https://doi.org/10.70265/JZPI2152

CYBER RESILIENCE OF GEODETIC SYSTEMS AS AN ELEMENT OF DIGITAL INFRASTRUCTURE

Ani Stefanova

Summary: *The digital transformation of geodesy integrates GNSS, cloud services, UAVs, and IoT within an interconnected infrastructure. While improving efficiency, this technological dependency increases exposure to cyber risks, including GNSS interference, cloud vulnerabilities, and compromise of geospatial data. The paper presents a systematic analysis of key risk profiles and proposes technological and organizational mechanisms to enhance the cyber resilience of geodetic systems.*

Keywords: *cyber resilience, cybersecurity, critical infrastructure, geodetic systems, GNSS*

INTRODUCTION

The digital transformation of geodesy over the past decade has led to the integration of Global Navigation Satellite Systems (GNSS), cloud-based data processing platforms, unmanned aerial vehicles (UAVs), intelligent sensor networks, and automated workflows. Contemporary geodetic activities are carried out within an interconnected digital environment characterized by real-time data exchange, remote access, and centralized processing.

Within the context of the modern security and defence environment, geodetic and GNSS infrastructures should be considered components of critical national digital infrastructure, whose reliable operation is directly related to crisis management, defence capabilities, including military navigation, situational awareness, and operational planning, as well as societal resilience.

Under these conditions, technological integration enhances the efficiency and analytical capabilities of geodetic practice while simultaneously increasing dependence on communication, software, and information infrastructures. As a result, modern geodetic activities function as cyber-physical systems in which GNSS interference, vulnerabilities in cloud services, and unauthorized access to geospatial data become significant risk factors.

Such a transformation of geodesy is also addressed within the concept of *Responsible Geodesy*, which integrates technological development,

ethical principles, and sustainable models for the digital geospatial environment (Stefanova, 2025).

The concept of *cyber resilience* refers to the ability of systems to prevent, detect, withstand, and recover from disruptions affecting their operation. In the context of geodetic practice, this implies the integration of technological and organizational mechanisms ensuring process continuity and operational reliability under conditions of increased technological dependence.

This paper presents a systematic analysis of the main risk profiles affecting contemporary geodetic systems and proposes mechanisms for enhancing their cyber resilience.

In the context of ongoing national digital infrastructure development, including positioning services, spatial data infrastructures, and crisis management systems, cyber resilience of geodetic systems becomes increasingly relevant for countries developing integrated security and defence architectures.

The scientific contribution of the study lies in the systematization of cyber risks associated with geodetic systems and in the development of a conceptual multilayer cyber-resilience model through which geodetic systems are interpreted as elements of modern digital infrastructure. The proposed multilayer model represents the primary scientific contribution of this research and provides a conceptual framework for integrating cyber-resilience principles into the development of Geodesy 4.0.

The objective of this study is to analyse cyber risks affecting contemporary geodetic systems and to develop a conceptual multilayer model for enhancing cyber resilience. The research object is the digital geodetic infrastructure, while the research subject focuses on cyber resilience mechanisms within integrated geodetic systems.

The study applies a systemic analytical approach combining architectural analysis, risk classification, and conceptual modelling. The central thesis of this study is that geodetic systems should be interpreted as components of critical digital infrastructure whose cyber resilience directly influences national security, crisis response capability, and infrastructure stability.

1. ARCHITECTURE OF GEODETIC SYSTEMS WITHIN DIGITAL INFRASTRUCTURE

From a cyber-resilience perspective, geodetic infrastructure can be interpreted as a multi-layered system in which different technological layers participate in the acquisition, transmission, processing, and management of spatial information. Consequently, geodetic systems may be considered an integrated cyber-physical architecture operating through the interaction of measurement, communication, and information components.

1.1. Measurement layer

The measurement layer includes GNSS receivers, total stations, unmanned aerial vehicles (UAVs), and various sensing devices through which primary spatial observations are generated. This layer represents the interface between physical reality and digital infrastructure. Cyber risks at this level are primarily associated with navigation signal interference and spoofing, manipulation of measurement data streams, or device compromise, which may directly affect the reliability of coordinate solutions.

1.2. Communication layer

The communication layer ensures data exchange between measurement devices, continuously operating reference station networks (CORS), central servers, and user applications through internet connections, mobile communication networks, and specialized protocols for transmitting GNSS corrections and geospatial information. The reliability and security of this layer are critical for maintaining positioning service continuity, data synchronization, and the resilience of real-time operational workflows.

1.3. Processing layer

The processing layer encompasses cloud platforms, computational servers, and software environments for the processing, analysis, and modelling of spatial data. Centralized processing enables high computational performance and automation of geodetic workflows; however, it simultaneously introduces dependencies related to information security, access management, and the robustness of the underlying digital infrastructure. Vulnerabilities at this stage may lead to service unavailability or compromise of processed information.

1.4. Information layer

The information layer includes geospatial databases, GIS platforms, cadastral registers, and spatial information management systems in which the results of geodetic processes are stored and utilized. This layer plays a critical role in subsequent engineering, administrative, and decision-making activities. The primary risks are related to data integrity violations, unauthorized modifications, and insufficient traceability of performed operations, which necessitate the implementation of version control, auditing procedures, and spatial data quality management mechanisms.

Consequently, cyber resilience should be understood as an integral property of the entire geodetic infrastructure, requiring a systemic analysis of the principal risk profiles affecting contemporary geodetic systems.

2. MAJOR CYBER RISKS IN CONTEMPORARY GEODETIC SYSTEMS

The integration of geodetic processes into an interconnected information architecture expands the surface of potential cyber risks. According to the annual ENISA threat landscape report, interconnected

infrastructure systems are exposed to diverse and evolving threats that require systematic risk assessment approaches (European Union Agency for Cybersecurity [ENISA], 2023). From this perspective, risks affecting geodetic systems primarily arise from their dependence on navigation services, communication infrastructure, and software platforms.

2.1. GNSS interference and spoofing

GNSS positioning constitutes a fundamental component of a significant portion of field surveying activities and continuously operating reference station (CORS) networks. Scientific literature and analyses of CORS infrastructures identify two principal forms of impact on civilian GNSS signals—jamming and spoofing (Humphreys, 2013; Psiaki & Humphreys, 2016), as well as their communication-related implications within CORS environments (Bakici et al., 2018; Xu et al., 2023).

Jamming represents electromagnetic interference that degrades or temporarily disrupts satellite signal reception. Such disturbances may lead to loss of fixed positioning solutions, increased positional uncertainty, or interruption of operational workflows.

Spoofing involves the transmission of manipulated navigation signals intended to influence positioning results. In the absence of verification mechanisms, such attacks may introduce coordinate deviations without immediate detection of anomalies. Cryptographic authentication approaches and secure data exchange mechanisms between stations and control centres have been proposed to enhance the security of GNSS data and services (Xu et al., 2023).

These phenomena are inherently linked to the open-access nature of civilian GNSS services and are therefore considered technological risks requiring additional validation and monitoring mechanisms.

2.2. Cloud processing and access control

The use of cloud platforms for storing and processing geospatial data provides scalability and optimization of geodetic workflows. At the same time, it introduces increased requirements for access management, change traceability, and data integrity protection.

Potential risk scenarios include:

- unauthorized access to project files and databases;
- unauthorized modification of spatial data layers;
- temporary service unavailability caused by infrastructure failures.

Due to the centralized nature of cloud processing, incidents may affect multiple users or projects simultaneously, which necessitates clearly defined policies for version management, data backup, and auditing procedures.

2.3. Integrity and traceability of geospatial databases

Cadastral and GIS databases constitute a structured informational foundation for engineering, administrative, and spatial planning activities.

Violations of data integrity may arise as a result of software errors, improper synchronization between systems, or unauthorized modifications.

Even minor alterations in coordinate or attribute data may generate inconsistencies in subsequent analyses and design processes. The assessment of spatial data quality and integrity should therefore rely on established international data quality standards and methodologies (International Organization for Standardization, 2013). Consequently, mechanisms for change tracking, version control, and activity logging represent essential components of risk management within geospatial information systems.

2.4. UAV and IoT solutions

Unmanned aerial systems and spatially distributed sensor networks operate through the integration of GNSS positioning, wireless communication, and remote control technologies (Zhang & Zhu, 2023). This technological combination makes such systems dependent both on navigation services and on the security of communication channels.

Potential risks include:

- disruption of control signals;
- interception or manipulation of telemetry data;
- unauthorized access to stored measurements.

As the number of interconnected devices continues to grow, the need for standardized mechanisms for encryption, authentication, and access control becomes increasingly critical.

The main components of geodetic systems, the associated cyber risks, and the corresponding mitigation approaches are summarized in Table 1.

Table 1. Key cyber risks within the architecture of geodetic systems and corresponding cyber resilience enhancement approaches

System Component	Primary Risk	Potential Impact	Mitigation Mechanisms
GNSS services and CORS networks	GNSS jamming and spoofing	Inaccurate coordinate solutions, interruption of operational workflows	Multi-sensor integration (GNSS+INS), signal verification, cryptographic protection
Communication infrastructure	Signal interception or disruption	Data loss, processing delays or service interruption	Encrypted communication channels, device authentication, traffic monitoring

Cloud processing and servers	Unauthorized access, service compromise	Reduced data availability and confidentiality	Access control, auditing, implementation of information security frameworks (e.g., ISO/IEC 27001)
Geospatial databases	Integrity violation, unauthorized modifications	Incorrect engineering decisions, model inconsistencies	Version control, activity logging, data quality management methodologies (ISO 19157)
UAV and IoT devices	Control signal disruption, telemetry manipulation	Loss of control, unreliable measurements	Encryption, authentication, secure communication protocols

3. MECHANISMS FOR ENHANCING CYBER RESILIENCE

The analysis of the identified cyber risks demonstrates that effective cyber resilience of geodetic systems can be achieved through the integration of technological, organizational, and professional mechanisms aimed at ensuring the integrity, availability, and traceability of geospatial information. Since vulnerabilities are distributed across the entire system architecture—from positioning services to cloud processing environments and geospatial databases—protective measures should be directed toward systematic information security management throughout the full architecture of geodetic systems. Such an approach establishes an integrated framework for managing cyber resilience within contemporary geodetic practice.

3.1. Technological mechanisms

Multisensor integration and verification

The integration of GNSS positioning with inertial navigation systems (INS), ground control points, and independent measurements enables the detection of anomalies and mitigation of navigation signal interference effects. Such an approach reduces dependence on a single positioning source and enhances the reliability of coordinate solutions.

Cryptographic protection and authentication

The use of encrypted communication channels, digital certificates, and user and device authentication mechanisms limits the risk of unauthorized access and data manipulation. Particular importance is assigned to securing telemetry data streams in UAV and IoT applications.

Version control and data backup

When working with geospatial databases and project files, maintaining version control, backup systems, and recovery mechanisms is essential. These measures ensure traceability of modifications and enable data restoration in cases of identified inconsistencies.

3.2. Organizational and procedural measures

Access management policies

The differentiation of user privileges and the application of the principle of least privilege reduce the risk of unauthorized modifications. Regular auditing of access rights and system activities supports early detection of irregularities.

Standardization and protocols

The implementation of structured information security management frameworks, including internationally recognized standards such as ISO/IEC 27001:2022 (International Organization for Standardization, 2022), contributes to systematic risk management, access control, and action traceability. Documented procedures for data processing and storage reduce the likelihood of human error and unauthorized alterations.

Business continuity

The development of contingency plans for service disruptions, including alternative positioning methods and options for local data processing, improves operational resilience and reduces dependence on single infrastructure components.

3.3. Professional competence

Cyber resilience cannot be achieved solely through technological solutions. An integrated approach combining technological, ethical, and organizational dimensions is discussed within the concept of responsible geodesy (Stefanova, 2025). The contemporary geodesist is therefore expected to possess fundamental knowledge of access management, data protection, and anomaly detection in measurement processes. Continuous professional development in the field of digital security supports the effective implementation of technical safeguards and reduces the risk of unauthorized actions or unintentional errors.

CONCLUSION

The analysis demonstrates that cyber resilience is becoming a system-forming factor for the reliability and sustainable operation of modern geodetic systems. The integration of GNSS services, cloud platforms, unmanned aerial systems, and intelligent sensor networks transforms geodesy into a complex cyber-physical infrastructure in which technological efficiency is directly linked to data security and the stability of the information environment.

The conducted analysis confirms that cyber threats affecting geodetic systems have a systemic nature and cannot be considered isolated

technological issues. Disruptions at the measurement, communication, processing, or information layer may influence the entire process of generating and utilizing spatial information.

The obtained findings highlight the necessity of an integrated approach to cyber resilience, combining technological solutions for protection and verification, organizational mechanisms for access management and data traceability, and the development of professional competencies related to digital security. In this context, the modern geodesist evolves from a mere operator of measurement technologies into an active participant in managing the security of spatial information.

From a strategic perspective, geodetic systems should be considered an element of critical digital infrastructure, whose reliable functioning is essential for engineering and governance processes. Consequently, cyber resilience emerges as a key factor determining the quality, reliability, and long-term sustainability of contemporary spatial information.

The proposed conceptual multilayer model of cyber resilience for geodetic systems may serve as a foundation for future research and for the development of integrated cyber resilience approaches within the framework of Geodesy 4.0.

In a broader strategic context, cyber resilience of geodetic systems emerges as a strategic enabler of national and infrastructure security. In the author's view, the growing dependence of crisis management, defence planning, and infrastructure governance on geodetic data transforms geodesy into a security-critical discipline rather than a purely engineering activity, positioning geodesy as an essential component of contemporary security architecture.

BIBLIOGRAPHY:

Bakici, S., Erkek, B., Manti, V., & Altekin, A. (2018). Challenges in data communication and cyber security of TUSAGA-Aktif (CORS-Tr). *Proceedings of the FIG Congress 2018*, Istanbul, Turkey, May 6–11.

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023.*

Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems, 49*(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400

International Organization for Standardization. (2013). *ISO 19157: Geographic information — Data quality.*

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems — Requirements.*

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

Stefanova, A. A. (2025). Responsible geodesy: Ethical and sustainable models for the digital transformation of geodesy. *Annals of Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, XV E*, 399–410. https://doi.org/10.46687/YT25AAS

Xu, C., Zhang, J., Zhang, Z., Hou, J., & Wen, X. (2023). Data and service security of GNSS sensors integrated with cryptographic module. *Micromachines, 14*(2), Article 454. https://doi.org/10.3390/mi14020454

Zhang, Z. & Zhu, L. (2023). A review on unmanned aerial vehicle remote sensing: platforms, sensors, data processing methods, and applications. *Drones, 7*(6), Article 398. https://doi.org/10.3390/drones7060398