SciencesPo

TECH & GLOBAL AFFAIRS
INNOVATION HUB

Navigating Vulnerabilities: Cyber Security Threats and the Future of GNSS

Kezia Wexøe-Mikkelsen
Analyst, Think Tank EUROPA

Kezia Wexøe-Mikkelsen holds a Master's degree in European and International Public Policy from the London School of Economics and Political Science, and a Bachelor's degree in International Business and Politics from Copenhagen Business School. She has also been a Crown Prince Frederik Fellow at Harvard Kennedy School. Currently, she is an analyst at the Danish-based Think Tank EUROPA. Here, Kezia focuses on the technology and the digital policy domain in relation to European politics. She has previously lived in Belgium, the United States, the United Kingdom, and France, and has gained practical experience from among others, Microsoft and the quantum computing company, Pasqal.

This document is part of the Policy Brief series published by the Paris School of International Affairs (PSIA) Technology and Global Affairs Innovation Hub, edited by **Pierre Noro** under the direction of **Constance de Leusse**.

The Hub's core mission is to accelerate collaborative technology and international governance to address global challenges. Its activities are specifically focused on technology and democracy, defense and security, sustainability and prosperity.

Learn more about the Hub on our website: www.sciencespo.fr/psia-innovation-hub/

Published in May 2026.

Suggested citation: Wexøe-Mikkelsen, Kezia, *Navigating Vulnerabilities: Cyber Security Threats and the Future of GNSS*, policy brief commissioned by the Sciences Po Tech & Global Affairs Innovation Hub, May 2026.

INTRODUCTION

According to a 2023 European Union Aviation Safety Agency (EASA) report, attacks on satellites that provide positioning, navigation, and timing services (also known as Global Navigation Satellite Systems, GNSS) have been rising sharply in intensity and sophistication, especially in and above the Black Sea, Middle East, Baltic Sea and the Arctic.[1] Several of these incidents represent attacks designed to disable GNSS usage in specific geographic areas rather than unintentional disruptions caused by internal technical issues. For example, Finnair had to cancel all flights to Tartu, Estonia, for a month due to threats to their navigational systems in April 2024, which is believed to have been caused by Russia.[2] Similarly, a plane carrying European Commissioner, Ursula Von der Leyen experienced GNSS jamming of their navigation system in the summer of 2025, an incident also suspected to be linked to Russia.[3]

This surge in GNSS disruptions is alarming. Attacks on GNSS can have enormous economic, security and environmental consequences,[4] not just for navigation but also for power grids, data centers, communication networks, as well as train and financial systems which all use GNSS for timing and synchronization.[5] Monetarily, this impact is measurable: an outage of the GNSS in the UK during seven days would cost around £7 664M and the outage of the GPS system would cause an economic loss of $1B per day to the US.[6]

Recent developments have made addressing this issue even more urgent. First, the rise of geopolitical tensions, particularly Russia's 2022 aggression on Ukraine, coincided with a stark increase in attacks on GNSS. Second, several of the GNSS architectures are up for renewal. The well-known US GPS is undergoing updates and additions with the launch of the GPS Block 3F, and advanced system upgrades are scheduled for the Chinese GNSS, BeiDou. These tensions and upcoming changes question which cyber resilience measures should be put in place to anticipate and counter emerging threats on GNSS.[7]

The implications of attacks on GNSS are far-reaching. They are the symptoms of a wider trend: the evolution of the Earth's orbit as a geostrategic and increasingly militarized space. These developments challenge the ambition of the prohibition of the militarization of space and its peaceful use, as outlined in the 1966 Outer Space Treaty article IV (although the latter focuses on nuclear weapons and weapons of mass destruction).[8] Emerging threats to GNSS are contesting the foundational dispositions of this treaty and prompting a reconsideration of the international legal framework governing spatial activities.

The intensification of these new threats on systems that are critical to the world's economy has become a strategic topic for both historic institutions, such as the UN Committee on the Peaceful Uses of Outer Space (COPUOS), the International Telecommunication Union (ITU), and the International Civil Aviation Organization (ICAO), and recently created space governance stakeholders, like the US Space Force or the African Space Agency.

This policy brief brings an overview of the GNSS threat landscape and explores how rising geopolitical tensions are shaping and intensifying these risks. In doing so, it seeks to answer a central question: ***What is the Future of GNSS in light of the growing number of geopolitical tensions and cyber threats?***

This policy brief pays special attention to the diversity of stakeholders, including national governments, institutions, space agencies, civil aviation authorities, but also non-State actors, such as private technology and satellite firms, and operators of critical infrastructures.

SECTION 1 - BACKGROUND: WHAT ARE GNSS AND WHY ARE THEY IMPORTANT?

a. GNSS: Infrastructures from Earth to Orbit

GNSS, as per the definition of the European Space Agency (ESA), is "*any satellite constellation that provides positioning, navigation, and timing services".*[9] GNSS consists of constellations of satellites orbiting Earth at a precise altitude. The satellites transmit radio signals to users on the ground. Ground receivers measure the time delay of these signals to calculate their distance from one satellite. By comparing their distances to multiple satellites (at least 3 different satellites are needed for exact positioning), ground users can determine their precise location. Beyond positioning, the receiver can also calculate the current local time with a very high precision, as GNSS satellites are equipped with an atomic clock. The time information is embedded in the signals broadcasted by the satellite. The usage of GNSS is often referred to as Positioning, Navigation and Timing (PNT).[10]

From an infrastructure standpoint, GNSS requires the existence of a constellation of satellites, called the "space segment", but also transnational networks of ground base stations, often referred to as the "control segment", that can track the transmission, maintain and position the satellites, but also send commands to reposition the constellation when needed.[11] GNSS performance criteria include accuracy (how close the measured position is to the true value), integrity (ability of the system to warn users that it is unreliable, due to disruptions), continuity (capacity of the system to operate with no interruption) and availabilities (the time a signal upholds the accuracy, integrity and continuity criteria).[12]

b. Four main Global Navigation Satellite Systems

The abbreviation GPS is commonly used instead of GNSS, but it only denotes one of the several existing global GNSS systems. Indeed, there are four main GNSS: the *Global Positioning System (GPS), GLONASS, Galileo, and BeiDou*.[13]

GPS was designed by the United States for military purposes, and it was established in 1973. Following the crash of a Korean aircraft shot down after accidentally entering Soviet airspace, the Reagan Administration made GPS's Positioning, Navigation and Timing (PNT) freely available for civil and commercial use in 1983.[14] Before too long, other countries followed suit. The USSR launched GLONASS in 1982, which became fully operational in 1995. However, GLONASS has experienced several challenges over the years, including a lack of funding, technical limitations (e.g., lower-performing on-board atomic clocks), a smaller number of satellites in orbit compared to other GNSS constellations, and ground monitoring mostly limited to the Russian territory. China launched BeiDou's first satellite in 2000, reaching its first full global coverage in 2020. BeiDou is today the world's largest GNSS constellation with 45 satellites and is one of the most accessible and accurate systems. It has dual usage functions for civilian and military purposes, including two-way messaging, that can be used both to receive and send messages.[15] Lastly came Galileo, launched by the EU, whose initial satellites were first installed in 2011. As of the time of writing, it includes 27 operational satellites. Galileo has a strong civilian and commercial backbone with civilian signal authentication.[16]

GNSS Group	**GPS**	**GLONASS**	**Beidou**	**Galileo**
Country	US	Russia	China	Europe
Launch date	1978	1982	1994	2011
# of satellites	31	24	45	27

Figure 1: Comparative Table of Global Navigation Satellite Systems (GNSS). The number of satellites displayed in the table is the number of usable, operational satellites for each constellation. This number can vary over time, depending on commissioning and decommissioning. The table therefore includes current operational satellites at the time of writing.[17]

c. Ubiquitous civilian and military applications

Most GNSS were originally developed to serve military use cases: they power navigation for troops and equipment (including drones), remote targeting and communications. Today, the military still relies on GNSS as critical infrastructures, which makes GNSS vital strategic assets, but also prime targets for disruptions in conflict scenarios.[18]

However, the essential nature of GNSS expands to civilian activities as well. GNSS underpin navigation from personal mobility to aviation (air traffic control systems), which relies heavily on precise positioning data. Additional civilian applications include, among others: agriculture (precision farming),[19] power grids (which rely on timing data provided by GNSS),[20] autonomous devices (such as drones and autonomous vehicles), and IoT (Internet of Things) devices to deliver services.[21] As such, a significant portion of the economy depends on GNSS: in the case of the UK, it was estimated that it supports £320B of GDP (15.3%),[22] and in the case of the US, experts from the US National Institute and Technology estimated that *"GPS has generated roughly $1.4 trillion in economic benefits*

(2017) since it was made available for civilian and commercial use in the 1980s", highlighting that "*the loss of GPS service would average a $1 billion per-day impact to the nation.*"[23]

SECTION 2 - WHY ARE GNSS AT RISK?

There are three main factors heightening the risks for GNSS:

1. The intensification of threats such as spoofing, jamming and anti-satellite weapons (ASAT), which can easily disrupt or manipulate satellites or their signals;
2. The limited integration of anti-interference capabilities into the resilience measures, leaving systems exposed to these threats;
3. Increased geopolitical tensions (such as the Russia-Ukraine war), leading to more cyber radio frequency and physical attacks targeting GNSS.

a. Three Types of Cybersecurity Threats to GNSS Space-Based Systems

Three common threats—jamming, spoofing and anti-satellite weapons—make up a large amount of the cyber attacks today (jamming and spoofing) and future risks (anti-satellite weapons) to GNSS. The first two constitute cyber-related attacks targeting the signal, while the latter is a physical attack directly targeting the satellite.

One of the most common and challenging cyber threats to GNSS is **jamming**. GNSS jammers use the same frequency (or very close frequencies) as GNSS devices to annihilate the signal sent by the GNSS to the receiver.[24] Criminals typically use jamming to prevent electronic surveillance and conceal drug trafficking activities,[25] cargo thefts (to block the tracking signals),[26] and airplane interference.[27] In the context of warfare, jamming is meant to disrupt airforces, drones, and guided weapons used by belligerents.[28] In March 2024, Russia was suspected of a 63-hour-long jamming attack that affected 1600 aircrafts in Europe.[29] The reported geographic scope of this disruption was significant: it impacted airplanes navigating in the Polish airspace but also over Germany, Denmark, Sweden, Latvia and Lithuania. This interference likely confused pilots about their actual geographical location. However, no severe damage was reported in relation to the incidents.[30]

Another common risk is **spoofing**, a practice where a malicious actor transmits a seemingly legitimate signal to a receiver antenna, while, in reality, the data is intentionally incorrect.[31] In the absence of robust cybersecurity measures, users are particularly vulnerable to being misled about their position, velocity, or time. This can result in serious consequences: aircrafts or ships may deviate from safe routes, autonomous vehicles could veer off course, and financial systems relying on precise timing could experience synchronization errors. Spoofing has increased, particularly, as the cost of those attacks has fallen - devices costing as low as 300 US dollars - and this technology is now used by both state and non-state actors.[32] One example of spoofing occurred in the Middle East, where Israel used spoofing to mislead satellites about its citizens' location. According to Israel, this measure was

intended to disrupt drone and missile attacks. However, the spoofing attacks have also had civilian consequences such as food orders arriving at inaccurate locations, Uber drivers making mistakes about clients' actual location, and dating apps showing users in neighbouring countries instead of Israeli user profiles.[33] That said, spoofing comes with limitations: to be efficient, spoofers must overcome authentication barriers and tamper cryptographic mechanisms.[34]

Additionally, **Anti-Satellite weapons** (ASAT) pose a physical threat to satellites in outer space, for instance by using missiles to collide with the targeted satellites, referred to as kinetic energy ASAT or KE-ASATs. As of 2025, there has been no clear case of offensive ASAT usage yet, but several testing facilities make it a clear possibility.[35] In January 2007, China successfully tested its ASAT capability, destroying one of its own satellites, with a ballistic missile at an altitude of more than 530 miles (800 kilometers).[36] In March 2019, India followed suit with an operation code named Mission Shakti, that destroyed one of its own low-orbit satellites, located 300 kilometers above the surface of the Earth.[37] More recently, in February 2024, the White House confirmed it had intelligence indicating Russia was working on ASAT weapons, including nuclear ASAT weapons.[38] While the two aforementioned attacks-jamming and spoofing are becoming increasingly accessible to non-State actors, ASAT remains a high-cost technology limited mainly to State actors.

b. Geopolitical tensions heighten threat levels

Risks of attacks on GNSS increase with geopolitical tensions. In the case of the Russian-Ukrainian war, there have been several examples of interference.[39] Notably, jamming incidents have multiplied in the Baltic region, as highlighted by the Estonian Foreign Affairs Minister's declaration in the spring of 2024, after a number of attacks affecting Estonia: "*We know that Russia has been jamming GPS signals since they started their aggression in Ukraine. Over the last year and a half, this issue has become very serious in our region. It is not only an Estonian issue, but also a Latvian, Lithuanian, Finnish, Norwegian, as well as southern Swedish and Polish issue.*"[40] This prompted an intense dialogue between affected countries, and most recently 13 European transport ministers signed a joint letter to the EU urging further action to respond.[41] This surge in jamming coincides with the use of drones and guided weapons by belligerents, which rely on GNSS. In *Satellites in the Russia-Ukraine War*, author Ron Gurantz mentions that "*In the first two months of 2024, the European air traffic control organization Eurocontrol received almost 1,000 reports of GPS jamming or spoofing from pilots. Some incidents have resulted in flights being diverted or receiving inaccurate warnings about dangerous terrain. Russia probably targeted some of the jamming intentionally at Ukrainian drones flying over the Black Sea, but Russia also has a history of incidental GPS jamming just over its borders during military exercises.*"[42]

There have also been growing concerns about China's BeiDou system, most notably on BeiDou's unique capacity to both send and receive messages, allowing system operators to potentially determine the location of users, raising privacy and surveillance concerns. In the

fishing industry more than 50.000 Chinese fishing boats use two-way messaging to send emergency signals, but with the catch that it can be used to monitor the location of users without their consent. More so, in theory, it could enable the transmission of malware onto a device. However, for now, the messages can only carry small amounts of data, thus limiting the hacking or spying capacity of the system.[43]

As a response to rising tensions, strategic collaborations between GNSS powers emerge to strengthen systems. Russia and China have collaborated on several occasions to improve the interoperability of their systems, including shared GNSS chips and satellite monitoring.[44] In the case of transatlantic collaborations, the US was initially skeptical towards the rise of Europe as another GNSS provider, but this stance later changed, prompting more collaboration between the two systems.[45] This includes compatibility from radio frequency, noninterference and national security perspectives.[46] These growing collaborations enable countries to strengthen systems by learning and leveraging other countries' capabilities.

However, fragmentation persists, which impacts developing countries' access to GNSS. For a long time, the GPS was the dominant system in the Global South - being the first global GNSS available for public use. However, that is no longer the case, with BeiDou challenging the US dominance.[47] In the case of Africa, China has sought to expand its influence, most notably through the Belt and Road Initiative (BRI). This massive Chinese-led investment and development programme involving around 150 countries across Asia, Europe, Oceania, South America, and Africa, has led to many strategic partnerships and increased the number of infrastructures funded, designed, built, and/or operated by China.[48] More specifically to spatial activities, China has announced several cooperation initiatives with African partners, such as the China-Africa BeiDou System Cooperation Forum,[49] funded satellites projects and ground infrastructures with several partners.[50] and accelerated professional exchanges and training between Chinese and African experts. The usage of BeiDou has provided opportunities to improve land mapping, urban construction or railway management.[51] This contrasts with the declining US GNSS and space engagements in the region, further criticized for the lack of a clear roadmap to coordinate cooperation between national agencies.[52]

SECTION 3 - GLOBAL EFFORTS TO PROTECT GNSS

a. Limited Anti-Interference capabilities available make GNSS vulnerable

Despite the growing awareness of the GNSS vulnerabilities highlighted above, current systems still face significant challenges in countering ongoing threats. Mitigation efforts have been initiated; however the effectiveness of these measures varies, and comprehensive resilience is therefore needed. Currently explored solutions include, but are not limited to:

- **Controlled reception pattern antennas** (**CRPA**): These antennas can detect and neutralize interferences, adapting against suspicious or unauthorized sources.

Designs of CRPA vary, typically employing multiple antennas, whose reception pattern can be adjusted by their receiver, and signal processing algorithms that can detect interferences.[53] CRPA are highly useful for military and defense applications, so that critical functions remain resilient during high-stake operations (for example military missions). However, CRPA are increasingly used in civilian domains, including aviation, maritime navigation and autonomous systems. For example, the US has broadened access to CRPA, since their removal from the International Traffic in Arms Regulation list in September 2025, enabling the sale of CRPA outside the US as dual-use commercial items.[54],[55] Nonetheless, CRPA remain energy-consuming, can be expensive, and relatively big, which can be an obstacle for weight-constrained or volume-constrained devices.[56]

- **Embedded GNSS Inertial (EGI) Navigators**: by coupling GNSS receivers with traditional inertial measurement units (such as gyroscopes and accelerometers), EGIs can provide continuous position, velocity, and timing capabilities during a period of time even when GNSS signals are unavailable e.g. due to jamming attacks[57]. However, EGI development is complex and involves extensive testing.[58]

- **Cryptography**: cryptographic algorithms may also be used to authenticate the signal. The navigation signal is encoded with an unforgeable signature or watermark and later verified to ensure that it genuinely comes from a trusted satellite.[59] Using such cryptographic techniques can require updates to GNSS, like with the recent data authentication function for the Galileo Open Service.[60] These techniques often fall into two categories: Navigation Message Authentication (NMA), and Spreading Code Authentication (SCA). In the case of NMA (which is implemented in the updated Galileo system), the receiver authenticates signals using digital signatures. While with SCA, watermarks are applied, and later verified by the receiver. SCA is usually reserved for critical use cases, justifying its higher cost.[61] Even though cryptography is a very useful method, research has shown that under certain conditions, particularly involving synchronized transmission/reception timing, an attacker may still be able to bypass cryptographic measures and disrupt GNSS signals.[62]

b. Quantum Navigation as a technological alternative to GNSS

Beyond the anti-jamming and spoofing technologies previously mentioned, the international community is exploring technological innovations to mitigate risks and safeguard its GNSS.

The major alternative currently explored is **Quantum Navigation**, which relies on the laws of quantum physics. Quantum navigation uses sensors that are able to detect the movement of a single atom in cryogenic conditions and can thus provide very accurate readings of speed and direction instead of relying on signals from satellites in space. This takes place inside the “point of use” (the aircraft, submarine, underground metro or wherever it is used), with no incoming signal for an attacker to intercept, jam or spoof.[63]

Private actors are spearheading current progress in quantum navigation with support from governments. In the US, Boeing successfully completed a four-hour flight test guided by quantum navigation technology.[64] Together with American quantum sensor specialist AOSense (funded by DARPA), Boeing used a quantum inertial measurement unit, showcasing the potential of quantum sensors enablement of providing navigation without GPS capabilities. In the UK, a consortium featuring private actors backed by government actors (UKRI, the national funding agency for science and research in the UK) also made headway towards quantum navigation tools that cannot be spoofed or jammed.[65]

However, Quantum Navigation is more expensive to deploy and not fully mature yet. Mainstream adoption is still years in the future, and Quantum Navigation will likely be used as a backup for GNSS for sensitive operations, or to support navigation where GNSS is not available, such as underwater.

c. Public and private efforts to achieve resilience

While national security strategies increasingly recognize the importance of space activities, there is simultaneously an uptake in private sector engagements in the field. Between 2015 and 2020, €23B were invested worldwide in space startups, and €9,1B in 2021 alone. This amount is unequally distributed, with US-based companies capturing 67% of those investments in 2020.[66] Examples of funding supporting GNSS and space include:

- The EU and its Agency for the Space Program signed a Memorandum of Understanding to promote R&D, alongside mobilizing funds such as CASSINI, a European initiative to support entrepreneurs, start-ups, and SMEs in the European Space sector.[67] Limited funding has been geared directly toward GNSS-relevant solutions, through dedicated “challenge calls” benefiting projects such as Germany-based Armadello, a navigation control system using Galileo Open Service Navigation Message Authentication (OSNMA) to protect rockets from GNSS spoofing.[68]

- The Defence Innovation Accelerator for the North Atlantic (DIANA) program was launched by the North Atlantic Treaty Organization (NATO) to enhance support to technologies mitigating security and defense challenges.[69] Last year’s DIANA challenge call specifically highlighted GNSS in relation to data, security and quantum usage.[70] The US-based company SandboxAQ, was selected among the 2025 cohort to develop AQNav, a navigation system using quantum sensors and relying on the earth’s magnetic field as a GNSS alternative resilient to jamming and spoofing.[71]

- The private sector provides solutions enhancing current GNSS capabilities to protect against interference. Many companies offer anti-GNSS spamming or spoofing antennas, or even combine GNSS with their own proprietary constellations of satellites, such as American company Spire which signed a government contract with Canada for CAD1,41M (roughly €1M) for real-time ship tracking data.[72]

- In the EU, the Commission attributed roughly €44M to a consortium of 18 companies from France, Germany, Italy, Belgium, and Spain to work on the Galileo EU Defence (GEODE) program. They are tasked to prototype and test several solutions enhancing the use of Galileo in military applications, including encryption technologies and anti-jamming antennas.[73]

d. Leveraging legal and regulatory avenues

Beyond technological breakthroughs and public-private initiatives, regulatory measures have also been adopted to combat GNSS attacks. Yet, limited progress has been made for two reasons.

The ambiguity of space law, and the difficulty of establishing jurisdiction and liability (politically, judicially, and financially) in the case of jamming or spoofing attacks make enforcement of national and international norms arduous: General principles referenced in the Outer Space Treaty from United Nations Office for Outer Space Affairs outlines the criticality of co-operation and mutual assistance "*with due regard to the corresponding interests of all other States Parties to the Treaty*"[74] but they are intrinsically difficult to enforce. However, ITU's Radicommunication Bureau counts amongst its missions to assist in resolving causes of harmful inferences, including for space activities (Radio Regulations, 13.2)[75] and thus has some degree of power to support a safer GNSS cyber space.[76] Specifically, ITU's RR No.15.28 is a good example that emphasizes the "*absolute international protection*" and the imperative responsibility of Member-States in the "*elimination of harmful interference*" to distress and safety flight frequencies.[77]

The multiplicity of actors and committees involved in the discussions: For historical reasons, the US has been setting most of the international norms for GNSS.[78] Yet, due to today's diversification of GNSS solutions, the broader international community has to find common solutions to the evolving threat landscape. However, there are multilateral organisations involved in the process and include but are not limited to: the United Nations Office for Outer Space Affairs (UNOOSA), the International Committee on Global Navigation systems (ICG)–a key forum for exchanges and setting best practices between different GNSS providers,[79] the Committee on the Peaceful Uses of Outer Space (COPUOS),[80] which are both hosted by UNOOSA, the International Civil Aviation Organization (ICAO) which works with member states to align standards within GNSS in relation to aviation.[81] The vast amount of forums and stakeholders creates fragmentation that, coupled with geopolitical tensions, hinders consensus on common solutions to the GNSS cybersecurity threats.[82] However, organizations still achieve progress, such as the ITU resolution 676 adopted in 2023 that supports the prevention and mitigation of harmful interference to the radionavigation satellite service.[83]

POLICY RECOMMENDATIONS

1. Expand collaborative testing and simulation to continuously uncover GNSS vulnerabilities.

Proactive testing is essential to identify GNSS vulnerabilities and solutions to enhance resilience. Testing is already occurring in particular at the national level.[84] However, international organizations can to a larger extend bring together public and private stakeholders to pool resources and expand efforts including more simulations of cyberattacks, field tests verification and annual cyber drills.

2. Increase funding to support GNSS resilience.

Greater investment in innovative GNSS cyber resilience solutions is critical. Additional and more targeted funding from both public and private sources, including public-private partnerships, is required to support the development of innovative cyber resilience solutions, such as quantum navigation, that represents a paradigm shift in the sector.

3. Re-focus and re-target existing space initiatives.

Innovation grants need to be expanded to include dedicated GNSS-focused funding tracks and government operators should also establish multi-year procurement commitments for GNSS security. Part of the €800B Rearm Europe plan could be dedicated to GNSS safety and resilience, and a dedicated co-investment vehicle could be created.

4. Encourage cross-pollination between different GNSS systems to foster security.

Identify two or three new high-impact interoperability pilots use cases to build the foundations for shared resilience strategies. Hold more annual workshops within international organizations to be better equipped to tackle cyber risks.[85] These efforts must prioritize mutual benefits, while safeguarding countries' technological sovereignty in GNSS.

5. Harmonize regulation and technical standards internationally.

As spoofing and jamming are not bound by borders, they are intrinsically international issues. Enhancing resilience and fostering cross-pollination (see above) thus requires better enforcement of current regulations and harmonization of standards for GNSS security across national borders, including centralising power to fewer international organisations such as the ICAO.

6. Stronger usage of international control.

A final suggestion is to improve control of spoofing and jamming devices to limit the accessibility of misuse. This could be combined with a moratorium on ASAT weapons by all UN member states, which would minimize the risk of the usage of destructive ASAT.

[1] *EASA updates SIB on GNSS Outage and Alterations*, EASA Safety Information Bulletin, 2023.

[2] See Finnair's official statement "Finnair Suspends Flights to Tartu for a Month." *Finnair Media Centre*, 2024, and media coverage such as Tomasso Lecca, Estonia blames Russia for GPS interference that forces Finnair to suspend flights, *Politico*, 2024.

[3] Maia Davies & Will Vernon, "EU chief Von der Leyen's plane hit by suspected Russian GPS jamming", *BBC*, 2025.

[4] Ranging from increased fuel usage to, indirectly, disturbances to the tracking of tagged animals. For more on this, see UK Space Agency, The economic impact on the UK of a disruption to GNSS - Executive summary, UK GOV, 2023, and Jiguet, Frédéric et al., GNSS spoofing in conflict zones disrupts wildlife tracking and hampers research and conservation efforts, *Nature*, 2025,

[5] See GNSS Market Report, issue 4, European Global Navigation Satellite Systems Agency, 2025, and Burgess, Matt, The Dangerous Rise of GPS Attacks, *WIRED*, 30 Apr. 2024.

[6] See the previously mentioned UK Space Agency report, McCord, David. "The 50th Anniversary of GPS: New Avenues for Cooperating with Europe's Galileo" *Belfer Center*, 9 Apr. 2024, p. 4, and Kathleen McTigue, *Economic Benefits of the Global Positioning System to the U.S. Private Sector Study*, NIST, 2019.

[7] See Hess, Amandine, "What can Europe do better to defend against GPS interference from Russia", *Euro News*, 2025, Gorman, Sean. "America is losing its GPS dominance to China's BeiDou satnav." *SpaceNews,* 2024, or Jones, Andrew. "China to launch next-generation Beidou satellites in 2027". *SpaceNews,* 2024.

[8] *"States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner. The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden."*

[9] "What Is GNSS." *EU Agency for the Space Programme*, 15 Jan. 2025.

[10] See: "GNSS". *NASA Earth Science Data, 2025.* "Satellite Navigation - GPS- How it works". *FAA*, 2025.

[11] "What is a GNSS", University of Southern Queensland, 2025. "Control Segment." *GPS.gov*, U.S. National Coordination Office for Space-Based Positioning, Navigation, and Timing, 2025.

[12] "What Is GNSS." *EU Agency for the Space Programme*, 15 Jan. 2025.

[13] Beyond these four global systems, India (NavIC) and Japan (QZSS) have also deployed regional GNSS.

[14] See: McCord, David. "The 50th Anniversary of GPS: New Avenues for Cooperating with Europe's Galileo." *Belfer Center*, 9 Apr. 2024, p. 4. Speakes, Larry. "Statement by Deputy Press Secretary on the Soviet Attack on a Korean Civilian Airliner." *Reagan Library*, 16 Sept. 1983.

[15] See: "China's BeiDou challenges US GPS dominance", *GPS world*, 2023.McCord, David. "The 50th Anniversary of GPS: New Avenues for Cooperating with Europe's Galileo." *Belfer Center*, 2024; Sewall, Sarah, Tyler Vandenberg and Kaj Malden, 2023; Xie Jun: BeiDou Navigation Satellite System in 2024, *GPS world,* 2024.

[16] ESA, "Galileo: Europe launches its first satellites for smart navigation system", McCord, David. "The 50th Anniversary of GPS: New Avenues for Cooperating with Europe's Galileo." *Belfer Center*, 2024. "Galileo Statelites", EUSPA, 2025.

[17] These figures come from: for GPS "Satellite Navigation - Global Positioning System", Federal Aviation Administration, 2025, for GLONASS NASA Earth Science Data: "GNSS", *NASA*, for BeiDou 2025, Xie Jun "BeiDou Navigation Satellite System in 2024", *GPS world,* 2024, and for Galileo "Galileo Statelites", EUSPA, 2025.

[18] Gallardo López, Francisco et al. "Protecting GNSS Critical Infrastructure in an Unstable world", *Universidad Politécnica de Madrid,* 2024.

[19] "GNSS at the Centre of a Revolution in Agriculture." *EU Agency for the Space Programme*, 2017.

[20] "Global Navigation Satellite Systems (GNSS)." *UNOOSA*, United Nations.

[21] See: Aurello, Patrik et al. "GNSS-Based Navigation Systems of Autonomous Drone for Delivering Items." *Journal of Big Data*, vol. 6, no. 53, 14 June 2019 and "Geolocation Technology on the Cusp of a Revolution." *EU Agency for the Space Programme*, 13 June 2017.

[22] UK Space Agency. *The Size and Health of the UK Space Industry 2022*. UK Space Agency, 28 Mar. 2023.

[23] O'Connor, Alan C., et al. *Economic Benefits of the Global Positioning System (GPS) to the U.S. Private Sector Study*. RTI International, 2019.

[24]Radoš, Katarina "Recent Advances on Jamming and Spoofing Detection in GNSS". *Advanced Localization and Motion Tracking with Dense Wireless Networks, 2024.*

[25] Brunker, Mike. "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War." *NBC News*, 8 Aug. 2016.

[26] "The Growing Problem of Signal Jammers in Mexico." *Overhaul*, 2024.

[27] Gorman, Sean. "The Urgent Need for a National GPS Jamming Detection System." *SpaceNews*, 27 Nov. 2024.

[28] Kirichenko, David. "A New and More Deadly Drone on Russia's Battlefields." *CEPA*, 3 Mar. 2025.

[29] Hsu, Jeremy. "Unprecedented GPS jamming attack affects 1600 aircraft over Europe." *New Scientist,* 2024.

[30] Amalaraj, Perkin. "More Than 1,600 Planes Hit by Mysterious GPS Jamming Over Europe; Russia Feared Responsible." *Daily Mail*, 26 Mar. 2024.

[31] Manulis, M., et al. "Cyber Security in New Space: Analysis of Threats, Key Enabling Technologies and Challenges." *International Journal of Information Security*, vol. 20, no. 3, 2021, pp. 287–311.

[32] See: Peng, Jiang et al. "DeepPOSE: Detecting GPS Spoofing Attack Via Deep Recurrent Neural Network p. 792" *Digital Communications and Networks, 2021*. Khalil, Jesse. "GNSS Spoofing Threatens Airline Safety, Alarming Pilots and Aviation Officials." *GPS World*, 24 Sept. 2024. Sánchez González, Èric. *GNSS Signal Spoofing Detection*. Directed by Luis Esteve Elfau, Universitat Politècnica de Catalunya, 28 Oct. 2022. The Significance of Accurate Timekeeping and Synchronization in Trading Systems. *Safran, 2025.*

[33] "Making love not war in the Middle East". *The Economist*. 2024.

[34] See: Caparra, Gianluca, et al. "Feasibility and Limitations of Self-Spoofing Attacks on GNSS Signals with Message Authentication." *Proceedings of the 35th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2022)*, 2022.

[35] Blatt, Talia. "Anti-Satellite Weapons and the Emerging Space Arms Race." *Harvard,* 2020.

[36] Zissis, Carin: "China's Anti-Satellite Test", Council on Foreign Relations, 2007.

[37] "India's Modi Announces Successful Anti-Satellite Missile Test." *CNN*, 27 Mar. 2019.

[38] Gorman, Sean. "Russian Nuclear Anti-Satellite Weapons Would Require a Firm U.S. Response, Not Hysteria." *Atlantic Council*, 22 Jan. 2024.

[39] Waterman, Shaun. "Russian Jamming Wreaks Havoc on GPS." *Air & Space Forces Magazine*, 2024.

[40] "Foreign Minister: Plenty of Evidence Russia Is Jamming GPS Systems." *ERR News*, 24 May 2024.

[41] "13 EU member states demand action on GNSS interference". *GPSworld, 2025.*

[42] Gurantz, Ron. *Satellites in the Russia-Ukraine War*. USAWC Press, Carlisle Barracks, PA, page 25, 21 Aug. 2024.

[43] Sewall, Sarah, Tyler Vandenberg, and Kaj Malden. "China's BeiDou: New Dimensions of Great Power Competition." *Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2023.

[44] Ibid.

[45] Beidleman, Lt. Col. Scott W. *GPS versus Galileo: Balancing for Position in Space*. College of Aerospace Doctrine, Research and Education (CADRE) Paper (No. 23), School of Advanced Air and Space Studies, May 1 2006. *National Security Archive*, George Washington University.

[46] *GPS Galileo Factsheet*. GPS.gov.

[47] See: European Space Agency. "Receiver Operations." *Navipedia*, edited by GSSC and GMV, GNSS Science Support Centre, 2021. Sewall, Sarah, Tyler Vandenberg og Kaj Malden. "China's BeiDou New Dimensions of Great Power Competition." *Belfer Center - Harvard Kennedy School* 2023.

[48] Chatzky, Andrew, and James McBride. "China's Massive Belt and Road Initiative." *Council on Foreign Relations*, 28 Jan. 2020.

[49] "Attend the first China-Africa BDS Cooperation Forum", Space in Africa, 2021.

[50] Nadin, R. and Kiryakova, E. (2024) China's growing space and communications presence in Africa. ODI Global Briefing Note. London: ODI Global.

[51] Iderawumi, Mustapha. "China and Africa to Strengthen Collaboration on BeiDou Satellite System." *Space in Africa*, 2021.

[52] Roulette, Joey, Eduardo Baptista, Sarah El Safty, and Joe Brock. "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid." *Reuters*, 11 Feb. 2025.

[53] Verdeguer Moreno, Ricardo. "CRPA Antennas Explained: Choosing and Testing the Best Anti-Jam Solutions for GPS/GNSS Resilience." *Spirent Communications*, 29 Nov. 2024.

[54] "Controlled Reception Pattern Antennas (CRPAs): Ensuring Resilient GPS and GNSS Performance". *MTI Wireless Edge, 2025.*

[55] Matteo Luccio: "First fix: Freeing CRPAs*". GPS World, 2025.*

[56] Verdeguer Moreno, Ricardo. "CRPA Antennas Explained: Choosing and Testing the Best Anti-Jam Solutions for GPS/GNSS Resilience." *Spirent Communications*, 29 Nov. 2024.

[57] *Honeywell Unveils Resilient EGI for GPS-Denied Environments*. *GPS World*. 2 Oct. 2024.

[58] "A True Reference: Theory Meets Reality in Synchronized Simulation Environments." *Inside GNSS*, 27 Feb. 2022.

[59] Muzi Yuan, Xiaomei Tang, Gang Ou. "Authenticating GNSS civilian signals: a survey". Satellite navigation, 2023.

[60] "Galileo Open Service Navigation Message Authentication (OSNMA)." EUSPA, 2025.

[61] Muzi Yuan, Xiaomei Tang, Gang Ou. "Authenticating GNSS civilian signals: a survey". Satellite navigation, 2023.

[62] Motallebighomi, Maryam, et al. "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals." *arXiv*, 2022.

[63] "What is quantum navigation – and could it replace GPS?" *World Economic Forum,* 2024.

[64] Swayne, Matt. "UK reports Successful Test of Un-jammable Quantum Navigation system", *Quantum Insider*, 2025.

[65]Swayne, Matt. "Boeing's Quantum-Based Navigation System Takes Flight in Historic Test." *The Quantum Insider*. 9 Aug. 2024.

[66] European Investment Bank (EIB) and European Union Agency for the Space Programme (EUSPA). "GNSS Investment Report 2021." *EIB*, 16 Mar. 2022.

[67] See: European Investment Bank (EIB) and European Union Agency for the Space Programme (EUSPA). "EIB and EUSPA Publish First Global Navigation Satellite Systems Investment Report." *EIB*, 16 Mar. 2022. "Cassini ". European Commission, 2025.

[68] See "Cassini Challenges" and "Winners". *EUSPA*, 2024.

[69] NATO Defence Innovation Accelerator for the North Atlantic (DIANA). *DIANA*, NATO, 2025.

[70] NATO DIANA. *2024 DIANA Challenge Programme Call for Proposals*, NATO, 2024.

[71] Khalil, Jesse. "NATO Selects SandboxAQ for 2025 Defense Innovation Accelerator Program." *GPS World*, 11 Feb. 2025. "SandboxAQ Announces AQNav: Commercial Real-Time Navigation System Powered by AI and Quantum to Address GPS Jamming." *Inside GNSS*, 26 June 2024.

[72] "Spire Global Awarded CA $1.41 Million Contract from Government of Canada for Ship Tracking Data" *Business Wire,* 2024. Vividha Chopra: "GNSS spoofing: A growing global threat" Spire, 2025.

[73] EU Commission, Factsheet on GEODE, 2020

[74] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies", US Department of State, 2025.

[75] Ciccorossi, Jorge. "Space Sustainability, Monitoring and Interference Reporting (SIRRS)." *ITU-R Seminar on Space Sustainability*, Dec. 2024, Geneva, Switzerland.

[76] "Radio Interference" ITU, 2025.

[77] Ciccorossi, Jorge. "Harmful Interference to Satellite Systems and the Current Challenge to GNSS." *Eurocontrol Stakeholder Forum on GNSS*, 4 Mar. 2021.

[78] Kahveci, Muzaffer, and Nazh Can. "Legal Issues in GNSS Applications: Past, Today and Tomorrow." *Proceedings of the 6th International Conference on Recent Advances in Space Technologies (RAST)*, 2013.

[79] Porter, Mackenzie, and Tony Porter. "Global Navigation Satellite Systems Infrastructure, From the Ground Up." *SSRN*, 2025.

[80] Note: COPUOS has a broader mandate within defense and security, with some focus on defense and security of GNSS. United Nations Office for Outer Space Affairs. "Committee on the Peaceful Uses of Outer Space." *UNOOSA*, United Nations.

[81] International Civil Aviation Organization. "Protect Satellite Navigation from Interference, UN Agencies Urge." *ICAO*, 25 Mar. 2025.

[82] During a session involving national representatives from key GNSS providers; the EU representative made a statement denouncing Russia's invasion of Ukraine. In response, the Russian representative refused to provide system updates, challenging collaboration and interoperability between systems; Porter, Mackenzie, and Tony Porter. "Global Navigation Satellite Systems Infrastructure, From the Ground Up." *SSRN*, 2025.

[83] 2023 World Radiocommunication Conference resolution n°676 "Prevention and mitigation of harmful interference to the radionavigation satellite service in the frequency bands 1 164-1 215 MHz and 1 559-1 610 MHz"

[84] Such as JammerTest in Norway, programs organized by the Department of Homeland Security in the US.

[85] Rohland, Barbeschi. "Securing space tech: Why we need to address cyber risks in orbit". WEF, 2025.