**UDC 528.2, 528.3**

[1,2,3,4,5,6,7]Ivan BRUSAK[1*] Volodymyr BABCHENKO[2*] Natalia SAVCHUK[3*] Vladyslav MARCHUK[4*] Yurii SHKVAROK[5*] Mykhailo TURIANYTSIA[6*]

[1,2,3,4,5,6,7]Institute of Geodesy, Lviv Polytechnic National University, 12 Bandery Str., Lviv, 79013, Ukraine, e-mail: [1]ivan.v.brusak@lpnu.ua, https://orcid.org/0000-0001-5434-4931, [2]volodymyr.a.babchenko@lpnu.ua, [3]nataliia.savchuk.hd.2021@lpnu.ua, https://orcid.org/0009-0005-3396-7706, [4]vladyslav.marchuk.hd.2022@lpnu.ua, https://orcid.org/0009-0004-8411-9806, [5]yurii.i.shkvarok@lpnu.ua https://orcid.org/0009-0001-8614-179X, [6]mykhailo.m.turianytsia@lpnu.ua, https://orcid.org/0009-0000-5433-2834

https://doi.org/10.23939/istcgcap2024.99.028

# NEW CHALLENGES FOR EXPLOITATION OF CONTINUOUSLY OPERATING REFERENCE GNSS STATIONS DURING HOSTILITIES. CASE STUDY OF UKRAINE

The study presents the current state of GNSS Continuously Operating Reference Stations (CORS) networks and their operational characteristics during the ongoing hostilities in Ukraine. Stable GNSS CORS network operation is crucial not only for agricultural, geodetic, and land management tasks but also for military navigation and topography. The aim of this work is to analyze the impact of hostilities in Ukraine's GNSS network, considering factors like temporary occupation of certain territories, power outages due to missile strikes on energy infrastructure, and GNSS signal jamming using radio-electronic methods in front-line regions. Another objective of this study is to highlight examples of incorrect RTK or VRS operation due to potential errors from radio-electronic jamming or GPS spoofing as well as to provide practical recommendations for surveyors. As a result, the research has analyzed changes in the number of properly functioning GNSS stations from 2021 to 2023 using the GeoTerrace and System.NET networks. These networks cover all regions of Ukraine except the temporarily occupied territories by russia. Daily processing of RINEX files with a sampling interval of 30 seconds from CORS GNSS stations was conducted using the Bernese GNSS v.5.2 software package over three years. It was noted that following the large-scale invasion in February 2022 and through the spring of that year, there was a sharp reduction of about 10% in the number of properly functioning active GNSS stations. Scientific novelty and practical importance. The article presents practical recommendations for users, such as surveyors and land managers, performing GNSS measurements in RTK or VRS modes using permanent stations, to assess the influence of radio-electronic jamming or GPS spoofing on observations. CORS network assessment and daily calculated coordinates of GNSS stations from 2021 to 2023 can be used for future geodynamic research in the region.

*Key words:* Continuously Operating Reference Stations, GNSS networks, Ukraine, GNSS data processing, GeoTerrace GNSS network, System.NET GNSS network, electromagnetic warfare of GNSS signal, GNSS spoofing.

## Introduction

The development of GNSS Continuously Operating Reference Stations (CORS) networks is crucial for ensuring the accuracy, reliability, and availability of geodetic and navigation services. It is also of significant value for various sectors of science, technology, economy, and defence. Nowadays, a number of CORS networks, both state-owned and private, operate across Ukraine. They belong to Main Astronomical Observatory National Academy of Sciences of Ukraine (MAO), State Geocadastre of Ukraine (UPM GNSS), System Solutions Ltd. (System.NET), Lviv Polytechnic National University (GeoTerrace), Navigation-Geodetic Center (NGC.net), Kyiv Institute of Land Relations (Kyiv POS), Ukrainian Coordinate-Time Providing System (NET.Spacecenter), and TNT TPI Company (RTKHUB Network), and other.

The first permanent GNSS station in Ukraine was established in 1997. And during 11 year period, the number of stations increased to 18 [Ishchenko, 2009]. Subsequently, the number of permanent GNSS stations has continually risen. By 2012, no fewer than 8 operators were servicing 98 stations [Savchuk, 2012]. 9 operators were managing 297 active GNSS stations: 257 privately owned and 40 state-owned according to the assessment by [Novikova et al., 2020] in 2019. In October 2021, a study [Khoda and Ishchenko, 2021] presented on 239 GNSS stations processed at the local analytical center of MAO NAS of Ukraine using Bernese GNSS Software for rapid daily data processing to monitor their stability. The daily coordinates obtained using CODE rapid products enable the monitoring of CORS stability. According to results [Khoda 2023], from May 2020 to November 2022,

273 Ukrainian permanent GNSS stations were used for the IGb14 system propagation. As for spring 2024, the latest update on the Ukrainian GNSS network website [Ukrainian GNSS Network] was made on November 10, 2020, listing 417 active and 108 dismantled Ukrainian CORS. It can be assumed that the total number of CORS in Ukraine exceeded 450 before the full-scale russian invasion in February 2022.

Among the GNSS stations used in the CORS networks, five Ukrainian stations such as Holosiiv (GLSV), Kharkiv (KHAR), Mykolaiv (MIKL), Poltava (POLV), Uzhhorod (UZHL) are part of the International GNSS Service [IGS] network. At the same time, 14 GNSS stations such as Chernihiv (CNIV), Horodok (GDRS), Dnipro (DNMU), Holosiiv (GLSV), Kropyvnytskyi (KRRS), Katsevely (KTVL), Mariupol (MARP), Mykolaiv (MIKL), Mukachevo (MKRS), Poltava (POLV), Pryluky (PRYL), Rivne (RVNE), Smila (SMLA), Uzhhorod (UZHL), are included in European Permanent GNSS Network [EUREF]. Stations such as Alchevsk (ALCI), Yevpatoria (EVPA), Izmail (IZRS), Vinnytsia (VNRS), and Zaporizhzhia (ZPRS) were also previously part of the EUREF network. They were, however, dismantled or ceased operations because the territories were temporarily occupied by russia starting from 2014.

In Ukraine, there are other private CORS stations not unified into a network. They are particularly used as a source of navigation corrections for agricultural enterprises and land departments in local areas of cities or regions.

Since none of the above-mentioned GNSS networks fully cover the whole territory of Ukraine, this study has selected two networks, such as GeoTerrace and System.NET, for assessing the characteristics and processing of data from CORS. These networks geographically complement each other and cover all regions of Ukraine except forthe temporarily occupied territories.

The GeoTerrace network of the Lviv Polytechnic National University uniformly covers the west, south, and central parts of Ukraine with every 70 km distance from each permanent GNSS station [Tretyak & Brusak 2022]. Specifically, among the regions of Ukraine that are fully or partially covered by the network are: Lviv, Volyn, Rivne, Ternopil, Chernivtsi, Ivano-Frankivsk, Zakarpattia, Khmelnytskyi, Vinnytsia, Odesa, Mykolaiv, Kherson, Dnipropetrovsk, Kirovohrad, Cherkasy, Poltava, Zaporizhzhia. GeoTerrace is the largest network of active GNSS stations owned by the state. It comprises approximately 80 active GNSS stations connected via the internet to a control center at Lviv Polytechnic University as of spring 2024.The stations of the GeoTerrace network are mainly equipped with GNSS receivers from Trimble and Leica companies. System.NET network processes a larger number of stations, reaching around 300 units in recent years. In 2019, the private System.NET network obtained the status of a geodetic network of special purpose [Novikova et al. 2020]. GNSS stations of System.NET network are predominantly equipped with Leica receivers. It is also worth noting that these networks provide full integration with the EUPOS networks (Poland, Slovakia, Hungary, Romania) and Moldova. GeoTerrace and System.NET networks are managed by separate control centers where continuous GNSS measurements are carried out using GPS, GLONASS, GALILEO, and BEIDOU systems.

GNSS CORS stations provide spatial coordinates of the ITRF, ETRF, and USK-2000 systems, and the Baltic Height System. The spatial coordinates of all stations are determined daily, creating a time series bank of their kinematics. GNSS CORS stations must meet several conditions for the operation. Firstly, stable electrical power supply is necessary to ensure that the equipment can work continuously and uninterruptedly. Secondly, a stable internet connection must ensure constant data transfer to the server. Thirdly, the GNSS antenna must be securely mounted and have visibility to satellites, that is, the sky should be open and unobstructed. To meet the above requirements, most GNSS CORS stations are installed on buildings built long ago. Antennas are mounted on a metal mast attached to the external northern side of a brick superstructure on the building's roof and are equipped with lightning protection. To strictly align the antenna plane horizontally, the antenna mount is equipped with a trigger with a pin, which is brought into a vertical position using screws and a spirit level. The antenna is oriented northward. The antenna is connected to the receiver with a coaxial cable, usually located in the utility room of the building. An example of the installation and operation of one of GNSS CORS

stations is TERE station which belongs to the GeoTerrace network. It is shown in detail in [Tretyak et al. 2022].

The continuity and stability of data receiving from permanent stations over long periods allow for the reliability of operations and the detection of anomalies in GNSS time series that may occur over an extended period. Continuous collection and analysis of data enable monitoring, specifically Earth crust monitoring, seasonal atmospheric fluctuations, which are important for identifying trends and predicting possible deformations [Tretyak et al., 2021, Tretyak & Brusak, 2022]. Thus, receiving data from GNSS CORS stations over a prolonged period is a key element in ensuring the stability, accuracy, and reliability of GNSS systems in various fields of practical, military, and civil applications and science.

## Aim

The **aim** of this work is to analyze the changes in the number of properly functioning GNSS CORS stations in the GeoTerrace and System.NET networks during the period from 2021 to 2023. In particular, it is important to assess the features of GNSS data processing before and after the full-scale russian invasion of Ukraine. It is worth considering several new features during the hostilities, related to spoofing attacks or jamming of GNSS signals, which require practical advice for civil users of CORS networks in real-time kinematic (RTK) mode. The stable operation of GNSS CORS networks is crucial not only for agricultural, geodetic, or land management work but also for refining navigation or topography for military purposes.

## Features of GNSS data processing

GNSS data processing from GeoTerrace and System.NET CORS networks from 2021 to 2023 was conducted using the Bernese GNSS v.5.2 software package, developed by the team at the University of Bern [Dach et al., 2015]. The initial data are raw data files in RINEX format with a sampling interval of 30 seconds. The processing was conducted using a double-difference method based on IGS network stations. Calculations are performed using only GPS signals. The latest IGS14 standards for phase center variation and other corrections required for accurate GNSS data calculations are observed.

The data processing started with the preliminary analysis of phase data for each baseline using triple-difference techniques. Any cycle slips are resolved by analyzing different linear combinations of L1 and L2 frequencies, and unreliable data points are removed or recalibrated. A 7-degree cutoff angle is set. The GMF and DRY-GMF models with a two-hour update frequency are utilized to assess tropospheric delays. Ionospheric effects are mitigated using the ionosphere-free linear combination of dual-frequency approaches. They improved the precision of the resolved ambiguities. Solid Earth tide extraction is calculated according to IERS 2010 Conventions, excluding ocean tidal loading and including atmospheric loading effects. Satellite orbits and Earth orientation parameters were derived using the most accurate IGS products to ensure high precision of the calculated coordinates.

The calculated coordinates of GNSS stations are generally obtained with a planned accuracy of 3-4 mm in longitude and latitude, respectively. The accuracy of the height component is 7-8 mm. Coordinate accuracy is presented at a 95% confidence level, which varies depending on the duration of the data, ensuring a reliable and thorough data processing methodology.

## Analysis of changes in the number of GNSS stations

As mentioned earlier in this research, only the GNSS stations of the GeoTerrace and System.NET networks will be considered. Therefore, for simplicity, we will use the term "network" to refer to these two networks.

As of the beginning of 2021, the network consisted of 171 stations. Throughout 2021, there was a gradual expansion of the network, with stations being modernized to improve accuracy and increase reliability. At the beginning of 2022, the network comprised 210 stations, covering the entire territory of Ukraine, except for temporarily occupied territories. The maximum number of stations in Ukraine was recorded on February 10, 11, and 15,

2022 [Khoda, 2024], and in the network we analyzed in this study, there were 227 daily files as of February 1. The dynamics of the increase in the number of stations and the expansion of their distribution grid were observed until February 24, 2022. The network operated stably throughout the year. A statistical diagram showing the monthly changes in the number of GNSS stations on the 1st day of each month is presented in Fig.1.

Following the onset of russia's full-scale invasion, there was a sharp reduction in the number of active GNSS stations, attributed to their damage from missile strikes, destruction of necessary infrastructure for functioning due to active combat operations, and the fact that some stations ended up in temporarily occupied territories. This is also evident in the research [Khoda, 2024]. By spring 2022, the number of properly functioning GNSS stations had significantly decreased, with several dozen stations ending up in temporarily occupied territories or being destroyed by missile strikes, accounting for approximately 10-20% of the total number. Additionally, in 2022, it is noticeable that not all daily files contain 24 hours of observations. The table below provides an overview of the data integrity of GNSS stations in the GeoTerrace and System.NET networks in 2022, taken every 10 days throughout the year.

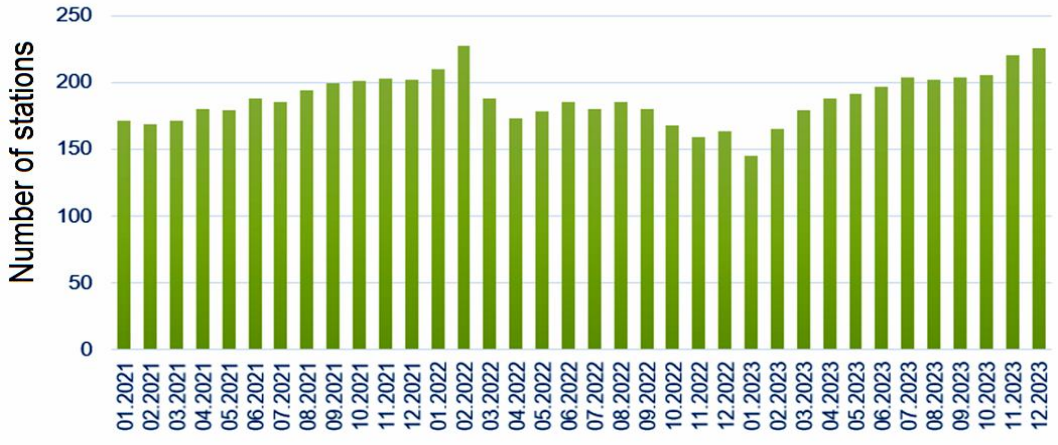


*Fig. 1. Histogram of the monthly change in the number of GNSS stations of the GeoTerrace and System.NET networks from 2021 to 2023*

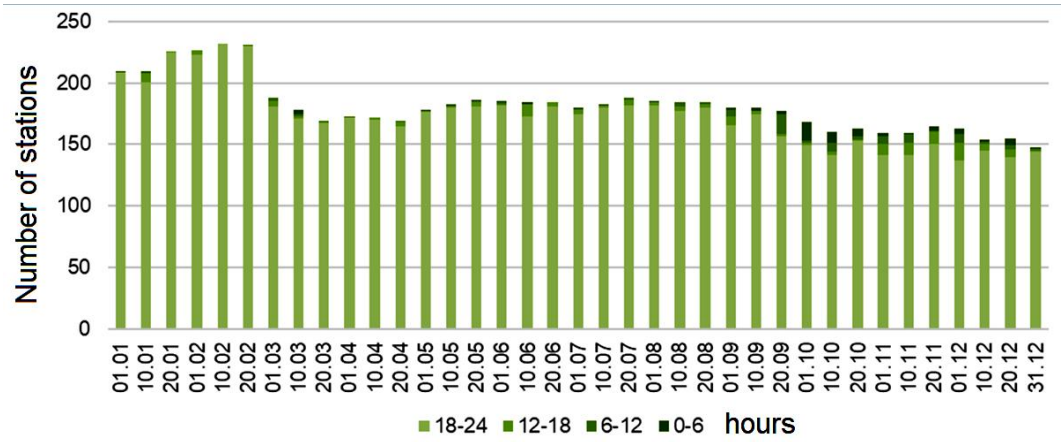


*Fig. 2. Histogram of the change in the number of GNSS stations and the number of observation hours in the daily RINEX file of the GeoTerrace and System.NET networks for 2022*

*Table*

**Data integrity of GeoTerrace and System.NET GNSS stations in 2022**

| The date of 2022 | GNSS stations in total | The number of hours of observations in the daily RINEX file | | | |
|---|---|---|---|---|---|
| | | 18-24 | 12-18 | 6-12 | 0-6 |
| 01.01 | 210 | 209 | - | - | 1 |
| 10.01 | 210 | 201 | 7 | 1 | 1 |
| 20.01 | 226 | 225 | 1 | - | - |
| 01.02 | 227 | 223 | 4 | - | - |
| 10.02 | 232 | 232 | - | - | - |
| 20.02 | 231 | 230 | - | 1 | - |
| 01.03 | 188 | 181 | 4 | 3 | - |
| 10.03 | 178 | 171 | 2 | 2 | 3 |
| 20.03 | 169 | 167 | 1 | 1 | - |
| 01.04 | 173 | 172 | - | 1 | - |
| 10.04 | 172 | 170 | 2 | - | - |
| 20.04 | 169 | 165 | 3 | 1 | - |
| 01.05 | 178 | 176 | 1 | - | 1 |
| 10.05 | 183 | 180 | 1 | 1 | 1 |
| 20.05 | 186 | 181 | 3 | 1 | 1 |
| 01.06 | 185 | 182 | 1 | 1 | 1 |
| 10.06 | 184 | 173 | 10 | - | 1 |
| 20.06 | 184 | 181 | 3 | - | - |
| 01.07 | 180 | 175 | 3 | 1 | 1 |
| 10.07 | 183 | 180 | 2 | - | 1 |
| 20.07 | 188 | 182 | 4 | 2 | - |
| 01.08 | 185 | 182 | 2 | - | 1 |
| 10.08 | 184 | 177 | 4 | 3 | - |
| 20.08 | 184 | 180 | 3 | 1 | - |
| 01.09 | 180 | 166 | 7 | 5 | 2 |
| 10.09 | 180 | 175 | 2 | - | 3 |
| 20.09 | 177 | 157 | 1 | 17 | 2 |
| 01.10 | 168 | 149 | 2 | 2 | 15 |
| 10.10 | 160 | 141 | 3 | 7 | 9 |
| 20.10 | 163 | 153 | 1 | 3 | 6 |
| 01.11 | 159 | 141 | 9 | 7 | 2 |
| 10.11 | 159 | 141 | 10 | 7 | 1 |
| 20.11 | 165 | 150 | 10 | 1 | 4 |
| 01.12 | 163 | 137 | 14 | 7 | 5 |
| 10.12 | 154 | 145 | 5 | 2 | 2 |
| 20.12 | 155 | 140 | 6 | 3 | 6 |
| 31.12 | 148 | 144 | 1 | 2 | 1 |

To illustrate the table, below is a graph of data integrity GNSS stations of GeoTerrace and System.NET networks in 2022 every for every 10 days of the year (Fig. 2).

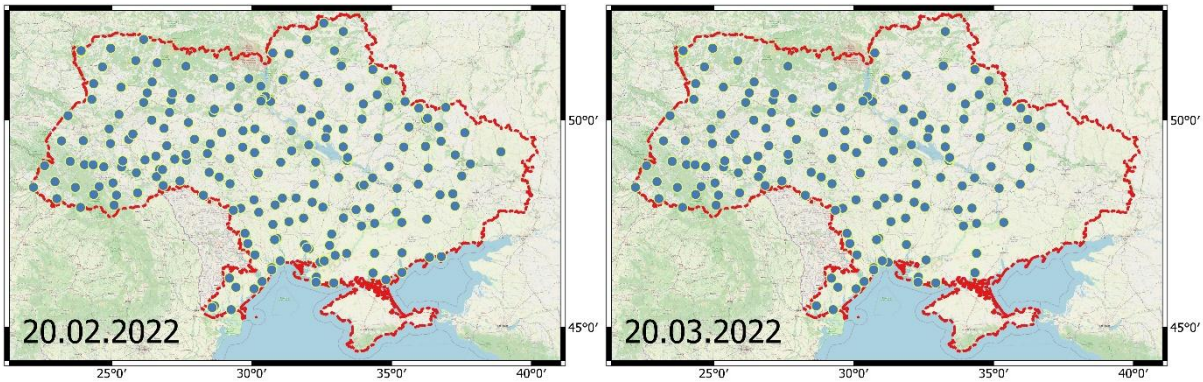


*Fig. 3. Location of active GNSS stations of GeoTerrace and System.NET CORS networks as of February 20 and March 20, 2022*

Taking into account the table and histogram, it can be observed that starting from March 2022, the number of GNSS stations in the network sharply decreased by approximately 10% of the total count. Meanwhile, the GNSS stations operated steadily.Almost all daily RINEX files until September 2022 contained between 18 to 24 hours of observations, except for July 10, when 10 stations recorded from 12to 18 hours of observations. Starting from September, the number of daily RINEX files containing less than 18 hours of observations increased. For instance, on September 20, 17 files contained 6 to 12 hours of observations, and on October 1, 15 files contained less than 6 hours of observations. This is associated with the widespread Russian missile strikes on Ukraine's energy infrastructure, resulting in power outages for the civilians and GNSS stations. Despite the majority of GNSS stations being equipped with backup power from a battery, which can ensure continuous station operation for up to 2 days, the constant lack of electricity prevented the batteries from recharging. Every tenth day of 2022 was examined to obtain a comprehensive overview of the network's performance, but it is evident that on certain days, the situation regarding the number of daily RINEX files could have been worse.

To review the territorial changes in GNSS stations before and after the invasion, below are the figures depicting the distribution of GNSS stations on February 20, 2022, when the highest number of stations was recorded, and on March 20, 2022, when the number sharply decreased and was at its minimum in March. In the figures, there were 231 stations in GeoTerrace and System.NET CORS networks as of February 20, and on March 20, there were 169 stations.

From the above-mentioned figures, it is evident that the number of stations that were operational after the full-scale advance on February 24, 2022, sharply decreased in the eastern, southern, and partially northern regions of Ukraine.

## Challenges for GNSS CORS network operations and factors caused by the hostilities

The accuracy and reliability of the CORS network have been significantly impacted by several new factors related to the hostilities. A significant increase in data processing errors was observed throughout 2022. These errors arose due to massive missile attacks across Ukraine, power outages, large-scale blackouts, and data losses, making it impossible to compute sufficiently accurate solutions. Notably, the CORS network's stability was greatly affected by the repeated and prolonged use of electromagnetic jamming and other electromagnetic warfare technologies. As a result, under the influence of deliberate obstacles, there was an increase in errors in daily RINEX file calculations. Additionally, during electromagnetic jamming and GPS spoofing, network users frequently experienced incorrect operation in RTK or VRS modes.

Electromagnetic jamming is the process of suppressing or blocking radio signals. The primary physical principle of jamming is based on the properties of radio waves and their interaction with objects. Jamming could be executed using electromagnetic devices that send interference or create disrup-

tions that mask or distort signals [Skolnik, 1980]. It can be used to hinder the proper functioning of GNSS receivers, creating false location measurements or blocking navigation system signals.

The term "GNSS spoofing" or "GPS spoofing" refers to the practice of manipulating global positioning system data, leading the navigation signal receiver to be misled about its actual location [Psiaki and Humphreys, 2016]. Spoofed signals imitate genuine ones, causing the receiver to perceive them as authentic. Consequently, the GNSS receiver processes these fake signals, resulting in distorted location data [Goward and Dana, 2017]. Spoofing works by using electromagnetic that suppresses the satellite system signal and replaces it with a distorted one. Spoofing attacks exploit GNSS infrastructure vulnerabilities, especially the weak signal strength from satellites. Faked signals transmitted from a short distance are perceived as genuine by the receiver due to their higher power compared to satellite signals. By implementing cryptographic methods in the GPS signal transmission process, receivers can verify the authenticity of incoming signals [Lundberg and Michael 2018; Meng et al., 2022]. This additional security layer helps prevent the acceptance of fake signals, enhancing overall GNSS system resilience. Receiving signals from multiple satellite systems complicates consistent signal manipulation for spoofing.

Different countries invest in making systems resilient to spoofing attacks by embedding security directly into their GNSS satellites. The Galileo constellation, for instance, with Open Service Navigation Message Authentication (OS-NMA), is the first satellite navigation system to introduce anti-spoofing directly into the civilian signal. OS-NMA is a free service on the E1 frequency that authenticates navigation data on Galileo and GPS satellites. GPS is also experimenting with satellite-based anti-spoofing for civilian users through its recent Chimera authentication system.

*Examples of Incorrect GNSS Measurements*

Below are examples provided by System.NET network users, particularly during real-time kinematic (RTK) GNSS measurements. These specific cases confirm that signal issues, previously unheard of in these areas, have sometimes arisen since February 2022. These reports came from various users with different GNSS equipment, but we intentionally do not specify this.

1. Coordinate Shift by Hundreds of Meters: During the office processing stage of a topographic survey in Vysnieve, Kyiv region, it was discovered that there was a coordinate shift of approximately 400 meters from the field survey location.Detailed examination confirmed that this error was not due to coordinate transformation into the SK-63 flat rectangular coordinate system. These raw data shifts were recorded in the global geodetic coordinate system WGS-84. Likely, this error was caused by jamming in the observation area.

2. Geodetic Work in Bucha, Kyiv Region: During static GNSS observations at five state geodetic network (SGN) points, two points (Bucha and Dmitrivka) showed precision issues compared to sessions from previous years. The remaining three SGN points and three other base points were used for the geodetic survey. Excluding the SGN points of Bucha and Dmitrivka, which showed unsatisfactory data precision, resulted in overall unsatisfactory accuracy for the base points included in the tachymetric surveying. All GNSS observation points had adequate satellite visibility, suggesting the GNSS satellite signal was distorted around the DGM points of Bucha and Dmitrivka.

These incidents illustrate that data obtained through GNSS observations in RTK and VRS modes in Ukraine are vulnerable to jamming. Such data are of low quality and reliability, making them unsuitable for high-precision work and scientific observations. It is crucial to note that the likelihood of technical failures and unreliable data due to jamming and radio direction-finding methods increases significantly in frontline cities, the capital, and regions with high missile strike threats and drone attacks. Special attention should be given to GNSS spoofing since it can affect many receivers in the attack zone. Spoofing attacks are dangerous as all stations consider the signal legitimate, complicating error source detection.

*Practical Recommendations for GNSS Measurements*

Due to active hostilities in Ukraine, technical failures and various errors can occur at any stage of obtaining and processing GNSS observation data. Here are practical recommendations for performing

GNSS measurements that can help explain error sources to surveyors in the field:

1. In RTK mode, gradual accuracy improvement may stop within decimeter limits, and each subsequent measurement may have unique accuracy despite identical connection conditions. Possible causes include a large distance to the base station, insufficient satellites, poor visibility, and the presence of artificial signal jamming. The L1 band (around 1575.42 MHz) typically has the highest frequency under normal conditions, so a drop to lower levels might indicate jamming since L1 is the most vulnerable to jamming.

Practically, checking the instrument's stability within two kilometers of the interference point can confirm jamming. At this distance, GNSS conditions remain similar, but simple jamming systems usually have a radius of about 2 kilometers, revealing correct satellite signals outside this range.

2. Internet access is crucial for obtaining RTK corrections for successful real-time GNSS receiver operation. It's recommended to update access points to check network availability. If accuracy improves or deteriorates sharply and the delay increases to 10 seconds, the issue might be attributed to the mobile operator. Manual switching to a lower-generation mobile network (e.g., from 4G to 3G) can enhance internet connection stability.

3. In GNSS measurements, a fixed solution status indicates the receiver has resolved ambiguity and determined its location based on satellite signals and internet corrections. Unique offsets in each new fixed solution suggest spoofing. The most effective practical method against spoofing attacks is to take control measurements of the same points a few hours apart. Recent research on signal spoofing reduction using dual-polarized antennas has also shown promise [De Wilde et al. 2018; Meng et al. 2022]. This research uses the polarization similarity of fake satellites for identification. The system records signals using a high-performance dual-polarized antenna optimized for low axial ratio, connected to a multi-frequency, multi-constellation receiver supporting coherent tracking of signal components. Testing conducted in an anechoic chamber simulating satellite signal polarization and field conditions was effective in combating spoofing attacks. For unmanned aerial vehicles, disabling the GNSS module during takeoff or when crossing areas likely under spoofing systems' influence, and using a filter between the GNSS signal receiver and flight controller, can help. The satellite signal first passes through the filter and then goes to the flight controller via a separate physical interface.

To sum up the specifics of GNSS measurements after February 2022, such measurements should be approached more carefully, as illustrated by the examples of incorrect GNSS observations, and field measurements should be additionally controlled, for example, RTK measurements should be closed to the starting point. The practical recommendations are not exhaustive but are based on user feedback and have proven effective, enhancing measurement reliability.

## Conclusions

The study provides a detailed description of the current state of GNSS networks, including a literature review and the latest publicly available statistical information on permanent GNSS stations in Ukraine. Given the constant growth in the number of GNSS CORSs and taking into account the available statistics, the authors estimate the total number of permanent GNSS stations in Ukraine more than 450 units before the start of russia's full-scale invasion in February 2022.

To analyze the changes in the number of properly operating GNSS CORS networks in Ukraine, this study selected two networks: GeoTerrace and System.NET. Geographically, these networks complement each other and cover all regions of Ukraine except for the territories temporarily occupied by russia. A three-year observation period from 2021 to 2023 was taken into account. As of early 2021, the network consisted of 240 stations, and in early 2022, the network included 285 stations. After the start of the full-scale invasion, by the summer of 2022, there was a sharp decrease in the number of GNSS stations by about 10% of the total. In the autumn of 2022, the volume of daily RINEX files of GNSS measurements at CORS decreased due to constant power outages in Ukraine. The completed assessment of GNSS stations can be used for geodynamic studies of the region in the future.

The time series of GNSS stations were processed using the Bernese GNSS v.5.2 software package using the double difference method. There are noticeable errors in results for some GNSS stations

due to insufficient data and new factors that appeared after February 2022. For example, due to the impact of radio-electronic jamming during the hostilities, there was an increase in measurement errors. During the radio-electronic jamming and the use of GPS spoofing, there were frequent and noticeable cases of incorrect operation by network users in RTK or VRS modes. The article provides examples of such instances and indicates the most likely reason for their occurrence, according to the authors. Based on the authors' experience and requests from GNSS CORS network users, the article provides features of GNSS signal interference detection for civilian users and practical recommendations regarding controlling GNSS observations in modern conditions after February 2022. These recommendations are not exhaustive but are of practical value.

After analyzing the study results and considering the operation and data processing features of GNSS CORS networks in Ukraine, it is crucial to conduct a detailed analysis of such data in the future. This is especially important as new military factors have emerged, which are impacting their operation.The recommendations given in this article are practical for users in RTK or VRS modes of active GNSS networks, and the results of processing of permanent GNSS stations can be used for future geodynamic or other studies of the territory of Ukraine.

## References


Dach, R., Lutz, S., Walser, P., & Fridez, P. (2015). Bernese GNSS software version 5.2. https://doi.org/10.7892/boris.72297

De Wilde, W., Sleewaegen, J. M., Bougard, B., Cuypers, G., Popugaev, A., Landmann, M., ... & Granados, G. S. (2018, September). Authentication by polarization: A powerful anti-spoofing method. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018) (pp. 3643-3658) URL: http://spcomnav.uab.es/docs/conferences/FANTASTIC_GNSS18-0248.pdf

EUREF Permanent GNSS Network. URL: https://epncb.oma.be/ (дата звернення: 01.03.2024).

Goward, Dana A. (July 11, 2017). "Mass GPS Spoofing Attack in Black Sea?". The Maritime Executive. An apparent mass and blatant, GPS spoofing attack involving over 20 vessels in the Black Sea last month has navigation experts and maritime executives scratching their heads. URL; https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

International GNSS Service. URL: https://igs.org/network-resources (дата звернення: 01.03.2024).

Ishchenko M.V (2009). Review of permanent GNSS-stations networks. Astronomical School's Report. 6 (9), 114-117. URL: http://astro.nau.edu.ua/papers/AstSR_2009_Vol_6_Iss_1_P_114.pdf (In Ukrainian).

Khoda, O. (2024). Propagation of the IGb14 Reference Frame on the Territory of Ukraine Based on Results of the Analysis of GNSS Observations for GPS Weeks 2106–2237. Kinematics and Physics of Celestial Bodies, 40(1), 47-53. https://doi.org/10.3103/S0884591324010057

Khoda, O., & Ishchenko, M. (2021). Rapid daily processing of observation data at the Ukrainian permanent GNSS stations for monitoring of their stability. In International Conference of Young Professionals «GeoTerrace-2021» (Vol. 2021, No. 1, pp. 1-5). European Association of Geoscientists & Engineers. https://doi.org/10.3997/2214-4609.20215K3014

Lundberg, E., & Michael, I. (2018). Novel Timing Antennas for Improved GNSS Resilience. *In Proceedings of the 49th Annual Precise Time and Time Interval Systems and Applications Meeting* 45-58. https://doi.org/10.33012/2018.15625

Meng L, Yang L, Yang W, Zhang L. (2022) A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing*. 14(19):4826. https://doi.org/10.3390/rs14194826

Novikova, O., Palamar, A., & Petkov, S. (2020, April). Operator service of GNSS networks of Ukraine. In The 12 th International scientific and practical conference «Impact of modernity on science and practice», Edmonton, Canada. URL: https://isg-konf.com/wp-content/uploads/2020/04/XII-Conference-13-14-Edmonton-Canada.pdf (In Ukrainian)

Poisel, R. (2011). *Modern communications jamming principles and techniques*. Artech house. URL: https://dl.acm.org/doi/abs/10.5555/2024614

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, *104*(6), 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658.

Savchuk S. Practical aspects of the application of the new USK2000 reference system. International scientific and practical conference GEOFORUM-2012. – Lviv-Yavoriv, Ukraine. URL: http://zgt.com.ua (In Ukrainian)

Skolnik, M. I. (1980). *Introduction to radar systems* (Vol. 3, pp. 81-92). New York: McGraw-hill. URL: https://soaneemrana.org/onewebmedia/INTRODUCA

TION%20TO%20RADAR%20SYSTEM%20BY%20MERRIL,%20I%20SKLOINK%20(4).pdf

Tretyak K., & Brusak I. (2022) Modern deformations of Earth crust of territory of Western Ukraine based on «GEOTERRACE» GNSS network data. *Geodynamics,* 32(1), 16-25. https://doi.org/10.23939/jgd2022.02.016

Tretyak, K., Korliatovych, T., Brusak, I., (2021). Applying the statistical method of GNSS time series analysis for the detection of vertical displacements of Dnister HPP-1 dam. *In International Conference of Young Professionals «GeoTerrace-2021». European Association of Geoscientists & Engineers*. DOI: 10.3997/2214-4609.20215K3012

Tretyak, K., Zayats, O., Hlotov V., Navodych M., & Brusak, I. (2022). Establishment of the automated system of geodetic monitoring for structures of Tereble-Ritska HPP. Geodesy, Cartography, and Aerial Photography, 95(1), 13-21. https://doi.org/10.23939/istcgcap2021.93.027

Ukrainian GNSS network (n.d.) Main Astronomical Observatory of the National Academy of Sciences of Ukraine. Retrieved 01.03.2024, from: http://gnss.mao.kiev.ua/?q=node/1

[1,2,3,4,5,6,7] Іван БРУСАК 1, Володимир БАБЧЕНКО 2, Наталія САВЧУК 3, Владислав МАРЧУК4, Юрій ШКВАРОК5, Михайло ТУРЯНИЦЯ6

[1,2,3,4,5,6,7] Інститут геодезії, Національний університет «Львівська політехніка», вул. Степана Бандери 12, Львів, 79013, Україна, e-mail: 1ivan.v.brusak@lpnu.ua, https://orcid.org/0000-0001-5434-4931, 2volodymyr.a.babchenko@lpnu.ua, 3nataliia.savchuk.hd.2021@lpnu.ua, https://orcid.org/0009-0005-3396-7706, 4vladyslav.marchuk.hd.2022@lpnu.ua, https://orcid.org/0009-0004-8411-9806, 5yurii.i.shkvarok@lpnu.ua https://orcid.org/0009-0001-8614-179X, 6mykhailo.m.turianytsia@lpnu.ua, https://orcid.org/0009-0000-5433-2834

## НОВІ ВИКЛИКИ ДЛЯ ФУНКЦІОНУВАННЯ АКТИВНИХ ПЕРМАНЕНТНИХ ГНСС-СТАНЦІЙ ПІД ЧАС БОЙОВИХ ДІЙ НА ПРИКЛАДІ УКРАЇНИ

У дослідженні наведено сучасний стан активних перманентних ГНСС-станцій та особливості їх роботи під час бойових дій на території України. Стабільна робота ГНСС-мереж на сьогодні є важливою не лише для робіт у сільському господарстві, геодезичних та землевпорядних роботах, а й для уточнення навігації чи топографії для військових цілей. Метою цієї роботи є аналіз впливу бойових дій на ГНСС-мережу України, враховуючи фактори тимчасової окупації окремих територій, перебої електроживлення через ракетні удари по енергетичній інфраструктурі та подавлення ГНСС-сигналу радіоелектронними методами в прифронтових регіонах. Інше завданням цього дослідження – висвітлити приклади некоректної роботи в RTK чи VRS режимі, враховуючи можливі помилки від радіоелектронного подавлення чи GPS-спуфінгу та надати практичні рекомендації для спостерігачів. У результаті роботи проведено аналіз змін кількості належно працюючих ГНСС-станцій за період з 2021 року до 2023 року на прикладі двох мереж GeoTerrace та System.NET, які разом досить повно охоплюють всі регіони України, окрім тимчасово окупованих росією територій. Виконано опрацювання добових 30-секундних RINEX-файлів перманентних ГНСС-станцій у програмному пакеті Bernese GNSS v.5.2 за три роки. Зафіксовано, що після початку повномасштабного вторгнення у лютому 2022 року та до весни цього ж року відбулося різке скорочення кількості належно працюючих активних ГНСС-станцій на близько 10 % від загальної кількості. Наукова новизна та практичне значення. У статті надано практичні рекомендації для користувачів – геодезистів та землевпорядників, які виконують ГНСС-виміри у RTK чи VRS режимах від перманентних станцій з метою оцінки спостережень на вплив радіоелектронного подавлення чи GPS-спуфінгу. Виконана оцінка мережі та щоденно обчислені координати ГНСС-станцій за період з 2021 року до 2023 року можуть бути використані для геодинамічних досліджень регіону у майбутньому.

*Ключові слова:* Активні перманентні ГНСС-станції, ГНСС-мережі, Україна, опрацювання ГНСС-даних, ГНСС-мережа GeoTerrace, ГНСС-мережа System.NET, радіоелектронне подавлення ГНСС-сигналу, ГНСС-спуфінг.

Received 09.05.2024