeasible, prohibitively expensive and possibly ineffectual.⁶⁰ The concerns raised by the DoD were also raised by the U.S. aviation industry, which determined that Adjacent Channel Interference from this 5G network could pose a safety risk to civil aviation.

Interference with radio navigation satellite services has become so widespread that the ITU published a warning in August 2022 stating: "Between 1 February 2021 and 31 January 2022, ITU received 329 reports of harmful interference or infringements of the Radio Regulations"⁶¹ and tabled this item at the 2023 World Radiocommunication Conference.

Food security may be at risk from compromised PNT

A GEO Inmarsat communications satellite provides GNSS augmentation in the Asia-Pacific region, enabling two-centimetre guidance accuracy for self-driving agricultural machinery. In April 2023, a suspected fault in one of the satellite's solar arrays interrupted all services, including Precision Agriculture, dependent on this capability. Farmers across Australia and New Zealand reported that their farm machinery was down for three days during the peak

⁵⁸ ITU 2020.

⁵⁹ PELKEY 2020.

⁶⁰ U.S. DoD 2022.

⁶¹ ITU 2022.

of the sowing season. One farmer said “the outage had taken his operation back about 25 years”. Another farmer with 1,700 hectares complained that a lot of boom sprays were out of operation, stating: “I haven’t been in a tractor without auto-steer for 15 years.” He was forced to use a backup free-to-air GPS that was much less accurate.⁶²

Failures of this nature are quite rare, but events such as this, affecting a broad user community including aviators, mariners and farmers, illustrates how space assets and orbital altitudes outside of GNSS MEO can have an impact on PNT when compromised.

Systemic and human factors can compromise PNT

All GNSS have experienced failures. At 23:26 UTC on 25 January 2016, a 13.7 microsecond error occurred during a data upload while retiring a single GPS satellite. This resulted in incorrect timing data being transmitted throughout the global constellation. The data error impacted telecommunications networks in the U.K., triggering hundreds of alarms while Digital Audio Broadcast radio services were disrupted. At the same time, public safety communications in the USA and digital TV services in Spain were also affected. The timing error, which also affected other GPS-dependent systems and services such as ATMs, continued for over half a day until the anomaly was corrected at 13:11 UTC on 26 January.⁶³

Although this specific fault only affected timing and did not disrupt positioning and navigation, a small but very important community of users worldwide were severely impacted by the timing fault. The severity of the impact was related to the specific design and implementation of the user’s PNT equipment and data processing systems.

⁶² CLAUGHTON-CONN 2023.

⁶³ KOVACH et al. 2016.

The Russian GLONASS and the Chinese BeiDou systems have also experienced various technical issues. However, none of these events can be compared to the weeklong outage of Galileo from 10 to 17 July 2019. The outage was caused by a ground infrastructure issue during an essential upgrade of the Galileo control centre, not by the Galileo satellites. The impact of this outage could have been far more severe if the 100 million plus Galileo receivers could not automatically switch to GPS as backup.⁶⁴ Because of this failover capability, most casual users would have been unaware of this extended Galileo system failure.

Outages from most of these causes are quite rare, and several interventions have been applied. However, this will not eliminate other systemic risks that could also compromise PNT.

The cost and impact of compromised GNSS PNT

The financial benefits to the U.K. from using GNSS have been monetised at £13.6 billion per annum. The economic loss due to a seven-day GNSS outage has been estimated at £7.6 billion.⁶⁵ A loss of GPS in the U.S. was estimated to have a \$1 billion per day impact, which could be 50% higher if this were to occur during the April and May planting season, owing to the widespread adoption of GPS-dependent Precision Agriculture.⁶⁶ Between 1999 and 2027, GNSS was estimated to contribute around €2 trillion in economic benefits and 100,000 highly skilled jobs in the EU.⁶⁷

Not all analysts agree that the risks and impact of compromised PNT justify large investments in backup GNSS. The U.S. think tank, the RAND

⁶⁴ TODD 2019.

⁶⁵ FLYTKJÆR et al. 2023.

⁶⁶ O'CONNOR et al. 2019.

⁶⁷ BONENBERG et al. 2023.

Corporation, issued a report in May 2021 entitled “Analyzing a More Resilient National Positioning, Navigation, and Timing Capability”, which asserted that “the risks of potential attacks or other failures of such systems may be exaggerated, and even impossible in some instances”.⁶⁸

Most of the risks and some of the alternative PNT solutions to GPS cited in the RAND report are valid and aligned with many of those identified in this analysis. However, it is difficult to give unqualified acceptance to their conclusions given the extent of natural and growing human threats that could compromise GNSS PNT, some of which cannot be easily mitigated. Some of the conclusions in the RAND report have also been challenged by several industry specialists, including Dana Goward, President of the Resilient Navigation and Timing Foundation and Dr Patrick Diamond, member of the (U.S.) President’s National Space-based PNT Advisory Board.⁶⁹ The basic premise of the RAND report was a cost–benefit assessment of a duplicate backup GPS system. Perhaps the report should have placed greater emphasis on wider alternative solutions to ensure PNT is not compromised.

It is difficult to compile an accurate comparative threat probability vs. impact assessment of the seven main threats to GNSS PNT as there is little data available with a common baseline. Furthermore, the scale of impact can be measured in many ways such as geographically, temporarily, safety of life, economic or social. However, a coarse qualitative assessment of the relative probability and impact of seven major natural and human threats to GNSS PNT is proposed in Figure 6.

Even if a precise assessment of specific threats to PNT could be convincingly accomplished, it is unlikely that such findings would alter the conclusion. The significant impact of denied access to accurate PNT is so great that adequate technical and financial investments in mitigation would be justifiable.

⁶⁸ MASON et al. 2021.

⁶⁹ GOWARD 2021.

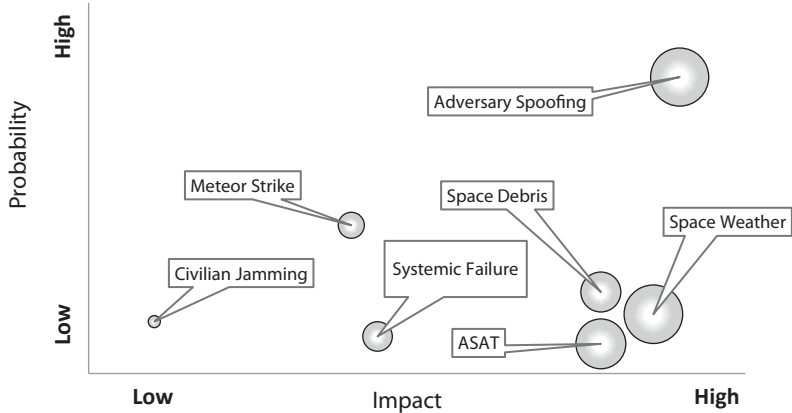


Figure 6

Threat probability vs. impact and scale (coarse qualitative assessment)

Source: Compiled by the author.

RESILIENT PNT INITIATIVES

The U.S. DoD recognises the importance of resilient PNT capability with the rollout of up to 32 upgraded next generation GPS III/IIIF satellites. These new satellites are three times more accurate, with an eight-fold improvement in anti-jamming capabilities, as well as greater compatibility and connectivity with other GNSS, such as Galileo.⁷⁰ The U.S. is not alone in undertaking initiatives to address space and Earth threats to minimise the risk of compromised PNT.

Redundancy and diversity in the space segment already exists. Over 100 GNSS satellites are in orbit within the four constellations operated by the U.S., Europe, Russia and China.⁷¹ Access to such a large population of GNSS satellites also improves accuracy and coverage. Together with the two RNSS constellations from India and Japan, the impact of a system outage, like the

⁷⁰ Lockheed Martin 2023.

⁷¹ GNSS from Russia and China may not be appropriate for all users.

January 2016 GPS or July 2019 Galileo events, is less likely to be as great, provided that user terminals can safely operate across all these systems.

Although MEO is used by the four existing GNSS, LEO is about to play a bigger role in contributing to PNT. Startups, such as Xona, Trustpoint, Satelles and Future Navigation Technology, are proposing PNT augmentation solutions that can offer up to 10 times the accuracy of GPS using LEO satellites with increased signal strength, enhanced security and worldwide coverage.⁷²

Successful PNT trials with Starlink as a Signal of Opportunity (SoP) have led to the company filing with the U.S. Patent and Trademark Office in December 2022 for “electronic global positioning and geo-locations systems”.⁷³

Researchers have developed an algorithm that can use a SoP from almost any satellite to locate any point on Earth with an accuracy of up to 5.8 metres for a stationary receiver.⁷⁴ Other LEO PNT solutions use the global Iridium constellation, which operates within the same L-Band as GNSS but on different frequencies. While it delivers a stronger signal than MEO GNSS, it does so with lower position and timing accuracy. Using SoP from non GNSS constellations such as Iridium has been examined to include other megaconstellations such as Starlink, OneWeb and Kuiper. Further research is needed, but these opportunities would require significant investment in user terminals and may not be universally accepted.

A LEO GNSS constellation from Xona Space Systems will consist of around 300 CubeSats,⁷⁵ which will provide sub-10 cm accuracy anywhere on Earth, independently⁷⁶ or to enhance legacy GNSS.⁷⁷ Geespace, a privately owned Chinese subsidiary of Geely, is rolling out a constellation of 240 LEO PNT satellites, with the first phase of 72 to be in orbit by 2025 to support their future

⁷² BONENBERG et al. 2023.

⁷³ DENNEHY 2022.

⁷⁴ WOODALL 2023.

⁷⁵ Miniaturised satellites less than 2 kg with a standardised form factor in multiples of 1 or more 10 cm³ units.

⁷⁶ With degraded performance in the absence of GNSS or ground sourced clock disciplining.

⁷⁷ LUCCIO 2023.

self-driving cars.⁷⁸ Another Chinese LEO constellation from Future Navigation (CentiSpace/Xiangrikui) has launched 6 out of a planned constellation of 120 PNT microsatellites to provide GNSS augmentation using laser Inter Satellite Links.⁷⁹ A conceptual design has been developed by the Iranian Ministry of Science Research and Technology to provide regional PNT using Commercial Off the Shelf LEO CubeSats.⁸⁰

In urban environments where GNSS is challenged or denied, it may be possible to obtain PNT using non-satellite SoP from diverse terrestrial radio frequency sources such as digital radio, TV, broadcast AM/FM and cellular radio signals, but only using special receivers.⁸¹ An example of such a novel solution is the StarNav Multi-Frequency Positioning and Timing Receiver. This is an aided inertial navigation system powered by one or more SoP such as cellular, television, Globalstar, Iridium, GPS or Xona Pulsar.

The benefits of diversity in space using multiple constellations, including SoP or LEO, can only be realised if the GNSS receivers are capable of using them. This may require substantial investment and re-fit across all sectors globally, considering that the number of installed GNSS devices are projected to grow from 5.6 billion in 2023 to almost 9.0 billion in 2033.⁸² However, solutions that can employ legacy hardware with firmware upgrades or minimal integration could streamline adoption.

Augmentation systems improve the accuracy, availability and integrity of GNSS PNT. Satellite Based Augmentation Systems (SBAS) provide PNT augmentation using GEO satellites to monitor signals received from GNSS at accurately surveyed sites to compare any error between the actual position and GNSS fix. These errors are uplinked to GEO satellites, which then broadcast any identified errors that are corrected by special user terminals. SBAS does not provide independent PNT; it only augments existing GNSS over a specified

⁷⁸ Geely 2022.

⁷⁹ KULU 2023.

⁸⁰ NASEH et al. 2021.

⁸¹ KASSAS 2021.

⁸² EUSPA 2024.

wide area. Four major SBAS systems are in place, including the European Geostationary Navigation Overlay Service, U.S. Wide Area Augmentation System, Japanese Multi-functional Satellite Augmentation System and the Indian GPS Aided Geo Augmented Navigation system.⁸³ The joint Australian and New Zealand Southern Positioning Augmentation Network uses Inmarsat GEO communications satellites to deliver SBAS accuracy down to 10 centimetres.⁸⁴

GBAS delivers high accuracy and integrity navigation for aircraft, making precision approaches to airports using GPS as an alternative to ILS. GBAS broadcast integrity values via VHF data link to the aircraft ILS style avionics to achieve protection levels of an actual vertical (4 m) or lateral (16 m) error being less than 1 in 10 million.⁸⁵

Another integrity architecture employed in aviation is the Aircraft Based Augmentation System (ABAS), which focuses on integrity rather than accuracy. ABAS is achieved with two techniques: Receiver Autonomous Integrity Monitoring (RAIM), which only uses GPS for inputs and Airborne Autonomous Integrity Monitoring (AAIM), which uses GPS and other on-board sensors.⁸⁶ Whereas RAIM only provides horizontal integrity. Advanced RAIM uses GPS and Galileo to increase the diversity and integrity of signals, especially ionospheric errors, to deliver 3D positions with improved integrity.⁸⁷

All these systems greatly enhance integrity but are not invincible to malicious or inadvertent jamming.

*Technical, voluntary and regulatory initiatives
to mitigate the risk of space debris*

Re-usable launch vehicles such as SpaceX, Blue Origin, United Launch Alliance and Rocket Lab may partially help alleviate the amount of space debris

⁸³ GRUNWALD 2023.

⁸⁴ Geoscience Australia 2023.

⁸⁵ FAA 2023.

⁸⁶ ESA 2014.

⁸⁷ COZZENS 2022.

compared to conventional launchers. Voluntary guidelines have been proposed by the Space Safety Coalition, which recommends the responsible design, management and disposal of space assets.⁸⁸ Regulators and space agencies are also taking action. The European Space Agency (ESA) introduced the Zero Debris Charter on 16 October 2023, intending to reduce debris in Earth and Lunar orbits by 2030.⁸⁹ The U.S. FCC has gone one step further in October 2023 by imposing a fine of \$150,000 to DISH, the operator of EchoStar-7, for failing to properly deorbit this satellite, which ran out of fuel and remains in orbit 178 km above the Earth.⁹⁰

Several space debris removal methods are being proposed and developed that range from ground and space based lasers to 'nudge' small debris (1–10 cm) into re-entry, through to physical sweeping, collection or recycling of larger objects (≥ 10 cm).⁹¹

Alternative capabilities that can deliver PNT

The European Commission Joint Research Centre initiated a project to analyse technologies that could deliver Alternative PNT independently from GNSS. The U.S. DOT commissioned an assessment of seven different Alternative PNT systems in May 2020. These include PNT systems based on networks of sparse radio beacons, a LEO satellite constellation providing a timing service on the ground, eLORAN, fibre optic networks with time and frequency transfer and navigation using map matching.⁹² The U.K. Government announced its '10 Point Policy Framework for Greater PNT Resilience' in October 2023. This includes setting up bodies and assessing alternative space and terrestrial based

⁸⁸ SSC 2023.

⁸⁹ ESA 2023c.

⁹⁰ WIKUIST 2023.

⁹¹ IYER 2023.

⁹² BONENBERG et al. 2023.

PNT capabilities, including U.K. SBAS, eLORAN, U.K. Quantum Navigator and a possible U.K. sovereign regional satellite system.⁹³

eLORAN offers many advantages over GNSS as its LF signal is three to five million times stronger with 99.999% reliability and availability. It can be used within buildings, in tunnels, underground and underwater. By applying encryption and authentication, it could provide spoof-resistant PNT throughout the U.S. using only six towers for timing and 19 for position and navigation.⁹⁴

Improvements in GNSS receivers, antennas and cybersecurity measures can contribute to a non-compromised PNT capability. Historically, shipboard systems were not designed to deal with cybersecurity threats. AIS does not employ authentication or integrity checks. Electronic Chart Display and Information Systems use input from multiple unsecured sensors. ICS relies on complex legacy systems, with some IT networks configured for third party remote access that are not effectively isolated from steering and navigation systems. Recognising these and other vulnerabilities, the International Maritime Organization mandated cybersecurity countermeasures to be employed from January 2021.

Galileo was the first satellite system to employ Open Service Navigation Message Authentication as an anti-spoofing method by authenticating the consistency of data signals from multiple satellites.⁹⁵

Aircraft operations are particularly susceptible to jamming and spoofing of GNSS PNT, even where GBAS is employed, because of the omnidirectional characteristics of most GNSS antennas. As a countermeasure, special anti-jamming antennas using sophisticated algorithms to identify any anomalies, block false signals that come from near the horizon while only accepting valid signals coming directly from above.⁹⁶

⁹³ FREEMAN 2023.

⁹⁴ SHEPARD 2020.

⁹⁵ ESA 2021b.

⁹⁶ HANDRIGAN 2022.

*Use of non-GNSS PNT sources independently
or integrated with GNSS*

Before GNSS, Inertial Navigation Systems (INS) provided aviators and mariners with an accurate Attitude and Heading Reference System source. Historically, these systems were large, expensive and power-hungry. Modern INS uses IMUs that typically contain a three-axis gyroscope, accelerometer and sometimes a magnetometer to measure angular rate and acceleration but do not retain the same level of accuracy over time as GNSS. Compact ‘postage stamp size’ INS are now available in low-Cost Size, Weight and Power (C-SWaP) form factors, with some units integrating GNSS modules as little as 11 cm³, 16 grams with less than 500 mW power consumption.⁹⁷ Future INS could employ Atomic Interferometer Gyroscopes that use tiny gyroscopes and atom interferometry techniques with lasers to derive accurate positioning. These devices could operate independently of GNSS and compete with current ring laser gyroscopes, fibre optic gyroscopes and hemispherical resonator gyroscopes.⁹⁸

For time-sensitive systems or applications that cannot withstand long ‘holdovers’ (loss of synchronisation with other devices or systems), there is a need to provide accurate timing backup in the event of GNSS failure or when operating in natural or urban canyons. Low C-SWaP atomic clocks such as Microchip’s CSAC-SA65 or Orolia’s MRO-50 employ a miniaturised rubidium oscillator offering superior timing oscillator holdover of anywhere between 11 and 29 hours compared to crystal oscillators that only provide holdovers of 9 minutes to just over an hour.⁹⁹ However, these devices can only provide short-term continuity of service by extending holdover until GNSS PNT is restored. In the next five to ten years, miniaturised quantum clocks may offer a more resilient and superior timing capability accurate to the picosecond compared to around 30 nanoseconds for GPS.¹⁰⁰

⁹⁷ Vectornav 2021.

⁹⁸ SHEPARD 2020.

⁹⁹ GARIGEN et al. 2021.

¹⁰⁰ FREEDBERG 2023.

Non-terrestrial platforms that could support PNT

Very Low Earth Orbit (VLEO) between 100–450 km (nominally 250–350 km) has the advantage of low launch costs at an orbital altitude relatively safe from space debris. However, this would be at the cost of reduced orbital lifetime and the need for larger constellations to provide adequate coverage. ITU regulations place constraints on power levels if operating in the same GNSS L-Band. High Altitude Long Endurance or High Altitude Platforms may potentially be employed for local PNT augmentation or emergency restoration, which could be done relatively quickly at a significantly lower cost than space-based vehicles. However, these systems would need access to a Stratum-0 reference¹⁰¹ to maintain timing accuracy, typically from existing GNSS, so they would potentially only offer augmentation, not substitution.

Space weather, debris or meteor impact mitigation

The main mitigation for space weather risks includes shielding, component tolerances and design redundancy within the space vehicle. Some constellations include ‘hot standby satellites’¹⁰² in orbit or on the ground. Less common are evasive manoeuvres for kinetic impact threats by temporarily aligning the satellite to expose the smallest area to known meteor showers or debris.¹⁰³ Should a Kessler syndrome event ever occur, this would almost certainly end all space operations at the affected orbital altitude.

Satellites in MEO orbit are exposed to ten times the radiation of LEO,¹⁰⁴ so they are designed and shielded to survive in that environment. The U.S. GPS satellites are further hardened against High Altitude Nuclear Explosion

¹⁰¹ A high-precision timing reference such as atomic clocks.

¹⁰² A redundant satellite, not in service, that can be quickly enabled to replace a failed or retired satellite.

¹⁰³ This would require unplanned delta-v thrust consuming station-keeping fuel reducing the satellite lifespan.

¹⁰⁴ TSUIKI et al. 2014.

radiation. Although the probability of a severe Carrington-like event is extremely low, with a once in 500-year likelihood,¹⁰⁵ shielding and system redundancy are unlikely to provide sufficient protection.

Space debris and space weather represent the lowest relative risks to GNSS PNT compared to jamming and spoofing. However, all space-based assets are exposed to multiple sources of risk, some of which cannot be entirely eliminated.

*Human factors that should be considered
in a compromised PNT event*

Navigation and timing requirements were satisfied without GNSS prior to the launch of GPS in 1978. Aviators, sailors and other travellers should retain sufficient skills and recency of experience with basic navigation principles to maintain their situational and spatial awareness in the event of GNSS loss.

According to a psychologist at Temple University specialising in spatial cognition: “GPS devices cause our navigational skills to atrophy, and there’s increasing evidence for it.”¹⁰⁶ Student pilots and sailors use traditional paper charts and methods for ab initio training before transitioning onto sophisticated electronic navigation. Regulatory bodies and training organisations should retain these fundamental skills in the curriculum. Not only to provide a solid foundation but as a final fallback in the event of total GNSS loss, provided they maintain proficiency and recency!

Other initiatives to mitigate against compromised PNT

ESA has acquired several patents that could enhance or avert compromised PNT. These patents cover hardware, software, machine learning, data analysis solutions and real-time analysis to detect jamming and spoofing.¹⁰⁷ System design should consider the natural and human threats to GNSS PNT to

¹⁰⁵ MAY–DOBRIJEVIC 2022.

¹⁰⁶ STROMBERG 2015.

¹⁰⁷ ESA s. a.

ensure greater resilience. For example, infrastructure reliant on GNSS to function, such as radio communications networks, Digital Audio Broadcast radio and some digital TV services, should consider alternative architecture or ground-based stable timing sources to increase holdover times in the event of GNSS interruption.

Blended technologies incorporating GNSS with INS and potentially radio-based PNT could provide enhanced assurance for transport and mobile users. Network-based timing and low C-SWaP atomic clocks, as well as radio timing signals could provide primary, holdover or augmented timing references for some use cases.

Each of these initiatives will require various levels of technical development and financial investment. Most of these are either mature and well-established, such as multi-constellation receivers which are common in most smartphones, or are progressively being implemented such as LEO Augmentation. As there is a very broad range of platforms, use cases, environments and user terminals, it is not possible to accurately assess the cost vs. complexity of PNT capability improvements or assurance initiatives on a global scale. Notwithstanding this challenge, Figure 7 offers a coarse attempt to qualitatively estimate the relative cost vs. complexity and scale of a sample of seven of the many initiatives that could be employed to enhance the resilience and performance of PNT. Some of these initiatives can or have been combined.

Eliminating a single point of failure is one of the best ways to achieve capability resilience and assurance. Industry and governments are now recognising the extent and potential impact of threats to GNSS. An October 2023 report from the Royal Institute of Navigation recognises society's over-reliance on the GNSS PNT 'fifth utility', especially for CNI, recommending multiple alternative technologies to maintain the capability.¹⁰⁸

¹⁰⁸ POTTLE et al. 2023.

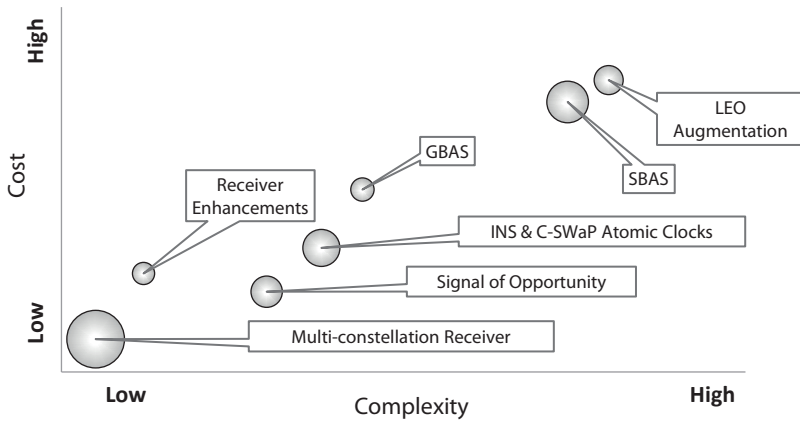


Figure 7

Initiative cost vs. complexity and scale (coarse qualitative assessment)

Source: Compiled by the author.

PNT IMPORTANCE AND CONCLUSIONS

There is little doubt that the world heavily depends on the accuracy, stability, integrity, continuity and availability of PNT. GNSS, pioneered by the U.S. GPS, has expanded the range of applications well beyond its original military function. Transportation in all three domains represents only a fraction of the use cases for PNT. This hidden utility supports communications, financial systems, agriculture, public utilities and emergency services in ways that most citizens are unaware of – that is, until PNT is compromised.

The global availability and relatively low cost of delivery and maintenance of GNSS PNT have replaced traditional radio-based systems used by aviators and mariners. GNSS PNT is a key enabler for drones, supports autonomous vehicles and revolutionises the Precision Agriculture industry. The European Union and several nations have invested in their own GNSS to deliver or augment PNT.

However, this invisible utility is fragile and vulnerable to natural and human threats, some of which cannot be mitigated. The most severe natural threats are space weather and impacts from meteors, which are reassuringly rare. The human threats in space from ASATs and space debris remain a concern.

However, the more significant human threat comes from hostile actors on Earth, with attacks growing in scope and scale that are having a measurable impact on transportation networks and other PNT users. Threats from less belligerent sources are difficult to manage owing to their localised nature and the ease with which they can be deployed at very low cost.

The significant adverse impact of compromised PNT has been evaluated in financial terms for some major economies. Although a cost–benefit assessment does not support GPS replication, the impact of unexpected PNT interruptions may be greater for some users, especially when alternative PNT fallback options cannot be easily, quickly, or economically implemented.

Nations and industries have developed countermeasures to mitigate against many of these threats. Further research and development is underway to expand the capability with ESA encouraging innovation through access to their Intellectual Property Rights.

There may be a role for terrestrial solutions such as eLORAN to provide a resilient fallback or adjunct to GNSS PNT, as would low C-SWaP INS and atomic clocks. Potentially, other platforms, such as High Altitude Long Endurance and High Altitude Platforms, may be able to deliver augmentation or restoration of GNSS, along with LEO and VLEO satellites.

The greatest challenge to mitigating compromised GNSS PNT will not be technological; it will be attitudinal. Society, government, industry and individuals often tend to accept the higher consequential costs of remediation rather than make prudent investments in prevention or mitigation.

As with all complex, high-value interventions required to address known risks, one must assess the probability of the risk occurring versus the societal and economic impact. Political imperatives make it difficult for governments to make hard choices on long-term, capital-intensive projects that reinforce or remediate an essential but invisible part of critical national infrastructure.

Some industry sectors or corporations may be reluctant to make large investments to “fix what ain’t broke”, that is, until it does break.

The G in GNSS highlights the importance of global cooperation, as very few nations will escape the adverse impacts of a compromised GNSS PNT, even with independent sovereign solutions. International maritime and air transport, as well as financial services, need access to globally available, reliable and accurate PNT.

GNSS PNT is probably used and relied upon by more people, directly or indirectly, than any other satellite service in the world.

Many of us have been lulled into a false sense of security or allowed our basic navigation skills to become less proficient, further exposing our vulnerability to compromised PNT. Greater awareness of the risks and impacts may help governments, society and industry recognise that further investment, development and implementation of alternative and backup PNT solutions should remain on the agenda. GNSS PNT is not only an invisible ‘fifth utility’; it is an indispensable utility that must be protected.

REFERENCES

- AKPAN, Frank – BENDIAB, Gueltoom – SHIAELES, Stavros – KARAMPERIDIS, Stavros – MICHALOLIAKOS, Michalis (2022): Cybersecurity Challenges in the Maritime Sector. *Network*, 2(1), 123–138. Online: <https://doi.org/10.3390/network2010009>
- ALWIN, A. (2023): The Minimum Operational Network (MON) and the Future of VORs. *National Stan Eval Newsletter*, February 2023. Online: https://web.archive.org/web/20240228173431/https://www.gocivilairpatrol.com/media/cms/CAP_StanEval_Feb_2023_ffobe8729506f.pdf
- ASCENCIO, Sheri (2021): Understanding Resilient PNT for Defense. *Safran*, 1 July 2021. Online: <https://web.archive.org/web/20240228173032/https://safran-navigation-timing.com/understanding-resilient-pnt-for-defense>

- AXE, David (2023): The Russians Installed a GPS-Jammer in Ukraine. *Forbes*, 31 October 2023. Online: <https://web.archive.org/web/20240228174346/https://www.forbes.com/sites/davidaxe/2023/10/31/the-russians-installed-a-gps-jammer-in-ukraine-the-ukrainians-blew-it-up-with-a-gps-guided-bomb>
- BARTLETT, Stephen – OFFERMANS, Gerard – SCHUE, Charles (2015): Innovation: Enhanced LORAN. *GPS World*, 23 November 2015. Online: <https://web.archive.org/web/20240228174314/https://www.gpsworld.com/innovation-enhanced-loran>
- BLAKE, Tanya (2017): Hackers Took ‘Full Control’ of Container Ship’s Navigation Systems for 10 Hours – IHS Fairplay. *RNTE*, 25 November 2017. Online: <https://web.archive.org/web/20240228174357/https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihf-fairplay>
- BONENBERG, Lukasz – FORTUNY-GUASCH, Joaquim – MOTELLA, Beatrice (2023): *Assessing Alternative Positioning, Navigation, and Timing Technologies for Potential Deployment in the EU*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2760/596229>
- BOWDITCH, Nathaniel (2022): Development of Electronic Navigation. In BOWDITCH, Jonathan Ingersoll (ed.): *American Practical Navigator*. United States: Legare Street Press.
- CASA (2016): Navigation Rationalisation Project 2016. *Airservicesaustralia.com*, 26 May 2016. Online: https://web.archive.org/web/20240909133859/https://www.airservicesaustralia.com/aip/pending/NRP_ERSA_handout_2016.pdf
- Center for Advanced Defense Studies (2019): Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria. *C4ADS*, 25 March 2019. Online: <https://perma.cc/7DJS-LTES>
- CHAMPION, Mark (2020): How to Deal with GPS Jamming and Spoofing. *CRFS*, 1 July 2020. Online: <https://web.archive.org/web/20230529075208/https://pages.crfs.com/blog/how-to-deal-with-gps-jamming-and-spoofing>
- CHAPMAN, Sandra C. – HORNE, Richard B. – WATKINS, Nicholas W. (2020): Using the aa Index Over the Last 14 Solar Cycles to Characterize Extreme Geomagnetic Activity. *Geophysical Research Letters*, 47(3). Online: <https://doi.org/10.1029/2019GL086524>
- CLAUGHTON, David – CONN, Anna (2023): Inmarsat I-4F1 Satellite Outage Disables Tractor GPS Services for Farming Operations and Some Maritime Safety. *ABC Rural*, 18 April 2023. Online: <https://web.archive.org/web/20240228181154/https://www.abc.net.au/news/rural/2023-04-18/inmarsat-i-4f1-satellite-outage-asia-pacific-gps-farms/102234678>

- COLVIN, Thomas J. – KARCZ, John – WUSK, Grace (2023): *Cost and Benefit Analysis of Orbital Debris Remediation*. NASA, Office of Technology, Policy, and Strategy. Online: https://web.archive.org/web/20240127215706/https://www.nasa.gov/wp-content/uploads/2023/03/otps_-_cost_and_benefit_analysis_of_orbital_debris_remediation_-_final.pdf
- COZZENS, Tracy (2022): Resilient PNT Is Critical, Industry Experts Say. *GPS World*, 12 May 2022. Online: <https://web.archive.org/web/20240229093722/https://www.gpsworld.com/resilient-pnt-is-critical-industry-experts-say>
- DAWSON, Linda (2018): *War in Space: The Science and Technology Behind Our Next Theater of Conflict*. Cham: Springer. Online: <https://doi.org/10.1007/978-3-319-93052-7>
- DENNEHY, Kevin (2022): Is Elon Musk Expanding Starlink to Include Satellite Positioning and Imaging Services? *Location Business News*, 26 October 2022. Online: <https://web.archive.org/web/20240228181754/https://locationbusinessnews.substack.com/p/is-elon-musk-expanding-starlink-to>
- DHgate (2024): Car GPS Signal Interference Blocker. *DHgate*, 20 February 2024. Online: <https://perma.cc/37KY-YK3Y>
- EASA (2023): Global Navigation Satellite System Outage and Alterations Leading to Navigation/Surveillance Degradation. *European Union Aviation Safety Agency*, 6 November 2023. Online: <https://perma.cc/MX27-NLEA>
- ERWIN, Sandra (2023): Space Competition Enters the Gray Zone. *spacenews.com*, 14 November 2023. Online: <https://perma.cc/BSE4-8ZRZ>
- ESA (2014): *RAIM*. Online: <https://web.archive.org/web/20240229094240/https://gssc.esa.int/navipedia/index.php/RAIM>
- ESA (2021a): *GPS General Introduction*. Online: https://web.archive.org/web/20240229095614/https://gssc.esa.int/navipedia/index.php/GPS_General_Introduction
- ESA (2021b): *Galileo Open Service Navigation Message Authentication*. Online: https://web.archive.org/web/20240229095431/https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication
- ESA (2023a): *New Galileo Service Set to Deliver 20 cm Accuracy*. Online: https://web.archive.org/web/20240229100059/https://www.esa.int/Applications/Navigation/New_Galileo_service_set_to_deliver_20_cm_accuracy

- ESA (2023b): *The Reference for Global Navigation Satellite Systems*. Online: https://web.archive.org/web/20240229130955/https://gssc.esa.int/navipedia/index.php?title=Main_Page
- ESA (2023c): *World-first Zero Debris Charter Goes Live*. Online: https://web.archive.org/web/20240229131219/https://www.esa.int/Space_Safety/Clean_Space/World-first_Zero_Debris_Charter_goes_live
- ESA (s. a.): *All Space IP – Patents*. Online: https://web.archive.org/web/2024022909552/https://www.esa.int/Enabling_Support/Space_Engineering_Technology/All_Space_IP
- EUSPA (2024): EUSPA EO and GNSS Market Report. *Euspa.europa.eu*, 23 January 2024. Online: https://web.archive.org/web/20240826093612/https://www.euspa.europa.eu/sites/default/files/euspa_market_report_2024.pdf
- FAA (2016): Flight Advisory GPS Interference Testing NAFB 16-03. *Federal Aviation Administration*, 18 June 2016. Online: https://web.archive.org/web/20240229152959/https://www.faa.gov/files/notices/2016/Jun/NAFB_16-03_GPS_Flight_Advisory.pdf
- FAA (2023): Satellite Navigation – GBAS – How It Works. *Federal Aviation Administration*, 17 February 2023. Online: https://web.archive.org/web/20240229153318/https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/laas/howitworks
- FIGUET, Benoit – WALTERT, Manuel – FELUX, Michael – OLIVE, Xavier (2022): GNSS Jamming and Its Effect on Air Traffic in Eastern Europe. *Engineering Proceedings*, 28(1). Online: <https://doi.org/10.3390/engproc2022028012>
- FLYTKJÆR, Rasmus – SABRI, Farooq – ESTEVE, Romain – JESSIE, Wesley – GOULDING, Tom – MATHEWSON, Patrick (2023): *The Economic Impact on the UK of a Disruption to GNSS*. London Economics, Final Report, August 2023. Online: https://web.archive.org/web/20240229153250/https://assets.publishing.service.gov.uk/media/652ebo446b6fb-f00odb7584e/20231018_London_Economics_Report_GNSS.pdf
- FREEDBERG, Sydney (2023): Quantum Clocks Could Revolutionize Precision Warfare within a Decade: Experts. *Breaking Defense*, 12 September 2023. Online: <https://web.archive.org/web/20240229153948/https://breakingdefense.com/2023/09/quantum-clocks-could-revolutionize-precision-warfare-with-a-decade-experts>

- FREEMAN, George (2023): Government Policy Framework for Greater Position, Navigation and Timing (PNT) Resilience. *U.K. Parliament*, 18 October 2023. Online: <https://web.archive.org/web/20240227150217/https://questions-statements.parliament.uk/written-statements/detail/2023-10-18/hcws1073>
- GARIGEN, David – TUNTEMEKE-WINTER, Alaiya – GROF, Serge – MELACHROINOS, Stavros (2021): Miniature Rb Atomic Clock Improves Military Communications Performance. *Orolia Defense and Security*, 3 December 2021. Online: <https://web.archive.org/web/20240229153352/https://docs.talen-x.com/ODS/Whitepapers/Miniature-Rb-Atomic-Clock-Improves-Military-Communications-Performance.pdf>
- Geely (2022): Geespace Successfully Launches First Nine Satellites. *Geely Technology Group*, 2 June 2022. Online: <https://web.archive.org/web/20240229154010/https://zgh.com/media-center/news/2022-06-02/?lang=en>
- Geoscience Australia (2023): Southern Positioning Augmentation Network (SouthPAN). *Ga.gov.au*, 1 November 2023. Online: <https://web.archive.org/save/https://www.ga.gov.au/scientific-topics/positioning-navigation/positioning-australia/about-the-program/southpan>
- GIANNAROS, Anastasios – KARRAS, Aristeidis – THEODORAKOPOULOS, Leonidas – KARRAS, Christos – KRANIAS, Panagiotis – SCHIZAS, Nikolaos – KALOGERATOS, Gerasimos – TSOLIS, Dimitrios (2023): Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy*, 3(3), 493–543. Online: <https://doi.org/10.3390/jcp3030025>
- GOWARD, Dana (2021): RAND: Federal Investment in Timing Network for GPS Backup Likely Worthwhile. *Gpsworld.com*, 22 June 2021. Online: <https://www.gpsworld.com/rand-federal-investment-in-timing-network-for-gps-backup-likely-worthwhile/>
- GRUNWALD, Grzegorz – CIEĆKO, Adam – KOZAKIEWICZ, Tomasz – KRASUSKI, Kamil (2023): Analysis of GPS/EGNOS Positioning Quality Using Different Ionospheric Models in UAV Navigation. *Sensors*, 23(3). Online: <https://doi.org/10.3390/s23031112>
- HAINAUT, Olivier (2020): Large Satellite Constellations & their Impact on Astronomy. *Eso.org*, 1 January 2020. Online: <https://web.archive.org/save/https://www.eso.org/~ohainaut/satellites/>

- HANDRIGAN, Brian (2022): How Common Is GPS Jamming? (And How to Protect Yourself). *Telnet Networks News*, 26 April 2022. Online: <https://web.archive.org/web/20240229154729/https://synctime.telnetnetworks.ca/news/how-common-is-gps-jamming-and-how-to-protect-yourself.html>
- HARRIS, Mark (2021): FAA Files Reveal a Surprising Threat to Airline Safety: The U.S. Military's GPS Tests. *IEEE Spectrum*, 21 January 2021. Online: <https://web.archive.org/web/20240229154915/https://spectrum.ieee.org/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests>
- HOPTRUFF, Richard – SUAREZ, Steve (2023): When GNSS Does Not Work. *GPS World*, 26 October 2023. Online: <https://web.archive.org/web/20240229155708/https://www.gpsworld.com/when-gnss-does-not-work>
- HOPTRUFF, Richard (2023): GNSS Vulnerabilities: Securing the Future of Finance with New PNT Solutions. *Finance Derivative*, 10 April 2023. Online: <https://perma.cc/A5XZ-2BBH>
- HUGUELY, Andrea (2013): American Airlines Completes Electronic Flight Bag Implementation. *American Airlines*, 24 June 2013. Online: https://web.archive.org/web/20240229155533/https://s202.q4cdn.com/986123435/files/doc_news/2013/06/1/NEW_pr_american_40968_eng.pdf
- IMO (2011): Electronic Nautical Charts (ENC) and Electronic Chart Display and Information Systems (ECDIS). *International Maritime Organization*, 1 January 2011. Online: <https://perma.cc/BY3C-2JNJ>
- Innovation News Network (2023): New Model Developed to Determine the Amount of Space Debris. *Innovation News Network*, 3 July 2023. Online: <https://www.innovation-newsnetwork.com/new-model-developed-to-determine-amount-of-space-debris/34412/>
- ISO (2021): Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. *Cdn.standards.iteh.ai*, 1 August 2021. Online: <https://web.archive.org/save/https://cdn.standards.iteh.ai/samples/73766/63c7c9dd67c147a1a7067be549d9653d/ISO-SAE-PRF-PAS-22736.pdf>
- ITU (2020): Considerations on the Use of GNSS as a Primary Time Reference in Telecommunications. *International Telecommunication Union*, 7 February 2020. Online: https://web.archive.org/web/20240229160324/https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2020-PDF-E.pdf

- ITU (2022): ITU issues warning on interference with radio navigation satellite service. *ITU News*, 23 August 2022. Online: <https://web.archive.org/web/20240229160658/https://www.itu.int/hub/2022/08/warning-harmful-interference-rnss>
- IYER, Vijay (2023): How Do You Clean Up 170 Million Pieces of Space Junk? *Federation of American Scientists*, 24 May 2023. Online: <https://web.archive.org/web/20240229161009/https://fas.org/publication/how-do-you-clean-up-170-million-pieces-of-space-junk>
- KASSAS, Zaher (2021): Navigation with Cellular Signals of Opportunity. In JADE MORTON, Y. T. – VAN DIGGELEN, Frank – SPILKER, James J., Jr. – PARKINSON, Bradford W. – LO, Sherman – GAO, Grace (eds.): *Position, Navigation, and Timing Technologies in the 21st Century. Integrated Satellite Navigation, Sensor Systems, and Civil Applications*. Hoboken: Wiley – IEEE Press, 1171–1223. Online: <https://doi.org/10.1002/9781119458555.ch38>
- KOVACH, Karl et al. (2016): GPS Receiver Impact from the UTC Offset (UTC0) Anomaly of 25–26 January 2016. *Gps.gov*, 24 October 2016. Online: <https://web.archive.org/web/20240807021656/https://www.gps.gov/systems/gps/performance/2016-UTC-off-set-anomaly-impact.pdf>
- KULU, Erik (2023): Future Navigation (CentiSpace/Xiangrikui). *Newspace.im*, 11 June 2023. Online: <https://web.archive.org/save/https://www.newspace.im/constellations/future-navigation>
- KUTHUNUR, Sharmila (2023): Over 1 Million Satellites Could Be Headed to Earth Orbit, and Scientists Are Worried. *Space.com*, 17 October 2023. Online: <https://web.archive.org/web/20240229161442/https://www.space.com/million-satellites-congest-low-earth-orbit-study-shows>
- LEITE, João Pedro (2018): A Brief History of GPS In-Car Navigation. *Ndrive*, 9 April 2018. Online: <https://web.archive.org/web/20240229161627/https://ndrive.com/brief-history-gps-car-navigation>
- LO, Chris (2019): GPS spoofing: What's the Risk for Ship Navigation? *RNTF*, 8 May 2019. Online: <https://web.archive.org/web/20240229161655/https://rntfnd.org/2019/05/08/gps-spoofing-whats-the-risk-for-ship-navigation-ship-technology>
- Lockheed Martin (2023): GPS III/IIIF. The New Generation of Positioning, Navigation and Timing. *Lockheed Martin Corporation*, 18 January 2023. Online: <https://web.archive.org/web/20240229162243/https://www.lockheedmartin.com/en-us/products/gps.html>

- LUCCIO, Matteo (2023): PNT by Other Means: Xona Space Systems. *GPS World*, 5 July 2023. Online: <https://web.archive.org/web/20240229162327/https://www.gpsworld.com/pnt-by-other-means-xona-space-systems>
- NASEH, Hassan et al. (2021): Conceptual Design of a Navigation CubeSat for Local Positioning System (Iran Region), Based on COTS Approach. *Journal of Technology in Aerospace Engineering*, 4(3), 13–1. Online: https://web.archive.org/save/https://jtae.ari.ac.ir/article_118812.html?lang=en
- NATO (2021): AIS (Automatic Identification System) overview. *Shipping.nato.int*, 22 October 2021. Online: <https://web.archive.org/web/20240909133904/https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview>
- MALIK, Tariq (2022): The Worst Solar Storms in History. *Space.com*, 20 July 2022. Online: <https://web.archive.org/web/20240229162336/https://www.space.com/12584-worst-solar-storms-sun-flares-history.html>
- MARAD (2023): 2023-013-Various-GPS Interference & AIS Spoofing. *Maritime.dot.gov*, 2 October 2023. Online: <https://web.archive.org/save/https://www.maritime.dot.gov/msci/2023-013-various-gps-interference-ais-spoofing>
- MASON, Richard et al. (2021): Analyzing a More Resilient National Positioning, Navigation, and Timing Capability. *Homeland Security Operational Analysis Center*, 11 May 2021. Online: https://web.archive.org/web/20240229171453/https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2970/RAND_RR2970.pdf
- MAY, Andrew – DOBRIJEVIC, Daisy (2022): The Carrington Event: History's Greatest Solar Storm. *Space.com*, 24 June 2022. Online: <https://web.archive.org/web/20240229171655/https://www.space.com/the-carrington-event>
- MUKHERJEE, Sohom – ZALANI, Chintan (2024): 29 Google Maps Statistics: Verified and Updated For 2024. *Onthemap.com*, 26 August 2024. Online: <https://web.archive.org/save/https://www.onthemap.com/blog/google-maps-statistics/>
- O'CONNOR, Alan C. – GALLAHER, Michael P. – CLARK-SUTTON, Kyle – LAPIDUS, Daniel – OLIVER, Zack T. – SCOTT, Troy J. – WOOD, Dallas W. – GONZALEZ, Manuel A. – BROWN, Elizabeth G. – FLETCHER, Joshua (2019): *Economic Benefits of the Global Positioning System (GPS)*. RTI International, Final Report, June 2019. Online: https://web.archive.org/web/20240229181552/https://www.nist.gov/system/files/documents/2020/02/06/gps_finalreport618.pdf

- Ordnance Survey (2023): PNT: The How, Where, and When. *Ordnance Survey*, 23 August 2023. Online: <https://perma.cc/6JD3-KG4C>
- PELKEY, Tina (2020): FCC Unanimously Approves Ligado's Application to Facilitate 5G and Internet of Things Services. *FCC News*, 20 April 2020. Online: <https://web.archive.org/web/20240229181349/https://docs.fcc.gov/public/attachments/DOC-363823A1.pdf>
- PETOVELLO, Mark (2019): What Are the Challenges to Localization in Autonomous Cars in the Arctic? *Inside GNSS*, 25 April 2019. Online: <https://web.archive.org/web/20240229182010/https://insidegnss.com/what-are-the-challenges-to-localization-in-autonomous-cars-in-the-arctic>
- POTTLE, John – FARAGHER, Ramsey – PROCTOR, Andy (2023): *Preparing for a Loss of Position and Timing*. Report of the Royal Institute of Navigation, U.K. PNT Advisory Group. Online: https://web.archive.org/web/20240229181916/https://nationalpreparednesscommission.uk/wp-content/uploads/2023/10/NPC_RIN_Preparing-for-a-Loss-of-Position-and-Timing_SEP2023HD-1.pdf
- SHEPARD, Jeff (2020): eLORAN a Terrestrial Alternative to GPS. *Microcontroller Tips*, 26 October 2023. Online: <https://web.archive.org/web/20240229182102/https://www.microcontrollertips.com/eloran-a-terrestrial-alternative-to-gps>
- SSC (2023): Best Practices for the Sustainability of Space Operations. *Space Safety Coalition*, 29 August 2023. Online: https://web.archive.org/web/20240229183536/https://spacesafety.org/wp-content/uploads/2023/08/SSC_Best_Practices_for_Space_Operations_Sustainability_v2.34.pdf
- STROMBERG, Joseph (2015): Is GPS Ruining Our Ability to Navigate for Ourselves? *Vox*, 2 September 2015. Online: <https://web.archive.org/web/20240229184021/https://www.vox.com/2015/9/2/9242049/gps-maps-navigation>
- TODD, David (2019): Galileo Navigation Signal Goes Down...and It Takes a Week to Return to Service (Updated). *Seradata News*, 15 July 2019. Online: <https://web.archive.org/web/20240229183856/https://www.seradata.com/galileo-navigation-signal-goes-down>
- TRIMBLE, Scott (2022): Precision Agriculture Policy & Adoption Outlook 2023. *Cid-inc.com*, 7 April 2022. Online: <https://web.archive.org/save/https://cid-inc.com/blog/precision-agriculture-policy-adoption-outlook-2023/>

- TSUIKI, Atsuo – UTASHIMA, Masayoshi – KOBAYASHI, Takashi – CHISHIKI, Yoshikazu – KATAYAMA, Haruyoshi – IIDA, Yukiei – KATO, Eri – OSHIMURA, Kouichi – SHINDOU, Hiroyuki – YAMAGUCHI, Hiroyuki (2014): A Study on Medium Earth Orbit Utilization. *Transactions of the Japan Society for Aeronautical and Space Sciences, Aerospace Technology Japan*, 12(ists29), 17–21. Online: https://doi.org/10.2322/tastj.12.Pn_17
- UKHO (2022): UKHO Announces Intention to Withdraw from Paper Chart Production. *U.K. Hydrographic Office*, 26 July 2022. Online: <https://web.archive.org/web/20240229184412/https://www.gov.uk/government/news/ukho-announces-intention-to-withdraw-from-paper-chart-production>
- U.S. DoD (2022): Press Release on the NASEM Section 1663 Report. *U.S. Department of Defense*, 9 September 2022. Online: <https://web.archive.org/web/20240229184629/https://www.defense.gov/News/Releases/Release/Article/3153449/press-release-on-the-nasem-section-1663-report>
- Vectornav (2021): Miniature, High-performance GNSS-Aided INS. *Vectornav*, 23 July 2021. Online: https://web.archive.org/web/20240229184441/https://www.vectornav.com/docs/default-source/datasheets/vn-200-datasheet-rev2.pdf?sfvrsn=e1a7b2ao_10
- WEEDEN, Brian (2014): Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space. *The Space Review*, 17 March 2014. Online: <https://web.archive.org/web/20240229184640/https://www.thespacereview.com/article/2473/1>
- WHETHAM, Bec (2021): Which Way Will Paper Maps Go in the Future? Cartographer Says They'll Still Be Crucial, even with GPS. *ABC News*, 14 August 2021. Online: <https://web.archive.org/web/20240229185122/https://www.abc.net.au/news/2021-08-15/paper-maps-have-a-future-says-cartographer-anthony-stephens/100303036>
- WIKQUIST, Will (2023): FCC Takes First Space Debris Enforcement Action. *FCC News*, 2 October 2023. Online: <https://web.archive.org/web/20240229184946/https://docs.fcc.gov/public/attachments/DOC-397412A1.pdf>
- WISEMAN, John (2022): GPS Jam. *Gpsjam.org*, 1 July 2022. Online: <https://web.archive.org/save/https://gpsjam.org/faq>

- WOODALL, Tatyana (2023): *This Algorithm Can Make Satellite Signals Act Like GPS*. Online: <https://web.archive.org/web/20240229185138/https://ece.osu.edu/news/2023/05/algorithm-can-make-satellite-signals-act-gps>
- ZEE, Mark (2023): Flights Misled Over Position, Navigation Failure Follows. *OPS Group*, 26 September 2023. Online: <https://web.archive.org/web/20240229185401/https://ops.group/blog/gps-spoof-attacks-irs>