Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, 233-257
doi: 10.28956/gbd.1685901

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, Thematic Issue on Policing Practices and Security Technologies 231-257
doi: 10.28956/gbd.1685901

Makale Türü ve Başlığı / Article Type and Title

Araştırma / Research Article

Strategic Role Of Gnss In Security Technologies And Alternative Approaches To National Navigation Systems

Güvenlik Teknolojilerinde Gnss'nin Stratejik Rolü ve Ulusal Navigasyon Sistemlerine Yönelik Alternatif Yaklaşimlar

Yazar(lar) / Writer(s)

Vedat YILMAZ, J.Mu.Yb.Dr. Jandarma ve Sahil Güvenlik Akademisi, Adli Bilimler Enstitüsü, Kriminalistik Anabilim Dalı, vedat.yilmaz@jsga.edu.tr, ORCID: 0000-0002-3112-9371

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 28.04.2025
Makale Kabul Tarihi / Accepted : 09.10.2025

Atıf Bilgisi / Citation:

Yılmaz V., (2025). Strategic Role Of Gnss In Security Technologies And Alternative Approaches To National Navigation Systems, *Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, ss 231-257. doi: 10.28956/gbd.1685901*

STRATEGIC ROLE OF GNSS IN SECURITY TECHNOLOGIES AND ALTERNATIVE APPROACHES TO NATIONAL NAVIGATION SYSTEMS

Abstract

Global Navigation Satellite Systems (GNSS) have become a critical infrastructure element in both civilian and military areas of the modern world. Thanks to the high-accuracy location, time and direction data they provide in the transportation, energy, finance and security sectors, GNSS systems have a wide range of use from daily life to strategic operations. However, this widespread use has brought with it serious security threats such as being vulnerable to jammer and spoofing attacks due to weak signal structure, geopolitical dependency and systemic collapse risks. These threats make GNSSs vulnerable, especially in electronic warfare and cyber attack environments. This article analyzes the effects of strategic dependency on GNSS on national security and emphasizes the importance of developing national terrestrial navigation systems as an alternative solution. Terrestrial systems such as eLoran, DGNSS and RTK stand out as complementary and backup to GNSS thanks to their strong signal structures, local controllability and jammer/spoofer resistance. In Türkiye, the establishment of a national terrestrial navigation infrastructure has become a necessity that must be carried out in parallel with defense industry strategies and national technology initiatives. In this regard, multi-layered navigation systems (GNSS and terrestrial systems) are suggested as a critical strategy for the sustainability of national security.

Keywords: *Security Technologies, GNSS, Positioning, Threat, Electronic Warfare*

GÜVENLİK TEKNOLOJİLERİNDE GNSS'NİN STRATEJİK ROLÜ VE ULUSAL NAVİGASYON SİSTEMLERİNE YÖNELİK ALTERNATİF YAKLAŞIMLAR

Öz

Küresel Navigasyon Uydu Sistemleri (GNSS), modern dünyanın hem sivil hem de askerî alanlarında kritik bir altyapı unsuru hâline gelmiştir. Ulaşım, enerji, finans ve güvenlik sektörlerinde sağladığı yüksek doğruluklu konum, zaman ve yön verileri sayesinde GNSS sistemleri, günlük yaşamdan stratejik operasyonlara kadar geniş bir kullanım alanına sahiptir. Ancak bu yaygın kullanım beraberinde zayıf sinyal yapısından kaynaklanan jammer ve spoofer saldırılarına açık olma, jeopolitik bağımlılık ve sistemik çökme riskleri gibi ciddi güvenlik tehditlerini getirmiştir. Bu tehditler, özellikle elektronik harp ve siber saldırı ortamlarında GNSS sistemlerini kırılgan hâle getirmektedir. Bu makale, GNSS'ye olan stratejik bağımlılığın ulusal güvenlik üzerindeki etkilerini analiz etmekte ve alternatif çözüm olarak ulusal karasal navigasyon sistemlerinin geliştirilmesinin önemini vurgulamaktadır. eLoran, DGNSS ve RTK gibi karasal sistemler; güçlü sinyal yapıları, yerel kontrol edilebilirlikleri ve jammer/spoofer dayanımları sayesinde GNSS'nin tamamlayıcısı ve yedeği olarak öne çıkmaktadır. Türkiye özelinde millî karasal navigasyon altyapısının kurulması, savunma sanayi stratejileri ve millî teknoloji hamleleriyle paralel yürütülmesi gereken bir zorunluluk hâline gelmiştir. Bu doğrultuda, çok katmanlı navigasyon sistemleri (GNSS ve karasal sistemler) ulusal güvenliğin sürdürülebilirliği açısından kritik bir strateji olarak önerilmektedir.

Anahtar Kelimeler: *Güvenlik Teknolojileri, GNSS, Konumlama, Tehdit, Elektronik Harp*

INTRODUCTION

Navigation technologies have evolved to fulfill humanity's ancient need to find direction and determine location. Advances in this field from ancient times to the present have directly affected not only areas such as maritime and trade, but also strategic areas such as military operations, logistics, air transportation and security technologies. (Selbesoğlu, Barutçu & Çökelez, 2021)

When the historical development of navigation technologies is examined; The first navigation applications were based on natural observations. The sun, stars (especially the Pole Star), the moon and other celestial bodies were utilized as primitive navigation tools. Ancient Egyptian, Phoenician and Chinese civilizations determined their routes by using astronomical observations in navigation. The invention of the magnetic compass in China in the 11th century revolutionized navigation skills and spread to Europe in a short time (Aktuğ, 2015). The increase in maritime activities during the period of geographical discoveries led to the development of precise maps and maritime instruments. Thanks to instruments such as the sextant, astrolabe and chronometer, latitude and longitude determination techniques became widespread (Aktuğ, 2015; Selbesoğlu, Barutçu & Çökelez, 2021). In particular, the acceptance of Greenwich Mean Time as the standard time unit and the use of chronometers made reliable position determination possible on long sea voyages (Sobel, 1995). With technological developments in the early 20th century, the first navigation systems working via radio signals were developed. During World War II, LORAN (Long Range Navigation) and similar radio-based systems were used especially for military purposes. These systems were based on calculating the user's position through triangulation methods using signals broadcast from terrestrial base stations (Son, Rhee & Seo 2017).

GPS (Global Positioning System), developed by the USA in the 1970s, revolutionized navigation technologies. Satellite-based positioning systems became capable of providing global coverage and high-precision location information in all weather conditions and at all hours of the day. In the following years, other major players such as Russia (GLONASS), the European Union (Galileo), and China (BeiDou) have also developed their own global systems. All of these systems are classified together under the umbrella of GNSS (Global Navigation Satellite System). Today, GNSS technologies are used not only in navigation but also in many critical sectors such as time synchronization, security systems, banking, energy infrastructures, and

communications (Dovis, 2015). This wide range of use has also brought about the vulnerabilities of GNSS systems. Threats such as jammers and spoofing pose serious security concerns in terms of civilian and military use of the systems (Dovis, 2015).

These security vulnerabilities and strategic dependency have led many countries to develop alternative or complementary systems to GNSS. Terrestrial navigation systems such as eLoran, DGNSS and Radio Frequency based short-range solutions have gained renewed importance, especially for critical infrastructures and defense applications (Johnson et al., 2017).

Today, GNSS (Global Navigation Satellite System) has become a critical technology in many different areas, from national security to infrastructure management, far beyond being just a navigation tool for individual users. GNSS's global coverage, high accuracy, real-time data production and multi-application potential make it indispensable for both civil and military applications.

GNSS systems are utilized in many areas of civil life today. In this context, the use of GNSS in many areas, which can be detailed in transportation and logistics, finance and telecommunications, disaster management and search and rescue, is presented below.

- Transportation and Logistics: Route optimization, traffic management and cargo tracking in land, air, sea and rail transportation are provided by GNSS. In particular, location verification systems mandated by ICAO (International Civil Aviation Organization) in aviation are based on GNSS (ICAO, 2021).

- Finance and Telecommunications: GNSS provides time synchronization with microsecond precision in banking transactions and 5G infrastructures (Koca & Ceylan, 2018).

- Disaster Management and Search and Rescue: In disasters such as earthquakes and floods, GNSS-supported maps and location services are vital for rapid response and guidance (Koca & Ceylan, 2018).

Although GNSS has indispensable use from individual to institutional civilians today, its real strategic importance manifests itself in military and security applications (Borodacz & Szczepański, 2024). In modern military/armies:

- It is used in smart ammunition and precision guidance systems,
- Coordination and tracking systems of military units,
- Navigation of UAVs (Unmanned Aerial Vehicles) and UCAV (Unmanned Combat Aerial Vehicles),
- Combined operations of land, air and sea vehicles,
- Border security, reconnaissance and surveillance systems (Kaplan & Hegarty, 2017, Borodacz & Szczepański, 2024).

This level of dependency in terms of National Security has caused GNSS systems to become a strategic "infrastructure foundation". For this reason, states are conducting serious studies on the security of these systems against cyber attacks on GNSS signals, electronic warfare threats and geopolitical control problems (Trýb & Hospodka, 2025).

The main purpose of this research is to analyze the increasing role of GNSSs (Global Satellite Navigation Systems) in security technologies and in this context to evaluate the importance of national terrestrial navigation systems by revealing the security vulnerabilities caused by strategic dependency on these systems.

Although GNSS systems are widely used in civil and military areas today; jamming, spoofing, electronic warfare interventions and geopolitical control risks question the reliability of these systems and create serious threats to national security (Borodacz & Szczepański, 2024). Therefore, this study aims;

- To explain the technical structure of GNSS systems and their function in security technologies,
- To analyze threats to GNSS (electronic warfare, cyber attacks, external dependency),
- To reveal the strategic advantages that national terrestrial navigation systems can provide against these threats,
- To evaluate technological, institutional and security-based justifications for the development of domestic terrestrial system infrastructures, specifically for Türkiye.

1. THREATS TO GNSS SYSTEMS AND ELECTRONIC WARFARE RISKS

GNSS systems have become vulnerable to both natural and intentional threats due to their widespread use and strategic importance. Since these systems operate based on low-power radio frequency signals, they can be targeted especially by electronic warfare methods (Trýb & Hospodka, 2025). The security of GNSS systems is critical for both the security of military operations and the sustainability of civilian infrastructures.

1.1. Strategic Dependency and National Risk

Most GNSS systems are connected to infrastructures controlled by certain states. For example, while GPS is completely managed by the US Department of Defense, other GNSS systems are similarly controlled by geopolitical power centers. (GPS: USA, GLONASS: Russia, Galileo: European Union, BeiDou: China). This structure makes countries using GNSS dependent on external sources in terms of data flow and service interruptions; which creates risks such as signal interruption or restriction at critical moments (Grejner-Brzezinska et al., 2016). The increase in threats such as electronic warfare and jammers/spoofers in particular has made it necessary to develop alternative systems.

Along with these security vulnerabilities, studies are being conducted worldwide for both diversification (multi-GNSS) and backup (eLoran, terrestrial systems, inertial navigation systems) of GNSS systems (Son, Rhee & Seo, 2017; Trýb & Hospodka, 2025). The European Union's development of the Galileo system and China's opening of the BeiDou system to global access show that navigation has become not only a technological but also a strategic and political competition area.

1.2. Threat Types to GNSS

Jamming

GNSS signals are very weak when they reach the ground (~-130 dBm). This weakness causes the signals to be easily drowned out by a stronger radio frequency source (Göde et al., 2024). Such attacks are usually carried out with portable jammer devices. In 2018, civil aviation flights in Norway and Finland lost orientation due to GPS jamming during a NATO exercise. It was claimed that Russia's electronic warfare units were behind the incident (Reuters, 2018).

Spoofing

In spoofing attacks, fake GNSS signals are sent to the user, causing the device to calculate an incorrect location. This method can be used to direct military vehicles, ships or UAVs to wrong routes. In 2013, an academic team managed to manipulate the GPS signal of a luxury yacht with a spoofer and change its route without it being noticed (Humphreys et al., 2013).

Meaconing

GNSS signals are recorded and rebroadcast elsewhere, providing the user with delayed or incorrect information. This method produces similar effects to spoofing, but is generally applicable with less sophisticated devices (Steiner, Pleninger & Hospodka, 2024).

Threats to Physical Infrastructure

Physical destruction of satellites, cyberattacks on satellite control centers, or sabotage of ground stations can also threaten GNSS systems.

Cyber Security Threats

Cyber attacks on software that processes GNSS signals or the network infrastructure through which this data is transferred can lead to the collapse of security systems. Critical security systems can be rendered dysfunctional with techniques such as fake data injections and coordinate manipulation.

These vulnerabilities can directly affect the success of military operations. They can make border security violable. They can disrupt public order in smart city security infrastructures. They can reduce the speed and accuracy of law enforcement interventions. Therefore, the protection, backup and support of GNSS systems with domestic solutions have become an integral part of national security policies (Jhanjhi, Gaur & Khan, 2024).

1.3.Electronic Warfare and GNSS Battlefield

In modern military doctrines, electronic warfare has become as critical as physical conflict. Field-programmable gate array (FPGA)-based embedded systems have begun to be used for real-time detection and analysis of RF signals for the detection of UAV/UCAV systems and the ground stations that manage these systems (Duraklar, 2025). Post-detection, interference with GNSS signals aims not only to paralyze enemy units' navigation capabilities but also to disrupt time synchronization, thereby disrupting their communications and

operational integrity. Loss of GNSS in military aircraft can disable targeting and coordination systems. Because civilian infrastructures, banking, energy, and telecommunications systems depend on GNSS time synchronization, the loss of GNSS can cause social chaos (Wu, 2024; Yu et al., 2025).

1.4. Reflection in Civil and Military Areas

Civilian Area: In applications such as port management systems, autonomous vehicles, drones and smart agricultural machines, the loss of GNSS signals can lead to scenarios that can cause material damage as well as loss of life. Military Area: GNSS-based precision guidance munitions and UAV systems are vulnerable to jamming and deception. This situation offers the opportunity to temporarily neutralize the enemy's technological superiority, especially in hybrid warfare scenarios.

1.5. Measures Developed for GNSS Security

Multi-GNSS Usage (Multi-Constellation): The combined use of GPS, Galileo, GLONASS and BeiDou systems increases signal security (Wen et al., 2025).

Directional Antennas and Filtering Technologies: These are hardware solutions used to reduce the jammer effect (Zhang, Wang & Wu, 2024).

GNSS + Inertial Navigation (INS) Integration: It ensures the continuation of position calculations in short-term GNSS outages (Wang et al., 2024).

eLoran and Terrestrial Alternatives: These are low-frequency, long-range terrestrial navigation systems developed as a backup system for GNSS (Son & Fang, 2024).

1.6. The Importance of National Terrestrial Systems in This Context

Global Satellite Navigation Systems (GNSS), although providing high accuracy and global coverage, pose a strategic risk to many countries in terms of national security due to electronic warfare threats, geopolitical dependency and signal weaknesses. For this reason, national terrestrial navigation systems developed as alternatives or complements to GNSS are increasingly on the agenda. The importance of these systems is not only to provide technical redundancy, but also to play a decisive role in issues such as sovereignty, data control and protection of critical infrastructures (Wu, 2024; Yu et al., 2025; Osechas & McGraw, 2025).

Advantages of national terrestrial systems;

National-scale terrestrial navigation systems (e.g. eLoran, DGNSS, terrestrial radio signal systems) provide the following advantages over GNSS (Osechas & McGraw,2025):

Stronger Signals: Signals used in terrestrial systems are stronger than GNSS signals and are more difficult to suppress by jammers.

Low Frequency Broadcasting: Since systems such as eLoran operate at very low frequencies (around 100 kHz), they are less affected by poor weather conditions.

Independence and Sovereignty: Since the management and infrastructure of national systems are provided by local institutions, the risk of external dependency is eliminated.

Comprehensive Backup: Terrestrial systems provide a backup solution in areas where GNSS signals are not available or are mixed (e.g. tunnels, between high-risk buildings in cities).

Protection of Critical Infrastructures: In high-risk sectors such as finance, energy, and transportation, the continuity of the infrastructure is maintained by providing backup for GNSS signals.

1.7. Importance Regarding National Security and Strategic Resilience

Terrestrial navigation systems are of critical importance in terms of cybersecurity, military operational flexibility, crisis management and strategic autonomy (Wu, 2024; Yu et al.,2025; Osechas & McGraw, 2025).

A terrestrial navigation network developed in accordance with a country's own geography:

- Creates a defensive layer against electronic warfare scenarios.

- Provides uninterrupted direction finding and time synchronization in emergencies and war conditions.

- Strengthens the national sovereignty ground against external interventions of GNSS systems.

In Türkiye, the development of domestic navigation solutions should be evaluated in parallel with domestic defense industry strategies and national technology moves.

2. PLACE OF GNSS SYSTEMS IN SECURITY TECHNOLOGIES

Global Satellite Navigation Systems (GNSS) are satellite-based navigation systems that provide location, speed and time information worldwide. GNSS systems generally consist of the following three main components (Petrovski, 2024):

Space Segment: Consists of satellites orbiting the Earth. These satellites continuously broadcast time-stamped signals.

Ground Control Segment: Consists of a network of ground stations that monitor, direct and control the orbit and clock accuracy of satellites.

User Segment: Devices that calculate location by receiving GNSS signals (military vehicles, mobile phones, aircraft, UAVs, security systems, etc.).

In the basic operation of this structure, three-dimensional location (latitude, longitude, altitude) and precise time information are obtained by receiving at least four satellite signals. The use of GNSS technology in numerous security, defense and public infrastructure applications has made it necessary to increase the diversity and reliability of these systems. In addition, apart from the four most common GNSS types, there are smaller and less common GNSS types called MSAS by Japan, NavIC by India, SouthPAN by Australia and New Zealand, KASS under development by South Korea, and ANGA for African countries (GPS, 2021).

2.1. The Role of Diversification of GNSS Systems in Security

Since each system has different signal structures, frequency bands and coverage features, users using signals from more than one GNSS system simultaneously (multi-GNSS) increase location accuracy and ensures security.

This strategy, especially in security technologies;

- increases resistance to electronic warfare scenarios,
- provides continuity against system failures,
- increases data security and accuracy.

The use of these multiple systems is becoming increasingly widespread in military platforms, UAVs, smart city security systems and border surveillance technologies.

2.2. Use of GNSS in the Security Sector

Security technologies today require high-precision location data. GNSS systems offer real-time, wide-coverage and low-cost solutions to meet this need. These advantages offered by GNSS have made its use inevitable in many areas, from law enforcement to military units, from border security to urban security infrastructures (Haloho & Supriyadi, 2024).

Border Security;

GNSS works in integration with both fixed and mobile sensor platforms in border surveillance systems, clearly determining the coordinates of UAVs, land vehicles and watchtowers, and providing digital mapping of moving targets and border violations. In addition, instant detection of smuggling and illegal crossings becomes more effective with GNSS-supported coordinate systems.

Military Operations;

Position superiority in the modern battlefield means strategic advantage.

GNSS-supported military applications include:

- Locking on the exact location of the target in precision-guided munitions (PGM) systems,

- Unit coordination and logistics tracking,

- Operation of navigation and targeting systems on air and land and sea platforms,

- Providing location awareness in night operations in low visibility conditions.

In NATO doctrines, GNSS is defined as a “force multiplier”

Smart City Surveillance

Drone-based surveillance systems rely on GNSS to perform autonomous patrols in certain areas. Vehicle tracking systems are used in directing emergency vehicles and monitoring urban security incidents. Solutions such as pedestrian safety systems and traffic light optimization are integrated with GNSS data.

Patrol Systems of Law Enforcement Forces

The instantaneous locations of police and gendarmerie vehicles are monitored by centers, and intervention times are optimized with GNSS data. The direction of patrol units closest to critical incidents is provided by the integration of

geographic information systems (GIS) and GNSS. In addition, the time and location stamps of data recorded by devices such as mobile cameras and body cameras are obtained via GNSS.

Table-1 General GNSS Systems

	Developer /Number of Satellites	**First Satellite Launch**	**Full Operational Status**	**Description**
GPS	USA /24	1978	1995	Provides high accuracy location and time information; available in military (P(Y)-Code) and civilian (C/A Code) modes of use. Critical Use: Military operations, guided munitions, crisis management, time synchronization.
GLONASS	Russia /24	1982	1996	It offers a stronger signal in the northern hemisphere and can work in parallel with GPS. Russia has reduced external dependency in defense by eliminating GNSS dependency with GLONASS.
Galileo	European Union /24	2011	2022	High precision civilian use includes encrypted Public Authority Service (PRS). To reduce Europe's dependence on GPS, providing high accuracy for civilian and autonomous systems.
BeiDou	China /35	2000	2020	It offers global service, is available for military and civilian use, has text messaging and localized services. It is used as an alternative to GPS in the Asia-Pacific region as part of China's bid to increase its digital dominance.

2.3. Terrestrial Navigation Systems

Global Satellite Navigation Systems (GNSS), despite providing high accuracy and global coverage, may be insufficient to provide a fully independent, sustainable and secure positioning infrastructure for many countries, especially due to their vulnerability to signal interruptions and external dependency problems. Terrestrial navigation systems developed to eliminate these vulnerabilities stand out as strategic backup systems that can both work as an alternative to GNSS and as integrated with it. Terrestrial navigation systems are systems in which the user's position is calculated via signals from fixed broadcasting stations on the earth. These systems are generally based on technologies such as Long-wave radio signals (Low Frequency) or Wide-area differential GNSS (DGNSS) networks (Wu, 2024; Yu et al.,2025; Osechas & McGraw, 2025). Unlike GNSS, since the signal sources in these systems are on the earth, the signals are less affected by atmospheric events and the signal strength is much higher. This makes them more resistant to jammer and spoofer attacks.

Major Terrestrial Navigation Systems

Loran-C / eLoran (Enhanced Loran): Uses low-frequency (100 kHz) radio signals. Intercontinental range; can be used in maritime, aviation and military systems. Provides time synchronization without requiring fiber optic infrastructure. Highly resistant to jamming and spoofing. Countries such as the USA, England and South Korea are re-commissioning or modernizing their eLoran infrastructures. eLoran is considered as a GNSS backup, especially for critical infrastructures (Son & Fang, 2024).

DGNSS (Differential GNSS): Fixed stations produce real-time correction data based on GNSS signals and this data is shared with mobile users. It can be used in areas such as port authorities, maritime, land transportation and agriculture. Provides high-accuracy location data; Although it works dependent on GNSS, it aims to correct its errors (Li, et al., 2024).

RTK (Real-Time Kinematic) Systems: Provides centimeter-level accuracy by applying precise differential corrections to GNSS signals. It is used especially in unmanned land vehicles, agricultural machinery and construction equipment. It works with real-time data sharing via terrestrial base stations (Fredeluces et al., 2024; Tavasci, Nex & Gandolfi, 2024).

Terrestrial navigation systems are not an alternative on their own; they offer a much more effective security solution when integrated with GNSS. This

integration ensures system continuity in the event of a GNSS outage or attack. The probability of error is minimized by performing multi-source verification in location data production. It provides high-precision backup in unmanned systems (UAV/ UCAV), military platforms and critical facilities.

In countries with a geopolitically critical position such as Türkiye, absolute dependence on GNSS can cause serious security and sovereignty problems. For this reason:

- Developing domestic terrestrial navigation infrastructures,
- Producing integrated solutions with institutions such as the Defence Insdustry Agency, TÜBİTAK, ASELSAN,
- Establishing terrestrial backup systems such as eLoran for critical facilities (airports, ports, power plants) should be among the strategic priorities in terms of national security policies.

Threats to GNSS Systems

GNSS systems, due to the technological sensitivity they contain, have serious security vulnerabilities, especially against electronic warfare (EW) techniques. The inherently weak signal strength of these systems puts them at risk in both civilian and military use as they can be targeted with methods such as jamming, spoofing and physical intervention.

Jamming attacks are based on the principle of suppressing GNSS signals with high-powered interference signals. This causes the receiving device to be unable to detect the GNSS signal and calculate its location. Jamming devices are usually portable and can be used in land vehicles, drones or fixed stations. Military convoys, air traffic, logistics lines and emergency services can be directly affected by jamming.

Spoofing is the process of sending fake signals to the user's GNSS receiver, causing it to receive false location information. Spoofing attacks can create scenarios such as manipulating the route of UAVs, redirecting guided munitions off-target, and misleading law enforcement and military vehicles to unintended areas. In 2013, a research group from the University of Texas used a GPS spoofer to divert a yacht off-course at sea, and presented this situation as a warning about security vulnerabilities worldwide (Humphreys et al., 2013).

Scenarios of Disabling GNSS through Enemy Interference

Enemy elements may perform actions such as suppressing signals in a wide area via electronic warfare platforms, targeting GNSS control centers through cyber attacks, using missiles to destroy GNSS satellites, physical sabotage or digital

interference on GNSS ground stations. These scenarios may cause a countries' navigation, reconnaissance, surveillance and weapon systems to be rendered ineffective, especially in times of war or crisis.

Absolute dependence on a single GNSS system: It may cause disruption of system synchronization in critical infrastructures (banking, energy, communication), loss of direction and time in sectors such as air traffic, land transportation and port management, mission cancellation or collisions in unmanned systems (UAV/UCAV, autonomous vehicles), collapse of the logistics chain in military operations. Therefore, the activation of alternative or complementary location systems (terrestrial systems, inertial navigation, etc.) has become mandatory for national security.

Realized Examples (Case Studies)

Norway – NATO Exercise (2018): During NATO's "Trident Juncture" exercise, civilian aircraft in Norway and Finland experienced GPS loss. It was claimed that the incident was caused by electronic warfare systems in Russia's Kola Peninsula (Reuters, 2018).

GNSS Spoofing Over the Black Sea (2017): A US Navy ship received fake signals in its GPS data indicating that the ship had run aground. Subsequent analysis showed that many ships in the area were experiencing similar problems at the same time (Androjna & Perkovič, 2021).

Israel – Jammer Operations (2022): GNSS jamming applications carried out against drone threats in Israeli airspace also affected the navigation systems of civilian aircraft in the vicinity (NDTV, 2023)

China BeiDou Satellite Signal Suppression – India Border (2020): Reports of BeiDou signal suppression along the China-India border have been reported, particularly affecting UAV patrols (iadnewa, 2022).

Table-2 Advantages and Disadvantages of Terrestrial Systems Compared to GNSS

Feature	Terrestrial Systems	GNSS Systems
Signal Strength	Very strong (jammer resistant)	Weak, easy to suppress
Coverage	Regional/continental	Global
Signal Source	Earth Stations	Area Orbiting Satellites

Time Synchronization	Possible with eLoran	Possible via GPS/Galileo
Complexity	Infrastructure setup costs can be high	Infrastructure already exists (but externally dependent)
Security	Advantage of local control	Risk of geopolitical dependency

Countries with geostrategic positions like Türkiye should establish their own terrestrial navigation infrastructures against possible threats from GNSS systems. In this context: Local Loran/eLoran station networks can be developed with joint projects of the Defense Industries Agency (SSB) and institutions such as ASELSAN and TÜBİTAK. The Ministry of Transport and Infrastructure can back up critical transportation networks by expanding the DGNSS infrastructure in ports and airports. Local atomic clocks will be a critical element to increase the sensitivity of signal sources. These infrastructures have strategic value in terms of Türkiye's military autonomy, cyber and electronic warfare defense, and civil infrastructure security.

Terrestrial systems can be used as redundant or fallback systems for GNSS systems:

- Thanks to dual-system receivers, both GNSS and terrestrial signals can be monitored.

- In scenarios where GNSS is disabled, terrestrial systems ensure mission continuity.

- Especially in critical mission applications (military targeting, time synchronization, disaster management), terrestrial systems play a vital role.

- Terrestrial solutions serve as critical backup infrastructure for sensitive sectors such as smart cities, 5G infrastructure, energy distribution systems, and financial time stamping.

3. APPLICATIONS IN TÜRKİYE AND THE WORLD

Developed and developing countries, aware of the threats to GNSS systems, are taking strategic steps to develop both independent global systems (GPS, BeiDou, Galileo, GLONASS) and ground-based alternative navigation solutions. In this context, the revival of terrestrial systems such as eLoran and the establishment of domestic GNSS infrastructures have become priorities in terms of national security and technological sovereignty.

USA eLoran Infrastructure Example; Although the US deactivated the Loran-C system in 2010, it has strategically put the reactivation of the eLoran system on the agenda due to the vulnerability of GNSS. In 2020, the U.S. Department of Transportation recommended that eLoran be evaluated as an alternative timing and positioning solution to GNSS. It is planned to be used especially in sectors dependent on GNSS such as energy infrastructure, emergency response systems, and banking systems. The US positions the eLoran system as a strategic reserve and is testing signal integrations at test sites run jointly with the private sector (Offermans, Bartlett & Schue, 2017).

Russia GLONASS & Chayka; GLONASS is a GNSS system under the control of the Russian Ministry of Defense and offers a global alternative to GPS. Chayka is a low-frequency terrestrial system similar to Loran-C. Russia ensures continuity with GLONASS-Chayka integration in the event of a GNSS outage (Kugler, 1999).

China BeiDou & PNT Alternatives; BeiDou is China's independent GNSS system. It provides high accuracy in Asia-Pacific and offers global access. In addition to the BeiDou system, China is developing short-range terrestrial PNT systems and fiber-based time synchronization systems. Russia and China are preparing for electronic warfare scenarios by building systems that provide full sovereignty in the GNSS field and are closed to external interventions (Koca, 2019).

3.1. Current GNSS Infrastructure and Alternative Navigation Projects in Türkiye

Türkiye is currently working with multiple GNSS receiver systems that can use GPS, Galileo, GLONASS and BeiDou signals. TÜRKSAT satellites and communication and observation satellites developed by TÜBİTAK UZAY do not directly produce GNSS, but they support data integrity. Institutions such as ASELSAN, TÜBİTAK BİLGEM, HAVELSAN are conducting studies on INS (Inertial Navigation Systems) and GNSS-supported terrestrial analysis infrastructures (TÜBİTAK, 2022). The National Satellite Timing and Positioning System project is among the long-term goals; it is aimed to reduce dependency on GNSS (TUALCOM, 2022). Türkiye Ports DGNSS System: It is a system established by the Ministry of Transport and Infrastructure in the maritime field and broadcasts real-time corrections.

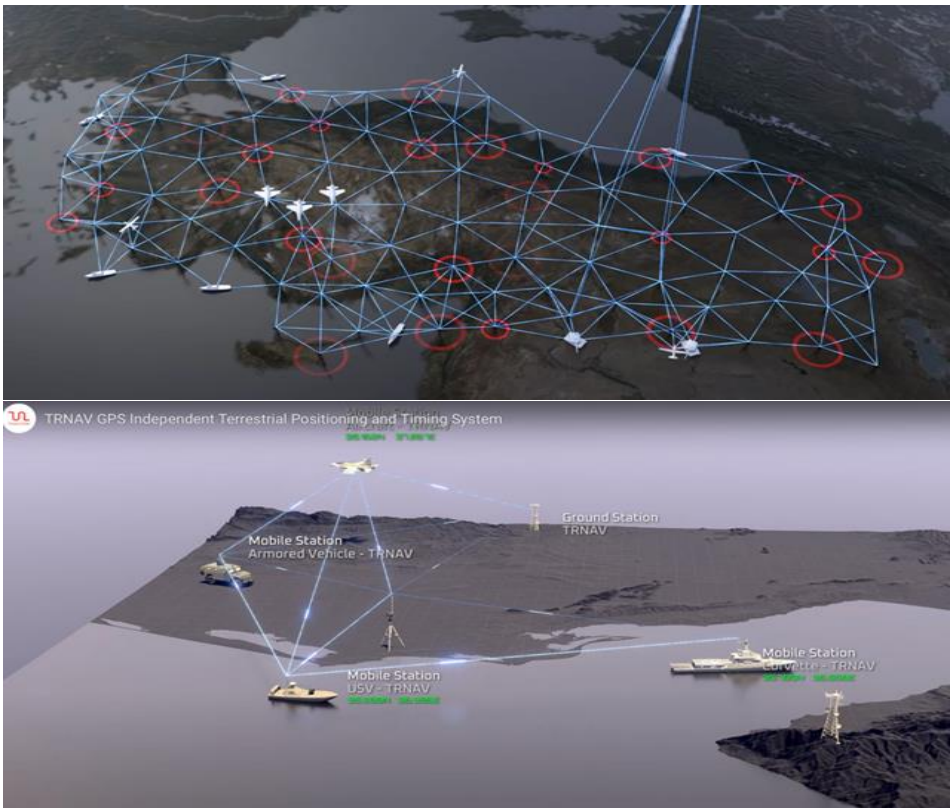

Figure-1 Independent Terrestrial Positioning and Timing System (TUALKOM, 2022)

UAV/ UCAV Systems: INS-GNSS hybrid systems are used in UAV platforms such as Bayraktar TB2, Akıncı and Anka, and when GNSS weakens, the inertial system is activated. Tactical Field Systems: Some command and control systems developed by ASELSAN have backup algorithms that can operate without a GNSS signal.

Autonomous Land Vehicles: Unmanned land vehicles developed by companies such as Roketsan and BMC are equipped with non-GNSS direction finding modules.

Reducing GNSS dependency in domestic defense products has become a necessity in order to ensure system continuity in the electronic warfare environment.

The dependency on GNSS systems on a global scale has led to the emergence of new areas of vulnerability in national security strategies. The dependency on location, time and direction data, especially in strategic areas such as military operations, energy distribution, the financial sector and critical public services, has made the uninterrupted operation of these systems a necessity. In this context, terrestrial navigation systems stand out not only as a technical backup in terms of national security policies, but also as an element of sovereignty and strategic resilience.

This situation particularly exposes user countries to risks such as: Signal interruption (intentional denial), Regional degradation, Political pressure or decommissioning in times of crisis. Therefore, the development of national terrestrial navigation systems should be one of the fundamental pillars of national defense and technology policies. Thus; External dependency is reduced, Domestic production capacity in critical technologies is increased, Strategic autonomy is ensured

3.2. Cyber Security Dimension of Terrestrial Navigation Systems

GNSS systems are generally vulnerable to threats at the physical layer (jammer, spoofer) because they use weak signals on the receiver side. However, terrestrial systems; are more resistant to physical interventions thanks to strong signal broadcasting, can be closed to external cyber manipulation due to fixed and locally controlled signal sources, can be integrated with critical communication networks (e.g. national fiber infrastructure, satellite-link supported signals), and they can ensure secure data transfer can be provided. Thus, terrestrial systems become an important component of both physical and cyber security architectures (Androjna et al., 2020).

Critical sectors such as energy, transportation, communication, banking: are dependent on GNSS-integrated time synchronization, Geographic location-based decision systems, Automatic routing and control algorithms.

GNSS outage or deviation in these systems can cause chain system errors and large-scale operational disruptions. Therefore; Terrestrial navigation systems should be activated as a backup for GNSS. In particular, energy grids, emergency response centers, airports and border control systems should be equipped with multiple navigation systems.

3.3. Multi-Layered Navigation Systems Proposal (GNSS + Terrestrial + Inertial Systems Integration)

Table-3 The Role of Systems

System Component	Role
GNSS	Global reach, high accuracy (primary source)
Terrestrial System (eLoran, DGNSS)	**Jammer/spoofer resistance, regional backup (second layer)**
Inertial Navigation (INS)	Heading/cone/acceleration tracking even without GNSS signal (last line of defense)

Thanks to this structure; when GNSS is disabled, the systems continue to work without interruption and even if a GNSS signal is received, verification can be made with terrestrial and inertial systems and system integrity is protected against enemy intervention. INS+GNSS hybrid structures are used in UCAV and missile systems developed in Türkiye, and these systems can continue their mission even in attacks on GNSS (van Toll, Cook & Geraerts, 2011).

CONCLUSION

GNSS systems have revolutionized both civil and military technologies with their high accuracy, global coverage, low cost and versatile application areas. They have digitized and automated business processes by providing location, time and direction data in many critical areas such as transportation, energy, communication, finance and defense. However, this widespread use has also made GNSS systems strategic vulnerabilities. Weak signal strength, vulnerability to electronic warfare attacks such as jammers and spoofers, geopolitical dependency, and the risk of systemic collapse from a single point stand out as threats that can overshadow the advantages of GNSS systems. Developing national terrestrial navigation systems against the above-mentioned vulnerabilities of GNSS systems is no longer an option, but a national security requirement. The high signal strength, local controllability and jammer/spoofer resistance of terrestrial systems make them a critical complement to GNSS. Establishing systems such as eLoran, DGNSS, RTK as regional networks, establishing national time and location infrastructures, and ensuring integration with INS (Inertial Navigation Systems) are the foundations of resilience in today's security technologies. These investments also contribute to the deepening of the domestic defense industry, the prevention of technology transfer, and the strengthening of national technological sovereignty.

For the sustainability and prevalence of terrestrial navigation systems, not only technological but also legal and administrative foundations need to be built:

- Legal Regulations: Regulation of terrestrial PNT systems, frequency allocation, cyber security protocols, data security and critical infrastructure coordination laws should be enacted.
- Institutional Coordination: Coordination should be established between institutions such as the Defense Industries Agency, Ministry of Transportation, AFAD, ASELSAN, TUBITAK and national PNT councils should be established.
- Infrastructure Planning: Ports, airports, military bases, energy production and distribution centers should be supported with terrestrial signal infrastructure.

Research and technology policies should support both academic and industrial R&D projects by focusing on non-GNSS direction finding technologies. Proposed research areas include:

- Cryptographic security of terrestrial navigation signal protocols
- INS-GNSS-eLoran triple navigation algorithms
- PNT backup scenarios for autonomous systems
- Development of indigenous atomic clock technology
- PNT architectures resistant to cyber attacks
- Urban micronavigation systems (RFID, 5G supported local systems)

The results of these studies will ensure the security of national PNT systems not only for military but also for civil critical infrastructures, financial markets, transportation systems and smart city applications. While GNSS technologies form the invisible backbone of the modern world, a multi-layered positioning infrastructure supported by terrestrial and inertial systems is now a necessity to prevent scenarios that may occur in the event of an interruption of this backbone. Increasing Türkiye's national capacity in this area is not only a technical advancement, but also a strategic security policy.

REFERENCES

Aktuğ, Ş. (2015). Art Of Celestial Navigation. İstanbul: Piri Reis Üniversitesi Yayınları.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 776.

Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, *10*(02), 361-373.

Borodacz, K., & Szczepański, C. (2024). GNSS denied navigation system for the manoeuvring flying objects. *Aircraft Engineering and Aerospace Technology*, *96*(1), 63-72.

Dovis, F. (Ed.). (2015). *GNSS interference threats and countermeasures*. Artech House.

Duraklar, K. (2025) FPGA-Based Embedded System for Real-Time Detection and Analysis of RF Signals in Tactical Electronic Warfare. 2nd International Conference on Engineering, Natural Sciences, and Technological Developments (ICENSTED 2025), 493.

Enge, P. K. (1994). The global positioning system: Signals, measurements, and performance. *International Journal of Wireless Information Networks*, *1*, 83-105.

Fredeluces, E., Ozeki, T., Kubo, N., & El-Mowafy, A. (2024). Modified RTK-GNSS for challenging environments. *Sensors*, *24*(9), 2712.

Göde, E., Teoman, A., Kushan, M. C., Tonbul, K., Öğünç, G. İ., & Daz, B. (2024). Global Navigation Satellite System (GNSS) Independent Navigation for Unmanned Aerial Vehicles (UAV). *Journal of Aviation Research*, *6*(1), 53-88.

GPS (2025). https://www-gps-gov.translate.goog/systems/gnss/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=tc (Access date: 22.04.2025)

Grejner-Brzezinska, D. A., Toth, C. K., Moore, T., Raquet, J. F., Miller, M. M., & Kealy, A. (2016). Multisensor navigation systems: A remedy for GNSS vulnerabilities?. *Proceedings of the IEEE*, *104*(6), 1339-1353.

Haloho, L. S., & Supriyadi, A. A. (2024). Utilization of satellite technology in communication systems, disaster monitoring, border surveillance, and military intelligence: A literature review. *Remote Sensing Technology in Defense and Environment*, *1*(1), 36-44.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2013). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proceedings of the Institute of Navigation GNSS Conference*, 2314-2325Selbesoğlu, H. Ş., Barutçu, B., & Çökelez, A. (2021). The Brief History of Early Marine-Navigation. *Advanced Geomatics*, *1*(1), 14-20.

ICAO. (2021). Performance-Based Navigation (PBN) Manual**.** International Civil Aviation Organization.

Iadnewa, (2022). https://iadnews.in/china-abruptly-restricts-the-use-of-beidou-along-borders-with-india/ (Access date: 18.04.2025)

Jhanjhi, N. Z., Gaur, L., & Khan, N. A. (2024). Global Navigation Satellite Systems for Logistics: Cybersecurity Issues and Challenges. *Cybersecurity in the Transportation Industry*, 49-67.

Johnson, G. W., Swaszek, P. F., Hoppe, M., Grant, A., & Šafář, J. (2017). Initial results of MF-DGNSS R-Mode as an alternative position navigation and timing service.

Kaplan, E. D., & Hegarty, C. J. (2017). Understanding GPS/GNSS: Principles and Applications (3rd ed.). Artech House.

Koca, B., & Ceylan, A. (2018). Uydu konum belirleme sistemlerindeki (GNSS) güncel durum ve son gelişmeler. *Geomatik*, *3*(1), 63-73.

Koca, B. (2019). GNSS sistemlerindeki güncel durum ve son gelişmelerin incelenmesi.

Kugler, D. (1999). Integration of GPS and Loran-C/Chayka: A European Perspective. *NAVIGATION: Journal of the Institute of Navigation*, *46*(1), 1-12.

Li, X., Cheng, F., Li, Y., Shen, P., Hu, Y., & Lu, X. (2024). DGVINS: tightly coupled differential GNSS/visual/inertial for robust positioning based on optimization approach. *Measurement Science and Technology*, *35*(8), 086307.

NDTV, (2023) "Planes losing gps signal over middle-east, indian regulator flags threat". https://www.ndtv.com/india- news/planes- losing- gps- signal-over- middle- east- indian- regulator- raises- concern- 4602298

Offermans, G., Bartlett, S., & Schue, C. (2017). Providing a resilient timing and UTC service using eLoran in the United States. *Navigation: Journal of The Institute of Navigation*, *64*(3), 339-349.

Osechas, O., & McGraw, G. (2025, January). Terrestrial Navigation Alternatives to Support PBN for Current and Future Aviation. In *Proceedings of the 2025 International Technical Meeting of The Institute of Navigation* (pp. 253-267).

Petrovski II, I. G. (2024). Instrument of Choice: GNSS. In *The Ionosphere with GNSS SDR: Specialized Software-Defined Radio for In-Depth Ionospheric Research* (pp. 77-144). Cham: Springer International Publishing.

Reuters. (2018, November 13). Norway accuses Russia of disrupting GPS signals during NATO drill. Retrieved from. https://www.reuters.com/article/world/norway-says-it-proved-russian-gps-interference-during-nato-exercises-idUSKCN1QZ1WM/(Access date: 10.04.2025)

Sobel, D. (2004). Longitude: The true story of a lone genius who solved the greatest scientific problem of his time. *Academy of Management Learning and Education*, *3*, 220-220.

Son, P. W., Rhee, J. H., & Seo, J. (2017). Novel multichain-based Loran positioning algorithm for resilient navigation. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(2), 666-679.

Son, P. W., & Fang, T. H. (2024). Enhancing coastal air navigation: eLoran 3D positioning and cycle slip mitigation. *IEEE Access*.

Steiner, J., Pleninger, S., & Hospodka, J. (2024, April). Assessing the Vulnerability of Aviation Systems to GNSS Meaconing Attacks. In *2024 New Trends in Civil Aviation (NTCA)*(pp. 213-218). IEEE Trýb, J., & Hospodka, J. (2025). GNSS Interference and Security: Impacts on Critical Infrastructure and Mitigation Strategies. *Procedia Computer Science*, *253*, 2635-2644.

Spilker Jr, J. J., Axelrad, P., Parkinson, B. W., & Enge, P. (Eds.). (1996). *Global positioning system: theory and applications, volume I*. American Institute of Aeronautics and Astronautics.

Tavasci, L., Nex, F., & Gandolfi, S. (2024). Reliability of Real-Time Kinematic (RTK) Positioning for Low-Cost Drones' Navigation across Global Navigation Satellite System (GNSS) Critical Environments. *Sensors (Basel, Switzerland)*, *24*(18), 6096.

TUALCOM (2022). https://www.tualcom.com/trnav-turkiyenin-milli-konumlama-ve-zamanlama-sistemi/(Access date: 11.04.2025)

TÜBİTAK SAGE. (2022). Yerli Navigasyon Sistemleri Ar-Ge Yol Haritası Raporu**.**

van Toll, W. G., Cook IV, A. F., & Geraerts, R. (2011). Multi-Layered Navigation Meshes. *ASCI-IPA-SIKS tracks, ICT. OPEN*, 317-323.

Yu, A., Kolotylo, I., Hashim, H. A., & Eltoukhy, A. E. (2025). Electronic Warfare Cyberattacks, Countermeasures and Modern Defensive Strategies of UAV Avionics: A Survey. *IEEE Access*.

Zhang, C., Wang, D., & Wu, J. (2024). Two-Dimensional Directions Determination for GNSS Spoofing Source Based on MEMS-Based Dual-GNSS/INS Integration. *Remote Sensing*, *16*(23), 4568.

Wang, L., Chen, L., Li, B., Liu, Z., Li, Z., & Lu, Z. (2024). Development status and challenges of anti-spoofing technology of GNSS/INS integrated navigation. *Frontiers in Physics*, *12*, 1425084.

Wen, X., Melgård, T., de Vries, R., Vigen, E., & Panosyan, A. (2025, January). Real-Time Multi-Constellation Navigation Message Authentication for Enhanced GNSS Security. In *Proceedings of the 2025 International Technical Meeting of The Institute of Navigation* (pp. 464-478).

Wu, D. L. (2024). GNSS Signal Jamming as Observed From Radio Occultation. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*.