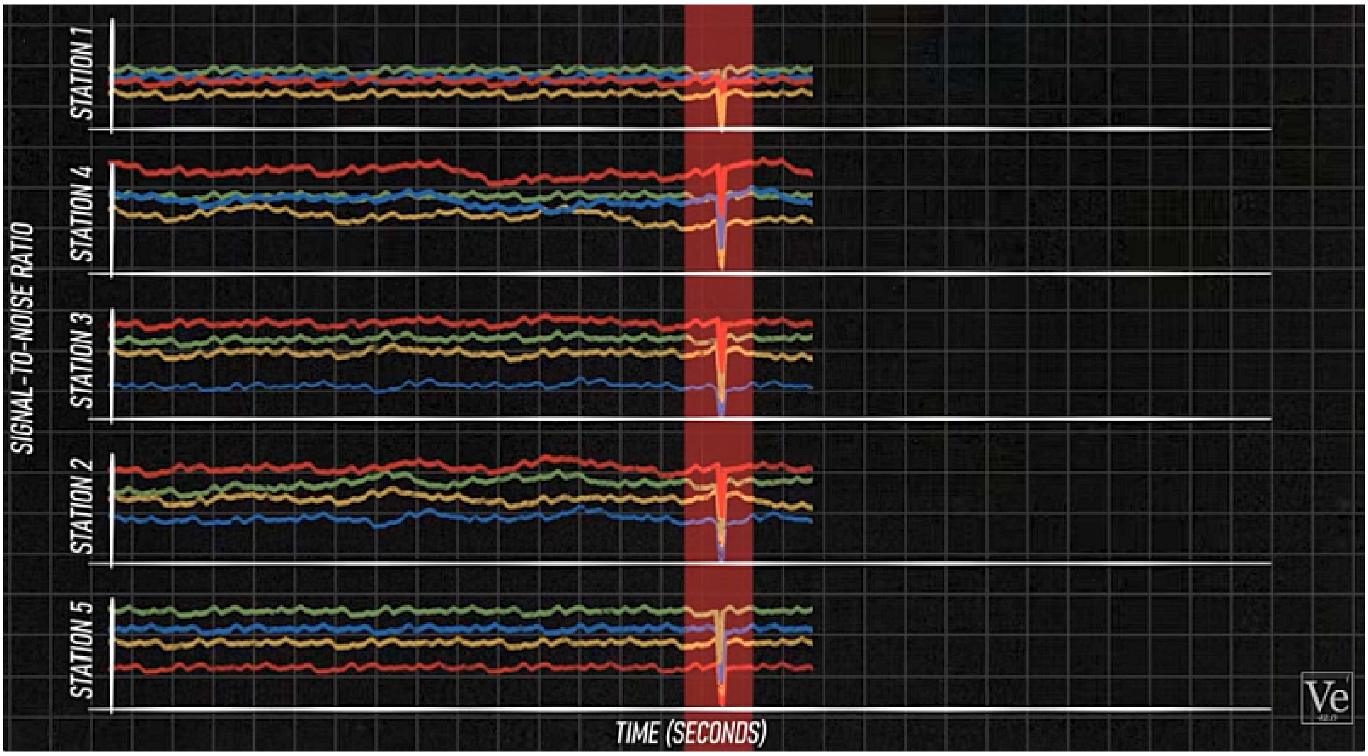
Russia’s hybrid warfare against the European GNSS system

How would you react if the sat-nav in your car suddenly stopped working? What if the mobile network went down and, all of a sudden, the power cut out too? These are, in fact, the main objectives of one of the tools of Russian hybrid warfare, the **GPS jamming**. If you happen to think this is just an empty threat, I’m afraid I must disabuse you of that notion; the Russians are already testing this capability almost every month.

In November 2024, **Professor Todd Humphreys** (*University of Texas at Austin*) was tipped off that it would be worth looking into a few specific dates in the public data from former GPS monitoring stations to get to the bottom of a strange phenomenon.

The signals from GPS satellites are recorded by several data collection stations worldwide, and there are dozens of such systems operating in Europe, too. These simply log the data from visible satellites, and these log files can be retrieved and analysed. Observers have noticed on several occasions that the European GPS signal ‘drops out’ for 2–3 seconds every few weeks *“drops out”*; all European units simultaneously detect a brief disruption in GPS activity. Looking back, 75 such days have been identified since 2019, when this same continent-wide pattern recurred – the effect was felt from Spain to Svalbard.



The moment the GNSS signals dropped out was recorded simultaneously by several stations; image: Veritasium

Let’s pause here for a moment, as I need to clarify: GPS is *‘colloquial’* term for global satellite navigation systems; let’s call them by their proper name, the **GNSS**(*Global Navigation Satellite System*). The American GPS is just one part of this entire system – albeit the oldest one still in operation – whilst the European Galileo, the Chinese BeiDou and the Russian GLONASS satellites also play a part in ensuring navigation safety. But first, let me provide the reader with some background information to highlight the significance of the case discussed in this post:

How does GPS locate us from outer space?

Imagine that the satellites orbiting the Earth are like lighthouses placed in outer space, each fitted with a super-accurate clock **lighthouses**. These satellites continuously broadcast the exact time and their own position to Earth. When our phone receives these radio signals, it calculates how long it took for the signal to reach it based on the speed of light, and from this, it works out how far away it is from that particular satellite. If our phone knows the distances to at least four of these ‘space lighthouses’ at the same time – using maths to find the points where the circles intersect – it can determine our exact position on the planet, down to the metre. The more satellites our phone can see and use at the same time, the more the data arriving from different directions corroborate each other, meaning that positioning can become accurate to within a centimetre.

What damage would a prolonged GNSS outage cause?

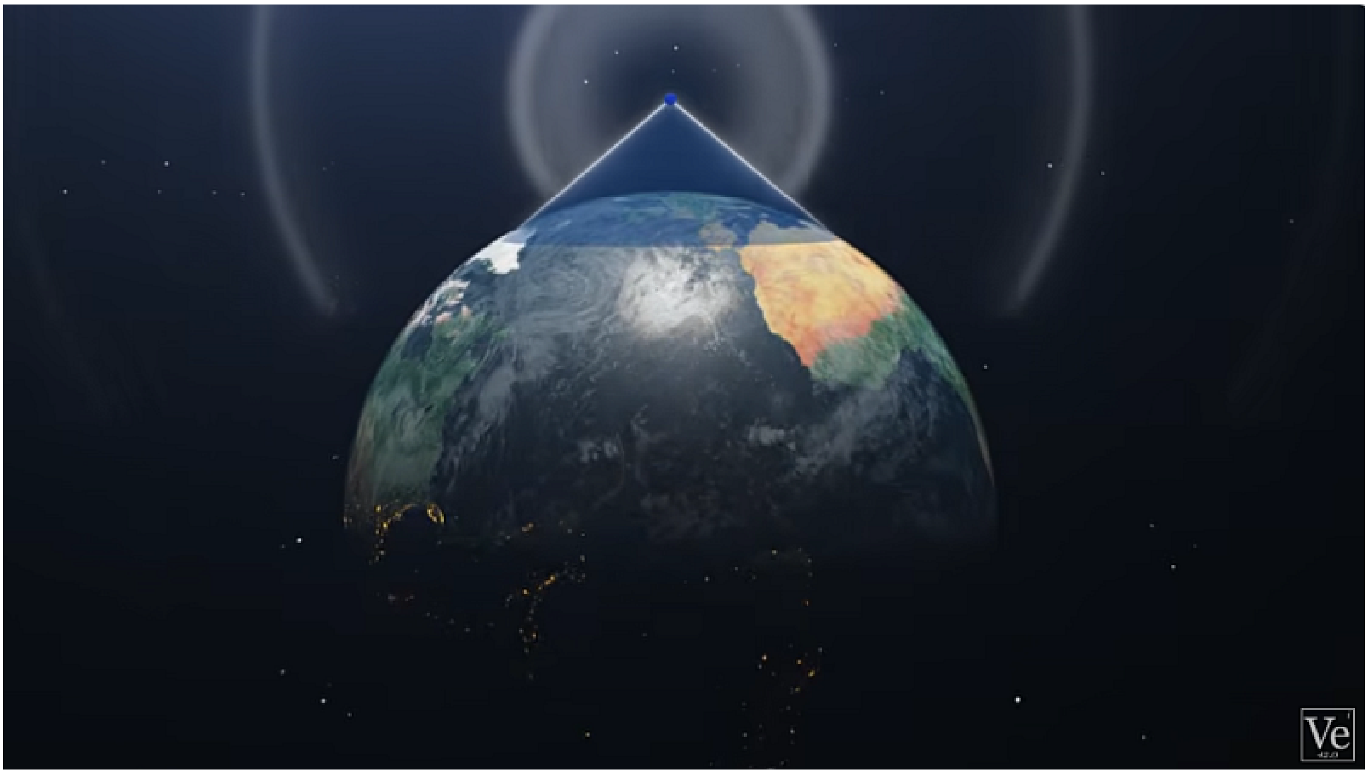
If, as part of a hybrid military operation, someone were to completely or partially disable the **GNSS** (*GPS, Galileo, GLONASS, BeiDou*) systems in Europe as part of a hybrid military operation, it would cause an immediate infrastructural and economic collapse, resulting in losses of several billion euros per day. According to OECD estimates, around 10 per cent of the modern economy relies directly on satellite-based positioning and timing (**PNT**), so the consequences would extend far beyond motorists losing access to Google Maps. Civil aviation would be paralysed immediately. Although aeroplanes can navigate using ground-based radar, airport approaches and the management of Europe's dense airspace would be impossible without GNSS. Thousands of flights would have to be cancelled or diverted to land.

Ports (e.g. Rotterdam, Hamburg) would grind to a halt, as automated container cranes and cargo ships rely on GNSS guidance accurate to the centimetre. Global supply chains would collapse within days. The *"just-in-time"* logistics networks and food delivery services would grind to a halt, causing immediate shortages of goods in supermarkets.

5G and 4G base stations synchronise the transmission of data packets with satellites to microsecond accuracy. Without GNSS, mobile networks would fall apart within hours, and calls and mobile internet would be disrupted. Electricity suppliers use GNSS time codes to synchronise the phases of the power distribution network. A loss of synchronisation could cause widespread power cuts (blackouts) across Europe.

Bank transactions, stock market trades and ATM cash withdrawals must be recorded with millisecond precision (*timestamp*). Without a satellite time signal, international bank transfers and card payment systems could automatically shut down for security reasons.

Emergency call centres would be unable to see the exact location of those in distress, and ambulances and fire engines would take longer to reach the scene without navigation, which would directly cost lives.



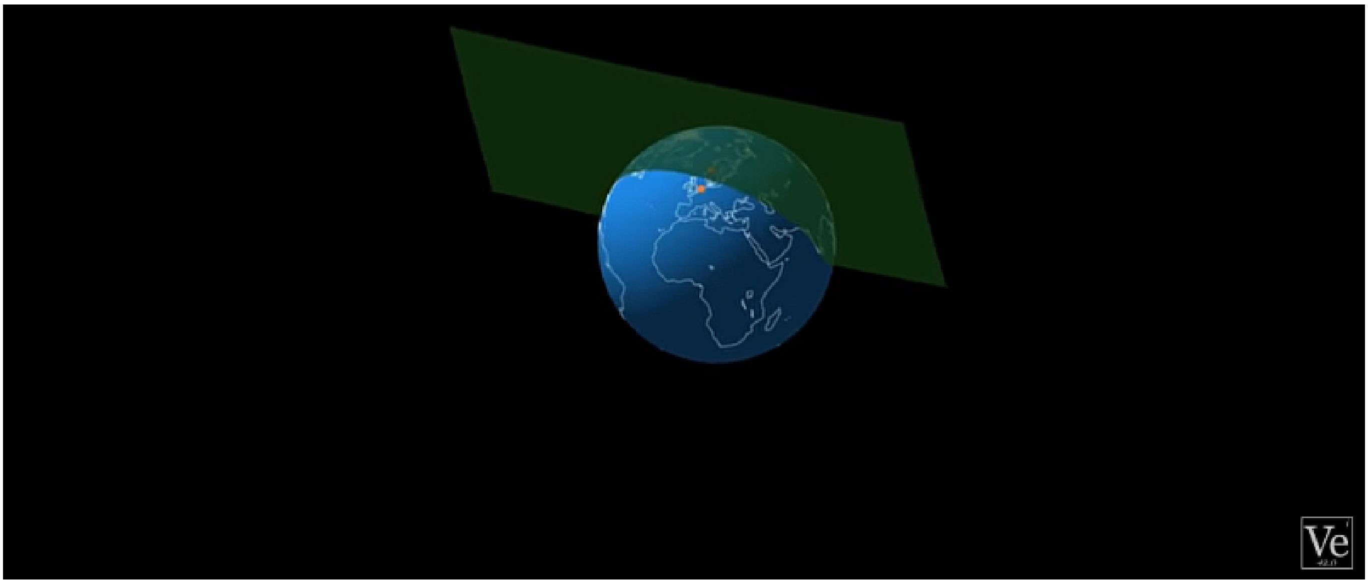
The "suspect" is believed to be at an altitude of 1,200 km; image: Vertiasium

The investigation

Initially, researchers suspected a ground-based jamming station (such as the military towers in the Russian exclave of Kaliningrad) – clearly, from the very outset of the investigation, there was no question as to which superpower's machinations lay behind the phenomenon. However, due to the curvature of the Earth, a ground-based transmitter cannot simultaneously cause coordinated interference across an entire continent. Geometric calculations showed that the source must be at least 1,200 km above the surface of the Earth.

In the early stages, the researchers narrowed the list down to 14 geostationary satellites, but the investigation stalled because the stations recording GNSS data did not record the data with sufficient (temporal) accuracy, making it impossible to narrow the field any further. The researchers shared their findings to date with other universities, hoping for their support. A breakthrough came in February 2026 when two institutes (in Amsterdam and Trondheim, Norway) simultaneously reported an outage and were able to provide highly accurate timestamps for their raw, digitised radio frequency voltage samples.

As the raw signals had been sampled at extremely high resolution, the researchers were able to determine when the interfering signal arrived in the two different cities. The signal reached Trondheim roughly 139 microseconds earlier than it reached Amsterdam. This hair's-breadth time difference defined a spatial surface (*hyperboloid*) on which the signal source must have been located.



The signal reached Trondheim roughly 139 microseconds earlier than it reached Amsterdam. This hair's-breadth time difference defined a surface in space on which the signal source had to be located.; image: Vertisium

Kosmos 2546

After the known orbits of all existing satellites were superimposed onto this mathematical model, only one spacecraft matched the measured data, and with pinpoint accuracy: the Russian **Kosmos 2546**. The satellite's orbit lay within a margin of error of just 200 metres (which is well within the uncertainty of publicly available orbital data) as it tracked the measurement area throughout the 2.3-second duration of the disturbance.

Initially, it caused some confusion that the satellite had only been launched on 22 May 2020, yet the first instances of interference had already been detected as early as 2019, but this issue was also resolved when it emerged that the satellite is part of a constellation of six satellites belonging to Russia's early missile defence warning system (**EKS / "Tundra"**) (the Russian "**Golden Dome**„).

What is the actual primary purpose of the EKS/‘Tundra’ satellite constellation?

The Tundra satellites are equipped with highly sensitive, five-spectrum optical sensors (including infrared and ultraviolet). Their primary task is to immediately detect and report the heat signatures from the engines of ballistic and hypersonic missiles launched from anywhere in the world – particularly from submarines in the oceans or from US territory – and to alert the military leadership in Moscow.

In addition, the satellites are equipped with a secondary, strictly protected communications payload. The purpose of this is to ensure the transmission of encrypted commands to Russia’s nuclear retaliatory forces in the event of a nuclear war.

Although six satellites were originally launched, the first unit (Kosmos 2510) had already become obsolete and ceased operations. The remaining four Tundra satellites form the backbone of the system, namely:

- Kosmos 2541 (Tundra 3 – Launch: 2019) – It is experiencing intermittent orbital correction and stability issues.
- Kosmos 2546 (Tundra 4 – Launch: 2020) – This is the specific satellite identified as the primary source of the GPS jamming.
- Kosmos 2552 (Tundra 5 – Launch: 2021) – This currently appears to be the most stable and reliable unit in the network.
- Kosmos 2563 (Tundra 6 – Launch: 2022) – The newest member of the constellation, although orbital anomalies were detected in this satellite during 2025.

Russia originally intended to expand the constellation to 10 units. However, due to Western sanctions following the invasion of Ukraine (in particular, the embargo on high-tech microchips and optical sensors), the Russian space industry is unable to manufacture new Tundra satellites, so the replenishment of the fleet has come to a complete standstill.

The members of the constellation are in extremely elongated, so-called **Molniya orbits** . This specialised elliptical orbit allows the satellites to slow down dramatically over the northern hemisphere and remain there for most of the day, whilst their altitude varies from 1,000–2,000 kilometres near the Earth to 40,000 kilometres far from the Earth.

The theoretical minimum altitude of 1,200 kilometres calculated by researchers coincides perfectly with that of **Kosmos 2546’s** , which was causing disruption to the continent whilst situated precisely within this near-Earth window. As the network provides global coverage, the Russians would theoretically be capable of carrying out similar GNSS jamming not only over Europe but even over the United States.

According to the raw data, Kosmos 2546 not only broadcast a powerful signal in the immediate vicinity of the GPS band (1577.5 MHz) but also at a lower frequency (1558.5 MHz), which overlaps with the frequency of the Chinese Beidou navigation system.


The interference was recorded in several European countries simultaneously; image: Vertiasium

The researchers titled their study *„Chasing Lightning: Detecting, Characterising, and Identifying a Powerful Space-Based GNSS Interference Source"* to the Institute the renowned professional organisation *of Navigation* *NAVIGATION* journal.

The The New York Times, which highlighted that the findings of the Texas-based researchers were corroborated by a completely independent European study.

Richard Bowden, of the Spanish **GMV** technology giant, confirmed with his own data that in at least three of the 75 documented cases, Russian military satellites were undoubtedly involved. The leading trade journal of the global navigation industry, the GPS World, has also covered the study in detail, noting that *the Russian embassy declined to comment on the allegations*.

Of course, anyone expecting an admission from the Russians is in for a long wait, but the sheer volume of data and measurements makes the culprit clear. Experts suggest two main reasons as to why Kosmos 2546 is bombarding the continent with only a few seconds' worth of frequency-shifted transmissions. On the one hand, this is a capability test (Todd Humphreys' theory): Russia is testing its space-based electronic warfare system in preparation for a potential armed conflict. The reason they are not transmitting directly on the GPS frequency and are only broadcasting for short periods is to avoid fully revealing the weapon's true power, whilst still verifying its functionality. According to an alternative theory proposed by another European research group, the interference is, in fact, a by-product of very short, encrypted communication messages. They use the protected navigation bands because enemy forces will not dare to jam these frequencies, for fear of paralysing their own navigation systems.

Reactions

The EU and the defence ministers of the Member States have repeatedly condemned Russia's actions. They have stated that the GPS outages experienced in the Baltic and Northern European regions directly threaten the safety of civil aviation.

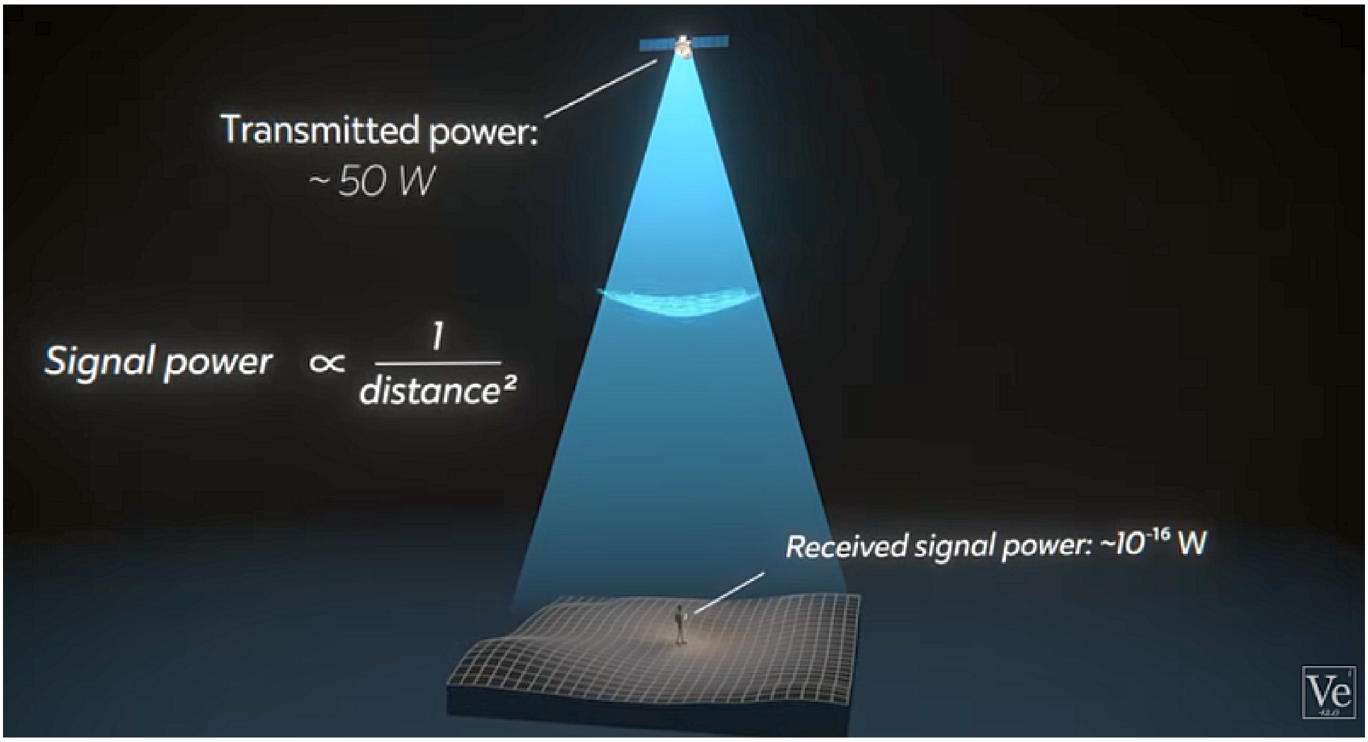
The *European Aviation Safety Agency* (**EASA**) and the *International Air Transport Association* (**IATA**) have set up a joint task force. They are continuously monitoring the geographical distribution of the disruptions and issuing Safety Information Bulletins (*Safety Information Bulletins*) to pilots.

As the source of the interference is a military satellite constellation, **NATO** has incorporated GPS protection into its collective defence strategy. Radio-electronic reconnaissance has been stepped up along the borders of the northern and Baltic member states.

US intelligence and the U.S. Space Command (*US Space Command*) assessed that this series of tests sent a clear message to both the United States and NATO. Russia has thus demonstrated that, should an armed conflict arise, it is capable of paralysing satellite navigation and the guidance of precision-guided weapons at the touch of a button, not only near the front lines but even over the American and European hinterlands.

What can be done to counter this threat?

There is no single *'silver bullet'*, which is why the EU and the aviation sector are employing a multi-layered defence strategy.



The GNSS signal is extremely weak and not difficult to jam; image: Vertiasium

The surest defence is not to rely entirely on signals from space. Across Europe, work has begun to modernise and recommission the **Loran** (*Long Range Navigation*) system, the **eLoran**.

This system is based on a network of high-power ground-based radio beacons. Due to its low frequency, the signal is extremely strong. It is roughly a million times stronger at the Earth's surface than the extremely weak GPS satellite signal, meaning that a jammer in space is unable to suppress it.

Interestingly, South Korea and China had already established their own eLoran networks, as North Korean ground-based GPS jamming is a daily problem for them.

Following the intensification of the Russian hybrid threat, the United Kingdom, Norway, and several other northern European countries have also begun rebuilding and reactivating their eLoran stations to protect critical ports and shipping routes.

Modern passenger aircraft no longer rely solely on GNSS. Ring laser gyroscopes (**RLG** – *Ring Laser Gyroscope*) and accelerometers, the aircraft's computer knows exactly which direction it is travelling in and at what speed from the moment of take-off. This is a completely closed system; it does not receive external radio signals, making it immune to interference or tampering. (The drawback is that a minimal positional error may accumulate over the course of a flight lasting several hours.)

In the vicinity of airports, the EU maintains and develops traditional, ground-based radio navigation networks (**DME** – *Distance Measuring Equipment*, **VOR** - *circular beacon*). If GPS is completely lost, pilots will be able to land with centimetre-level accuracy using these ground-based transmitters.

eLoran (enhanced Loran)

eLoran (**enhanced Loran**) is a long-range, exclusively ground-based radio navigation system, established as the primary backup for the GPS and Galileo satellite networks.

This technology is a fully digital, modernised version of the analogue LORAN-C system, which was developed during the Second World War but was subsequently superseded by GPS in the 2000s.

The system does not transmit its extremely low-frequency (100 kHz) signals from space, but rather from gigantic radio antennas built on the Earth's surface. The receiver (for example, on a ship or aeroplane) picks up signals from the surrounding ground-based towers and, based on the time difference between the arrival of these signals, precisely calculates its own position – in exactly the same way as GPS, but using ground-based transmitters. eLoran does not replace GPS, but complements it; if GPS is lost, it immediately takes its place, as it is technically almost indestructible and cannot be jammed from space.

Unfortunately, existing GPS/Galileo chips are currently physically incapable of receiving eLoran signals, as they operate on completely different frequency bands (GPS operates in the 1.2–1.5 GHz microwave band, whilst eLoran operates in the 100 kHz long-wave band).

The integration of this technology is currently at a critical transitional stage, where the miniaturisation of the chips has already been successful, but its entry into the consumer market (smartphones) is still pending. The main obstacle to eLoran finding its way into standard smartphones or cars is not the silicon chip itself, but the size of the antenna.

GPS has a short wavelength (approx. 20 cm), so even a tiny piece of metal in the corner of a phone is sufficient to act as an antenna. eLoran's wavelength, however, is extremely long (3,000 metres). Traditionally, this has required huge whip antennas.

The British **Roke** development company has developed the **ESA** , unveiled the first miniaturised eLoran antenna (**Nav-Sync Pulse**) that is just 55 mm in size and specifically designed for handheld and portable devices.

Once mass production of the miniature antennas and integrated chips developed by ESA and Roke begins, they could be incorporated into the navigation systems of premium cars and, eventually, into top-of-the-range smartphones as a secondary line of defence.

The latest posts on the blog

The story of Route 18’ (07 Aug 2026)
Point Nemo (04 Aug 2026)
LAWS (31 July 2026)
The Ozempic War (22 July 2026)
Half an hour left of your life (19 July 2026)
How thick is your book? (11 July 2026)
Orwell was wrong; bureaucracy has triumphed (5 July 2026)
Russia’s hybrid warfare against the European GNSS system (27 June 2026)
Ebola outbreak in the Congo (28 May 2026)
When a solar power station turns the desert into an oasis (13 May 2026)
Boeing 737 MAX / MCAS (5 May 2026)
The shadow of Chernobyl: Forty years after the disaster (26 April 2026)
The trivial disaster of the Mars Climate Orbiter (MCO) programme (24 April 2026)
Therac-25: The error message nobody understood (19 April 2026)
When the King is the co-pilot (17 April 2026)
Chongqing, the world’s largest city (6 May 2025)

2026/07/16 13:11 · vamsan

Dear reader! If you’ve got this far in your reading, I think I’m fair in assuming that you haven’t found this post entirely uninteresting. Oh, please don’t close the tab just yet; I’m not trying to squeeze any money out of you.

All I’m asking is that if you know anyone with whom you could have a good discussion about what’s written here, or if you’d simply like to share it with them, please don’t hesitate!

I’m still looking for opportunities to get my writing published. If you have any ideas, please do share them with me! My contact details can be found in the the Legal Notice section at.

The only platform on which passport.blog is currently published is Facebook. If you’d like to be notified of new posts, follow the Bolyongó Facebook page.

If you’d like to print this post or save it separately, the easiest way is to convert it to PDF format. You can do this using the fourth icon from the top on the right-hand side (Adobe).

Previous posts on bolyongó.hu

All posts, sorted alphabetically, indexe can be found here. Posts on the blog that are linked to specific locations can also be found on Google Maps: The true wonders of the world.

2026/07/15 22:45 · vamsan

Sources

This post was written using **Gemini AI** .

I based this post primarily on the following video from Vertiasium (the images are also taken from there):
YouTube: Something GPS jamming across Europe. Here’s what we found
GPSWord: Todd Humphreys: Russian satellites are the cause of GNSS jamming across Europe

Ars Technica: Tests suggests that Russian satellites can jam GPS on a continental scale
Gizmodo: Russian Satellites Are Jamming GPS Signals, Study Says
Humphreys, T. et al.: Chasing Lightning: Detecting, Characterising, and Identifying a Powerful Space-Based GNSS Interference Source. Published in the NAVIGATION: Journal of the Institute of Navigation.
Joint reports by the European Aviation Safety Agency (EASA) and the International Air Transport Association (IATA) on GNSS jamming in the Baltic region and Eastern Europe: EASA Pro - SIB Countering GNSS Jamming and Spoofing
Official technology announcement by the European Space Agency (ESA) and Roke Manor Research: Roke Systems – Nav-Sync Pulse Miniaturised Antenna Technical Specs.
Public tracking data for Russia’s early missile defence warning system (EKS) and the Tundra constellation orbiting in the Molniya orbit: Space-Track.org (Joint Force Space Component Command)

2026, interesting story, Todd Humphreys, tech, investigative, journalism, Russia, GPS, GNSS, Galileo, GLONASS, BeiDou, Europe, EU, blackout, Cosmos 2541, Cosmos 2546, Cosmos 2552, Cosmos 2563, Tundra, Golden Dome, Molnyija, NATO, eLoran, enhanced Loran, Nav-Sync Pulse, ESA, Roke, EASA, IATA