GLL
Geomatics, Landmanagement and Landscape No. 4 • 2025, 31–38

ISSN 2300-1496 https://doi.org/10.15576/GLL/213751

Research paper

Received: 1.10.2025
Accepted: 29.10.2025
Published: 10.12.2025

Geospatial data as an opportunity and a risk for national security

Robert Szewczyk 0000-0003-0885-8610

Department of Agricultural Surveying, Cadastre and Photogrammetry,
University of Agriculture in Krakow
✉ Corresponding author: robert.szewczyk@urk.edu.pl

Summary

The development of an information society is one of the European Union's key objectives. In this context, geospatial data play a particularly important role, and are regulated by the INSPIRE directive and the Spatial Information Infrastructure Act in Poland. These data include, among others, the BDOT10k, GESUT, and orthophoto maps, which are widely available through geoportals and network services such as WMS and WFS. Up-to-date spatial information supports institutions, businesses, and citizens in planning and economic development. At the same time, the protection of critical infrastructure (CI) is becoming increasingly important. CI includes energy, telecommunication, financial, water, healthcare, transport, rescue, and administrative systems. Disruption in their functioning can lead to serious crises. Poland has implemented the National Critical Infrastructure Protection Program, which aims to ensure the security and continuity of these systems. This protection involves physical, technical, personnel, and teleinformation measures, with cyberattacks emerging as one of the most significant threats. The conclusions emphasise the need to balance open access to data with the protection of strategic information. In particular, access to data on high-capacity transmission networks should be restricted, while the physical and cyber protection of critical infrastructure must be strengthened. The current model of publishing geospatial data requires a thorough review and adjustment in the light contemporary threats.

Keywords

critical infrastructure • geospatial data • national security • geoportals • INSPIRE

1. Information society

The development of the information society is one of the European Union's key strategic objectives. In order to achieve a well-functioning knowledge-based economy, it

has become necessary to create conditions for the unrestricted flow of information [Goodchild 2007, Georgiadou et al. 2009]. Geospatial data, i.e. information relating to specific locations in space, has a special role to play in this process [Gaździcki 2011].

In order to unify the rules for collecting and sharing spatial data, the European Union adopted the INSPIRE (Infrastructure for Spatial Information in the European Community) Directive. This document obliged Member States to implement national regulations on the establishment and maintenance of spatial information infrastructure.

In Poland, these regulations are reflected in the Act on Spatial Information Infrastructure, which defines the rules for collecting, sharing and using spatial data.

The data covered by the regulations includes, among others:

- BDOT10k – a database of topographical objects, including the locations of transmission masts, roads and public utility facilities,
- GESUT – a geodetic database of utilities, containing information on the layout of water, gas and power networks, including the location of transformer stations and pumping stations,
- Orthophotomap – raster representation of the terrain surface created by processing aerial photographs.

A key element in the development of spatial information infrastructure was the creation of instruments for the widespread sharing of data. For this purpose, various types of geoportals were set up – that is, websites enabling the visualisation and downloading of spatial data.

The data is provided through specialised network services, such as:

- WMS (Web Map Service) – enabling the display of maps as raster images,
- WFS (Web Feature Service) – allowing vector data to be downloaded together with attributes.

Currently, geospatial data is commonly published by both state and local government institutions. For example:

- orthophotomaps and the BDOT10k database are made available by the Chief Surveyor of Poland,
- data concerning the local utilities network – via county servers.

As a result, every citizen, enterprise or institution may benefit from reliable and up-to-date spatial information, thus promoting economic development and spatial planning, and increasing the transparency of public administration activities.

2. Protection of critical infrastructure

The modern state, economy and society rely on the efficient functioning of complex systems, whose damage, destruction or disruption could have catastrophic consequences. These systems, strategic for the functioning of the country, are referred to as critical infrastructure (CI). Securing their safety and continuity of operation is the

overarching goal of the National Protection of Critical Infrastructure, which is one of the foundations of national security [Barć 2021].

National CI protection is an essential element in guaranteeing the stability and security of the state, its citizens and its economy. Without adequate protection, the state becomes vulnerable to a variety of threats – ranging from technical failures and natural disasters to deliberate acts of sabotage or terrorism [Leśnikowski 2025].

The main objectives of CI protection include:

- preventing disruptions to critical infrastructure,
- preparing for emergencies that could adversely affect critical infrastructure,
- responding to the destruction or disruption of critical infrastructure,
- restoring critical infrastructure.

The protection of CI is a fundamental responsibility of the state to its citizens. Unlike private companies, the state has resources and capabilities at its disposal, as well as a legal obligation to coordinate actions on a macro scale. Effective CI protection increases the state's resilience to crises, which in practice means a shorter return to normality and minimisation of losses.

In Poland, the Government Security Centre (RCB) is responsible for the preparation and implementation of the National Programme for Critical Infrastructure Protection (NPOIK). This programme, developed in cooperation with ministries and central authorities, aims to create conditions for improving CI security in terms of prevention, preparation, response and recovery.

National Programme for Critical Infrastructure Protection determines:

- criteria for identifying objects, installations, equipment and services that comprise IK systems,
- priorities, objectives and standards that serve to ensure the efficient functioning of the IK,
- bodies responsible for different infrastructure systems.

According to Polish law, critical infrastructure includes the following systems:

- power, including storage, energy and fuel supply,
- ITC networks,
- banking and finance,
- food and water supply,
- healthcare,
- transport,
- rescue,
- for securing the continuity of public administration.

Critical infrastructure protection is a complex process that requires a multidimensional approach, including:

- physical protection – securing buildings and facilities against unauthorised access,

- technical protection – the use of technology (e.g. alarm systems, monitoring) to secure facilities,
- personal protection – vetting of personnel and security procedures,
- ICT protection – prevention of cyber attacks, including access control and firewalling.

As technology plays an increasingly important role, cyberattacks are one of the biggest threats to critical infrastructure. Malware and hackers can paralyse key systems, leading to serious disruptions in the functioning of the state. The new generation of cybercriminals is becoming increasingly specialised, and the tools for carrying out attacks are becoming more readily available. ICT protection must constantly evolve to respond to fast-changing threats. It is not just about defending against existing attacks, but also about constantly seeking new, more secure solutions.

3. Geospatial data published online

Under the provisions of the Act on Spatial Information Infrastructure and the Act on Geodesy and Cartography, data concerning utilities networks are collected by county administration. These data are labelled in accordance with Polish regulations and stored in the GESUT database. In the case of power networks, data are grouped according to transmission parameters. Data on power grids are collected in the GESUT database and include a distribution based on transmission parameters:

- extra-high voltage (eHV) – lines above 400 kV, serving as the backbone of the national power system.
- high voltage (HV) – 110–400 kV transmission networks, connecting regions and supplying urban agglomerations,
- medium voltage (eS) – 1–110 kV networks, distributing energy to larger consumers and transformer stations,
- low voltage (eN) – local networks, usually up to 1 kV, used to supply households and small businesses,

As shown in Figure 1, these data are published on county geoportals and made available via the WMS web service to other geoportals, e.g. the national geoportal operated by the Main Office of Geodesy and Cartography (GUGiK), and its operation falls within the remit of the Chief Surveyor of Poland, who creates and maintains this spatial information infrastructure. The data is also made available to geospatial analysis software such as qgis via the wms service.

Similarly to the power industry, gas networks are classified according to the transmission parameter, i.e. operating pressure:

- high-pressure networks (gw) – strategic national and international pipelines, crucial for energy security,
- networks of increased pressure (gp) – gas transmission between regions and to large plants,

- medium pressure networks (gs) – serving larger clusters of industrial customers,
- low-pressure networks (gn) – used mainly for gas distribution in residential areas,

The data available on geoportals feature, among others, gas reduction stations, which are critical points in the system as they regulate transmission pressure and enable safe fuel distribution. For example, an image of a reduction station with an accompanying gas network is shown in Figure 2.

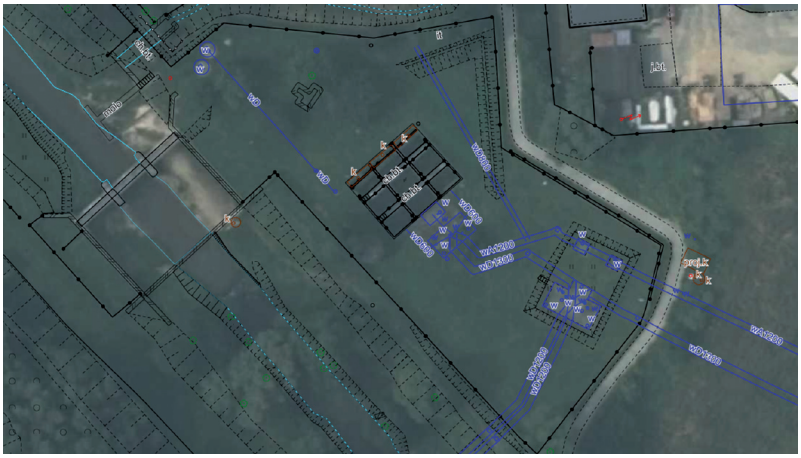
Source: geoportal.gov.pl

Fig. 1. Image of electricity transmission networks

Source: geoportal.gov.pl

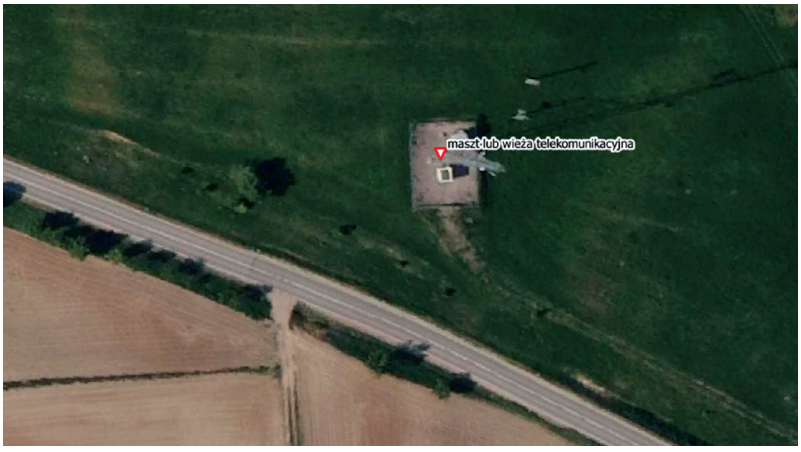
Fig. 2. Image of a gas reduction station with gas transmission network infrastructure

Another example are water supply networks. In their case, the key parameter is the diameter of the transmission pipe. These data, published in GESUT, allow for the identification of objects such as: water mains, water intakes, storage reservoirs, and pumping stations. Water intakes are particularly sensitive elements, as they are a strategic source of drinking water for towns and municipalities. Based on the diameter of the pipe, we can easily identify water intakes. An example of such an intake is provided in Figure 3.



Source: geoportal.gov.pl

Fig. 3. Water intake together with water supply infrastructure



Source: own study based on information from the BDOT 10k database

Fig. 4. Location of a telecommunications mast or tower

A further example of public access to critical infrastructure is the data made available through the WFS service. This service is used by the Head Office of Geodesy and Cartography to share data from the BDOT 10k database. Among the many details contained in this database, we can find information about telecommunications masts and towers.

As the examples above demonstrate, it is nowadays very easy to access data on high-capacity networks that can be classified as critical infrastructure. No specialist knowledge is required to identify these facilities, as the data can be presented on a map background including terrain details such as streets, pavements and house numbers, or on backgrounds based on aerial photographs (orthophotomaps).

4. Discussion and conclusions

The ideas guiding the INSPIRE Directive – openness and universal accessibility of data – now need to be re-examined in the context of security threats. Armed conflicts today, including the war in Ukraine, prove that transmission, electricity and gas infrastructures are among the main targets of attacks.

Experience from the conflict in Ukraine suggests that networks with high-transmission parameters are particularly vulnerable to attack. It should also be borne in mind that these facilities are not particularly well protected by the state and may therefore be easy targets for sabotage. Comparing the regulations on critical infrastructure protection and the above-mentioned examples of full transparency on the internet of key infrastructure facilities, such as water intakes, power and gas transmission lines, and telecommunications masts, and taking into account the current events in Ukraine, it should be concluded that:

- Data on high-parameter transmission networks (high-voltage lines, high-pressure gas pipelines) should have special protection.
- Pen access to information about strategic facilities, such as gas reduction stations or power plants, should be restricted.
- Transparency for citizens must go hand in hand with national security – some data should be public, but critical information should be subject to restrictions.
- Attacks on transmission infrastructure can cause social and economic chaos, so the state's priority should be to strengthen both physical and cyber security.

In summary, protecting information about critical infrastructure requires a balance between the principle of open access to data and the need to guarantee national security. Contemporary threats make it clear that the current model for publishing geospatial data should be revised.

References

Barć M. 2021. Rodzaje ochrony infrastruktury krytycznej. Rocznik Bezpieczeństwa. Akademia Marynarki Wojennej im. Bohaterów Westerplatte. https://doi.org/10.5604/01.3001.0015.0196

Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32007L0002

Gaździcki J. 2011. Infrastruktura informacji przestrzennej w Polsce. Główny Urząd Geodezji i Kartografii, Warszawa.

Georgiadou Y., Miscione G., Lance K. et al. 2009. Framing the use of geo-information in government: a tale of two perspectives. Earth Sci. Inform., 2, 271–282. https://doi.org/10.1007/s12145-009-0036-5

Główny Urząd Geodezji i Kartografii (GUGiK). https://www.geoportal.gov.pl

Goodchild M.F. 2007. Citizens as sensors: the world of volunteered geography. GeoJournal, 69(4), 211–221. https://doi.org/10.1007/s10708-007-9111-y

Leśnikowski W. Cyberatak na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania rozwiniętych państw. https://archiwum-cdissz.wp.mil.pl/plik/file/Publikacje/cyberataki-na-infrastruktur-krytyczn.pdf [accessed: 28.10.2025].

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. 2010 nr 83 poz. 541). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20100830541

Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 lipca 2021 r. w sprawie geodezyjnej ewidencji sieci uzbrojenia terenu (GESUT) (Dz.U. 2021 poz. 1374).

Rządowe Centrum Bezpieczeństwa. Narodowy Program Ochrony Infrastruktury Krytycznej. https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej

Ustawa z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne (Dz.U. z 2024 r. poz. 1151, 1824, z 2025 r. poz. 1019). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19890300163

Ustawa z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej (Dz.U. 2010 nr 76 poz. 489 z późn. zm.). https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20100760489