Quality implications of requirements to make the data both open and secure

Raitis Bolšakovs
Latvian Geospatial Information Agency
5th International Workshop on Spatial Data Quality

Introduction

- I’ve been working in GIS field for 12 years and the last 9 years have been mostly about the spatial data quality

- The idea to dive into this topic has been in my head for some time, as I’ve seen both good examples of opening the data and making it secure, and some bad examples, too

- There’s been constant demand from users to open more data as long as I’ve been involved in this field:
    - At the beginning the main issue was, who’s going to pay for the opening and maintaining the data
    - Lately the main concern has been the data security

Wider scope

- The conflicting needs of making the data both open and secure is not a unique topic

- In the last General Assembly of EuroGeographics in May 2025 in Riga there were two presentations dedicated to this topic, which illustrates the importance of this issue

- Both Hanna Cook, head of Norwegian Mapping Authority, and Jiri Pilar, Legal and Policy Officer at the European Commission, emphasized the needs and challenges of the data openness and the data security

Wider scope – Hanna Cook

- The data is the new gold – it holds the key to innovation, and it is the critical raw material for producing digital products and services

- The Open Data Directive that was established in 2019, since then much has changed:
    - Top risks by World Economic Forum (WEF) in 2019 were extreme weather events, climate change, natural disasters, data fraud, cyber-attacks, man-made environmental disasters and large-scale migration
    - In 2025 top risks by WEF are state based military conflicts, extreme weather events, geoeconomic confrontation, misinformation and disinformation, polarization and economic downturn

- As a result, the data sharing has become a balancing act on WHAT to share and what to protect, HOW to share effectively and safely, WHO can access the data and WHICH data sources to trust

- <u>Share what we can, protect what we must</u>

Wider scope – Jiri Pilar

- There's an obligation to share the data via the Open Data Directive, however, these rules only apply to the publicly accessible data and member states of the EU are the ones deciding what is public

- Rules of the data reuse don't cover third party intellectual property, personal data, national and public security, defense, statistical and commercial confidentiality, and information about critical infrastructure – security needs are more important

- Data can build EU competitiveness – from underutilization of the available data, except for legislation purposes, to driving AI development, as AI companies need more data

- However geopolitical tensions lead to uncertainty of the data flows

Obligation to make data accessible

- The Open Data Directive encourages the EU countries to make as much information available for reuse, as possible

- It addresses material held by public bodies in EU countries at all levels, including ministries, state agencies, municipalities and organizations funded or under control of public authorities

- Once adopted to national level, the Directive will stimulate the publishing of dynamic data and the uptake of Application Program Interfaces (APIs), and limit the exceptions which currently allow public bodies to charge more than the marginal costs of dissemination for the re-use of their data

Obligation to make data accessible

- The Open Data Directive introduces the concept of high-value datasets. The re-use of high-value datasets is associated with important benefits for the society and economy, ensuring their availability free of charge, in machine readable formats. They are provided via APIs and, where relevant, as a bulk download

- The thematic categories of high-value datasets are:
  - geospatial
  - earth observation and environment
  - meteorological
  - statistics
  - companies and company ownership
  - mobility

Obligation to make data accessible

- Data Governance Act – entered into force in June 2022, applicable since September 2023

- Aims to make more data available and facilitate sharing across sectors and EU countries:
    - ○ Has mechanisms to facilitate the reuse of certain public sector data, that can’t be made available as open data (like health data)
    - ○ Measures to ensure that data intermediaries function as trustworthy organizers of data sharing or pooling
    - ○ Measures to make citizens and businesses easier to share their data for the benefit of the society
    - ○ Measures to facilitate data sharing across borders and sectors

Obligation to make data accessible

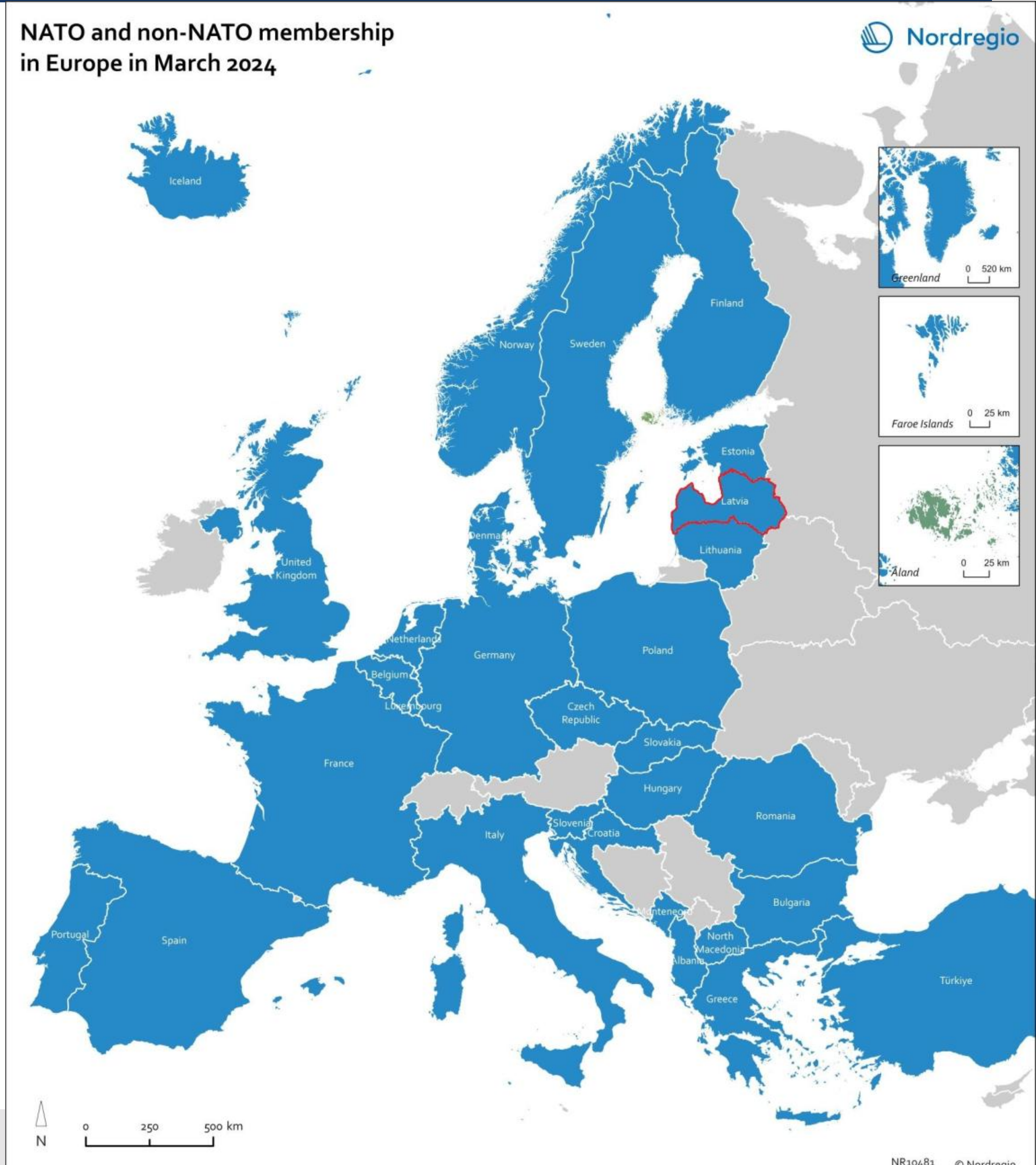
- In February 2024 a new Initiative introduced – GreenData4All

- Main aims of the Initiative:
  - Revise the INSPIRE Directive by modernizing its technological aspects and extend its scope to non-spatial, citizen science and business data
  - Align the legal framework with recent and emerging EU data legislation
  - Ensure coherence regarding data reuse schemes between the legislation on data sharing (Data Governance Act, Open Data Directive)

Local factors

- Latvia is part of the EU and NATO since 2004, and our Eastern border is the outer border of both these organizations

- Eastern and Southeastern neighbors of Latvia currently can’t be described as «friendly countries»

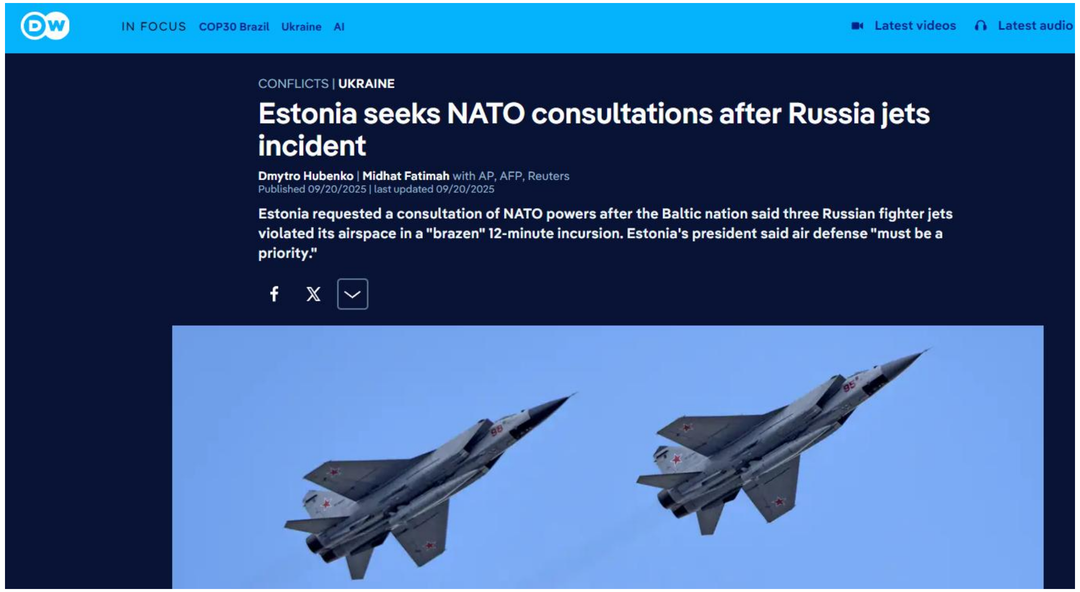

NATO and non-NATO membership in Europe in March 2024

Turning point

- Since 24th February 2022 there has been a shift in thinking about the accessibility of the spatial data in Latvia
- Previously the common goal was to open as much spatial data as possible as soon as possible and use this data for the good of the society under open data licenses
- Now, however, questions are being asked - who can access the data and what security risks does it pose
- The idea is still to pay for the capture and production of the data only once and then use the data for the good of the society
- Safeguarding the high value data from malicious use currently is a hot topic

Incidents

- Lately there have been numerous incidents, that both directly and indirectly affect the security of spatial data:
  - Incursions of military aviation into the airspace of Baltic nations that requires scrambling of NATO jets for interception
  - Website *www.defensenews.com* states that NATO jets have had to intercept foreign aircraft approaching NATO airspace without prior notice ~400 times in 2023 and 2024, with peak activity being in 2022, when there were ~570 such missions



CONFLICTS | UKRAINE

Estonia seeks NATO consultations after Russia jets incident

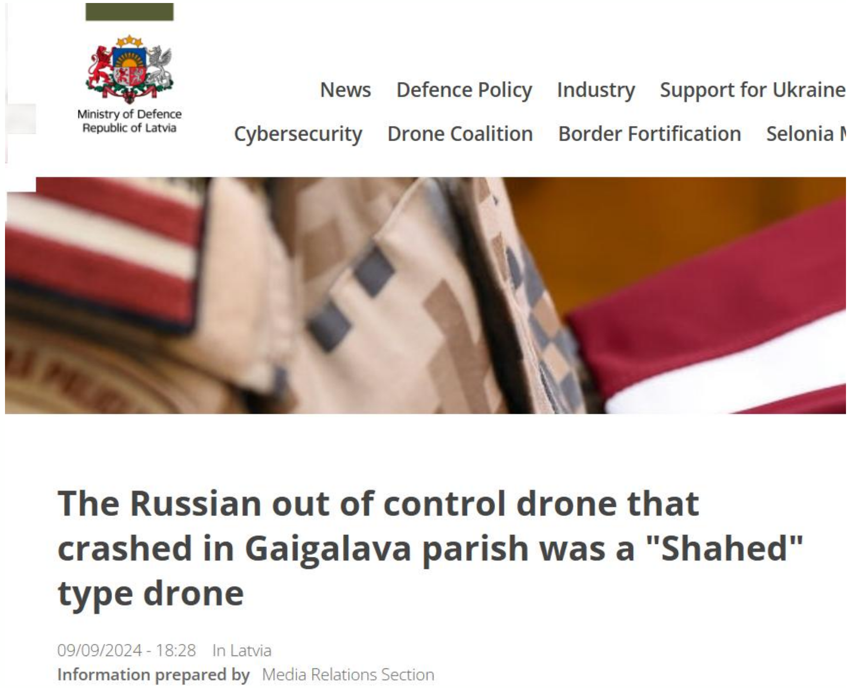
Dmytro Hubenko | Midhat Fatimah with AP, AFP, Reuters
Published 09/20/2025 | last updated 09/20/2025

Estonia requested a consultation of NATO powers after the Baltic nation said three Russian fighter jets violated its airspace in a "brazen" 12-minute incursion. Estonia's president said air defense "must be a priority."

Quality implications of requirements to make the data both open and secure

Incidents

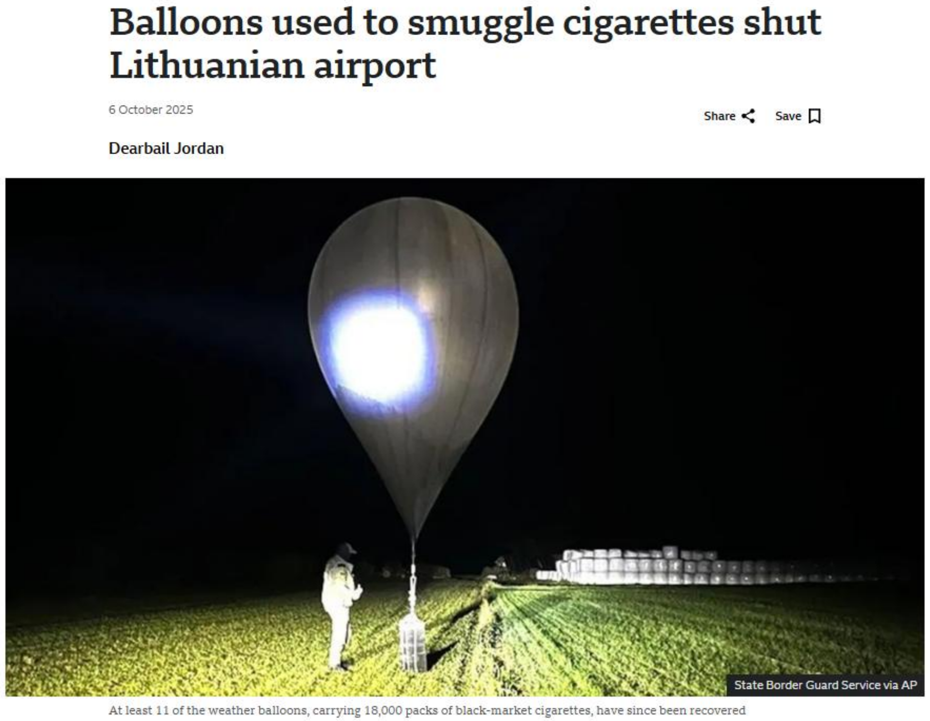
- Incursions of unidentified UAVs in all 3 Baltic countries, the UAV that fell in Latvia was even carrying explosives; Lithuania lately has been dealing with weather balloons sent from the territory of Belarus that has prompted the closing of Vilnius airport several times



The Russian out of control drone that crashed in Gaigalava parish was a "Shahed" type drone

09/09/2024 - 18:28 In Latvia

Information prepared by Media Relations Section



Balloons used to smuggle cigarettes shut Lithuanian airport

6 October 2025

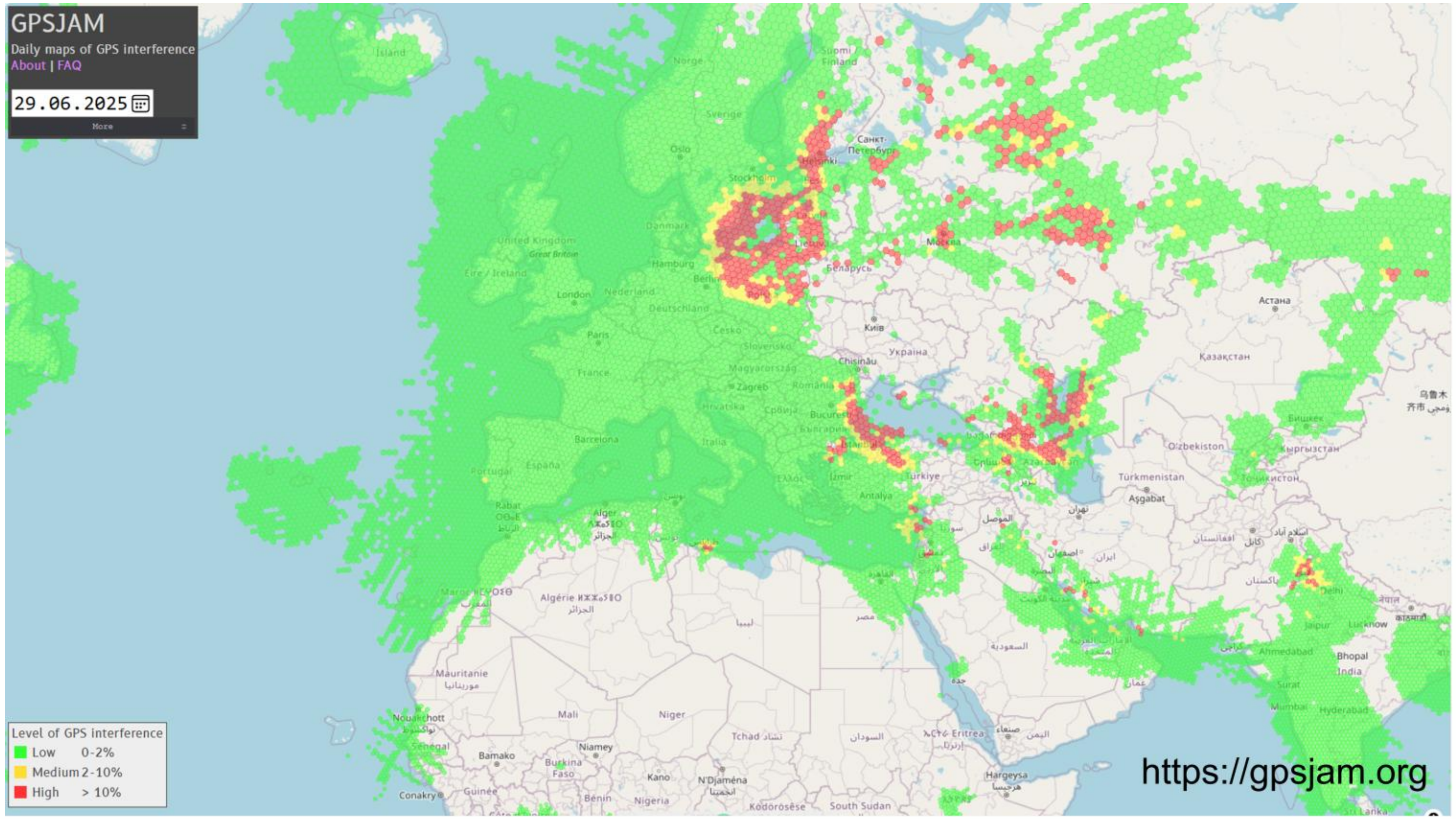
Dearbail Jordan

State Border Guard Service via AP

At least 11 of the weather balloons, carrying 18,000 packs of black-market cigarettes, have since been recovered

Incidents

- ○ Spoofing and jamming of GNSS signals over countries around the Baltic sea – disrupts geomagnetic measurements and GPS navigation
- ○ The GNSS signal is very susceptible to disruptions due to the distance that it needs to travel from the satellite, and it has a significant natural loss which makes spoofing easier

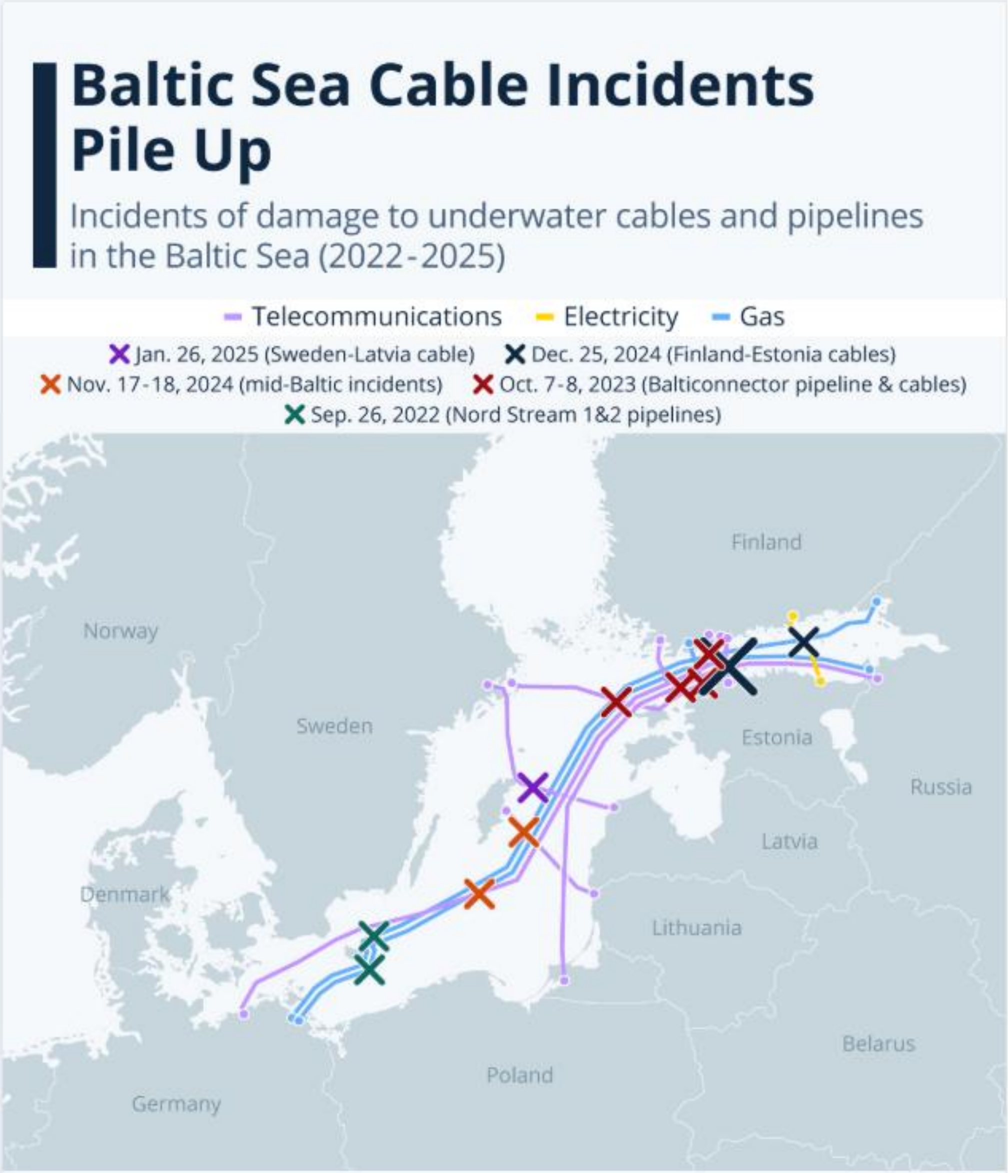


https://gpsjam.org

Quality implications of requirements to make the data both open and secure

Incidents

- Damaging the underwater communications in the Baltic sea
- In the last 3 years there have been several incidents that have damaged gas pipelines, telecommunications and electricity cables
- Damage mostly caused by ships who drop their anchors while shipping over the underwater cables
- NATO increased its presence in the Baltic sea in January 2025 launching «Baltic Shephard» mission and after that there have been no reports on new incidents



Baltic Sea Cable Incidents Pile Up

Incidents of damage to underwater cables and pipelines in the Baltic Sea (2022-2025)

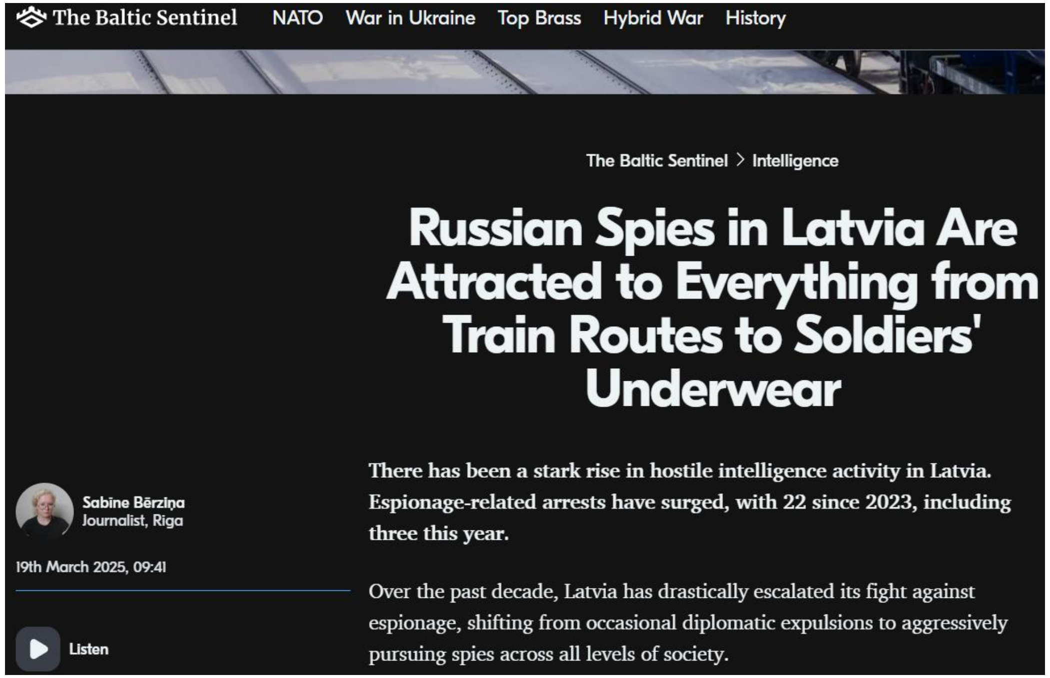
- Telecommunications
- Electricity
- Gas

X Jan. 26, 2025 (Sweden-Latvia cable)
X Dec. 25, 2024 (Finland-Estonia cables)
X Nov. 17-18, 2024 (mid-Baltic incidents)
X Oct. 7-8, 2023 (Balticonnector pipeline & cables)
X Sep. 26, 2022 (Nord Stream 1&2 pipelines)

Quality implications of requirements to make the data both open and secure

Incidents

- Frequent news about persons arrested for capturing military/critical infrastructure objects on photo/video and reporting it to Russia, highest profile cases of spying include a former member of parliament and a former member of European parliament



The Baltic Sentinel NATO War in Ukraine Top Brass Hybrid War History

The Baltic Sentinel > Intelligence

Russian Spies in Latvia Are Attracted to Everything from Train Routes to Soldiers' Underwear

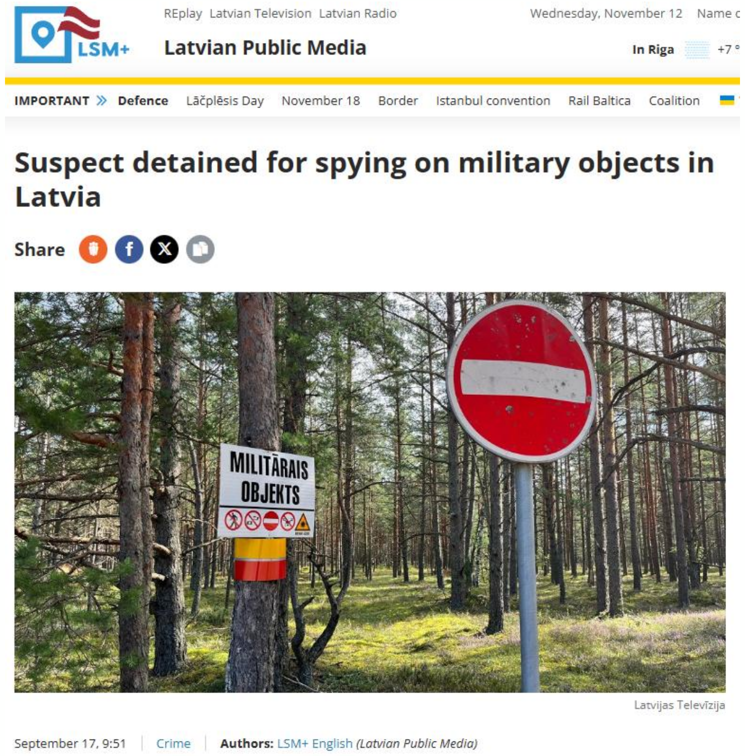
Sabine Bērziņa
Journalist, Riga

19th March 2025, 09:41

Listen

There has been a stark rise in hostile intelligence activity in Latvia. Espionage-related arrests have surged, with 22 since 2023, including three this year.

Over the past decade, Latvia has drastically escalated its fight against espionage, shifting from occasional diplomatic expulsions to aggressively pursuing spies across all levels of society.



LSM+ REplay Latvian Television Latvian Radio Wednesday, November 12 Name c

Latvian Public Media In Riga +7 °

IMPORTANT » Defence Lāčplēsis Day November 18 Border Istanbul convention Rail Baltica Coalition

Suspect detained for spying on military objects in Latvia

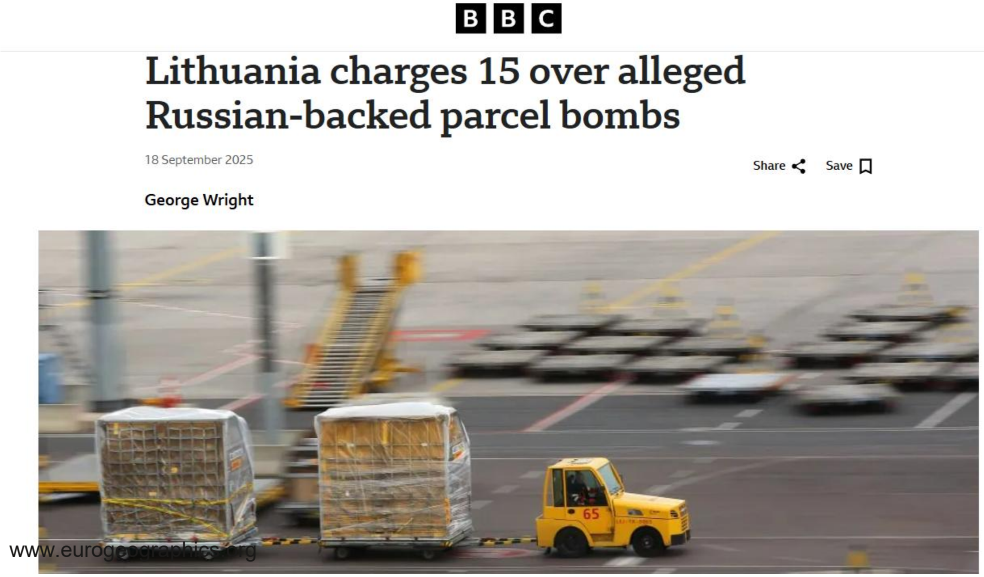
Share

Latvijas Televīzija

September 17, 9:51 | Crime | Authors: LSM+ English (Latvian Public Media)

Incidents

○ Persons arrested because of planned and partially executed sabotage by sending homemade explosives via courier service with successful combustions in a warehouse in Birmingham, logistics center in Leipzig and on a highway in Poland, packages sent from Latvia



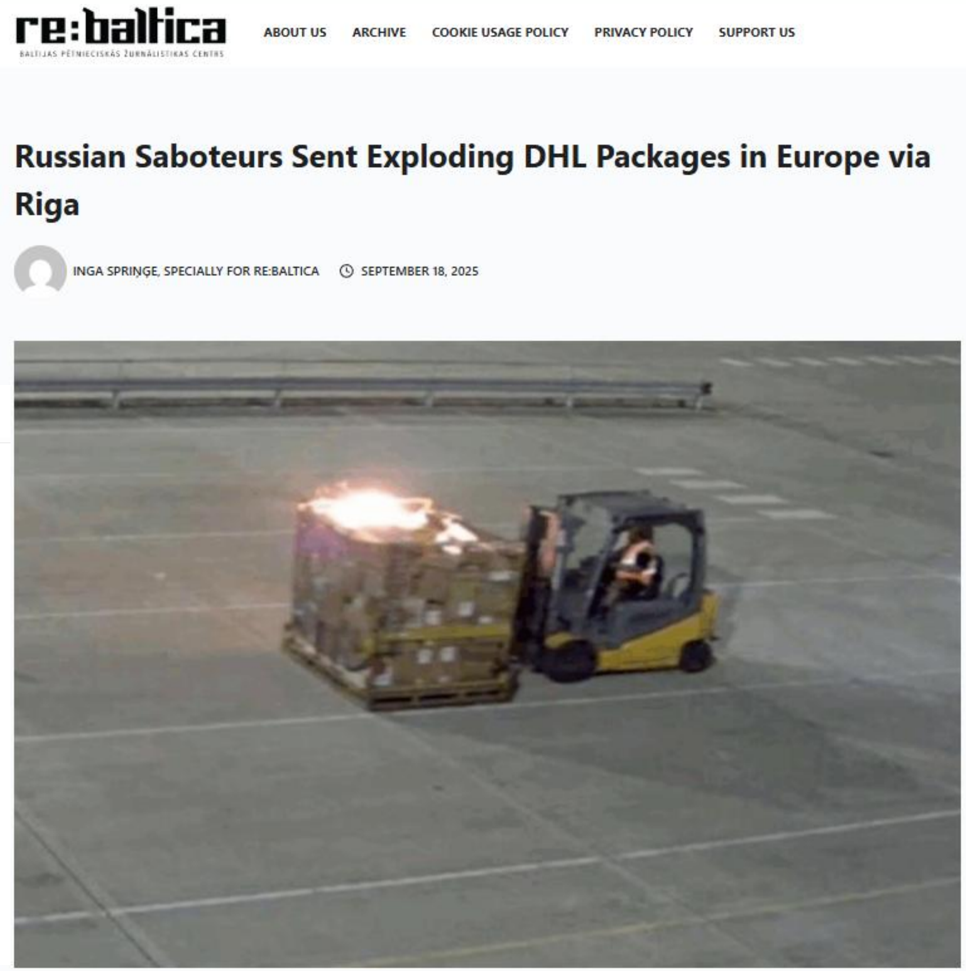
BBC

Lithuania charges 15 over alleged Russian-backed parcel bombs

18 September 2025

Share Save

George Wright



re:baltica BALTIJAS PĒTNIECISKĀS ŽURNĀLISTIKAS CENTRS

ABOUT US ARCHIVE COOKIE USAGE POLICY PRIVACY POLICY SUPPORT US

Russian Saboteurs Sent Exploding DHL Packages in Europe via Riga

INGA SPRINGE, SPECIALLY FOR RE:BALTICA SEPTEMBER 18, 2025

Incidents

- Cyberattacks
  - The National Cyber Incident Response Institution of Latvia (CERT) reports that in 2025 almost every month there is a ransomware attack that either paralyses a company's IT infrastructure, leads to a data loss or stops the company's work altogether

  - Several municipalities, governmental websites and private companies have been targeted by wide-scale DDoS attacks in September 2025

  - Public sector employees advised not to use certain applications, that are known to be under the control of foreign intelligence services or are suspected to be

Preventive actions to safeguard the data

- Quite often the weakest link in the data security is the human operating with the data
- Using strong passwords, regularly changing the passwords and keeping them safe are straightforward steps, but these simple actions are still being ignored too often
- Limiting the access/rights to data for a single user is a useful step for an organization in preventing a data leakage, damage or loss
- There always is someone with the rights to access and edit everything, so this person must be well educated and prudent in the field of the data security

Preventive actions to safeguard the data

- During the Quality KEN spring meeting in 2025, which was an online event, there were breakout rooms on the topic of Open Data directive vs security issues

- Some of the issues from these breakout rooms:
    - One of the participating state agencies had recently been under cyber attack which led to significant issues in its everyday operations and lot of services going offline
    - Several participants stated that masking of sensitive data/objects is ongoing in their organizations
    - Most organizations limit the access to their authoritative data only to registered users
    - Some organizations limit the scale you can zoom to in their map browsers
    - Some organizations already limit the amount of a dataset per download - no easy access to the data for a whole country

Preventive actions to safeguard the data

- All the employees of LGIA have yearly training in IT safety and are instructed how to act in case of being contacted by foreign intelligence

- Identifying that one is being targeted by a foreign intelligence is quite hard for the average person as it can happen through friends and even relatives, it can start as a simple and unharmful favor

- A common way for authorities to safeguard important information lately is editing the data to exclude the sensitive parts from publicly available sources

- Access to datasets only for registered users after login, different levels of access

- While moving data to a cloud and working with online tools seems very tempting, the cloud services come with a risk

Recent cloud service issues

- Amazon Web Service (AWS) crashed on 21st October 2025 and brought with it major disruptions to millions of users worldwide, impacting social platforms like Snapchat and Reddit, banks like Lloyds and Halifax, games like Roblox and Fortnite

- The irony in the AWS issue – the company sells its services stating that it will look after any business's computing needs, but if the AWS itself fails, the company buying the service is left with no backup option

- The AWS in one 3 major actors in world’s cloud services and is considered the leader in this segment, all of the three being based in the USA, which exposes Europe’s reliance on USA in the base functions of the world wide web

Recent cloud service issues

- As recently as last week there was also an issue in Latvia with Latvian State Radio and Television Centre (LVRTC) which provides cloud service due to technical issues with server clusters

- Mostly the results of these issues warried – some websites were slower than usual, other sites and services stopped working altogether

- Even though both these examples currently are deemed to be technical issues, it shows that data security sometimes can be subject to technical malfunctions even without malicious actions from outside

Editing the data to exclude sensitive parts

- There are datasets of objects of Military importance in Latvia, a dataset that defines protective zones around them

- There's also a list of objects that are considered as critical infrastructure, all of them fall under the scope of the law about State secret

- For the spatial data producers there are restrictions that must be considered, as the information about these objects may be available to public only partially and not as a spatial dataset with whole list and exact location of these objects

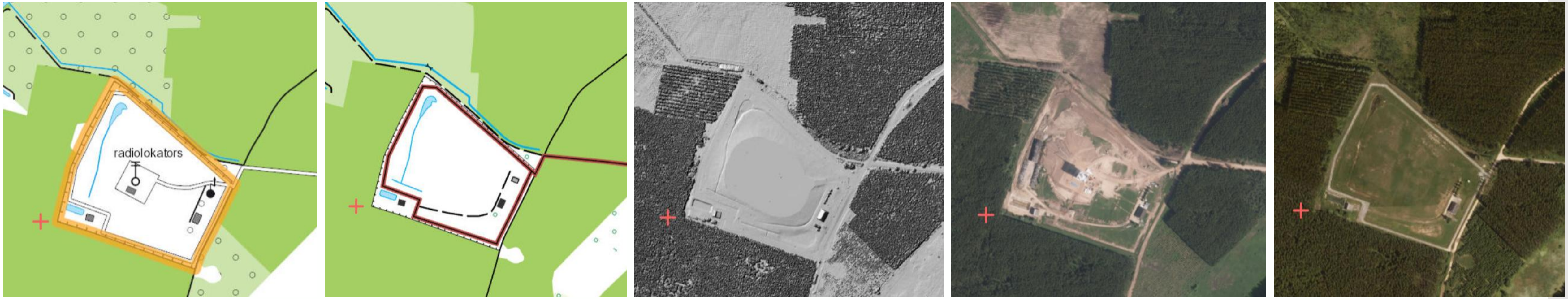
Editing the data to exclude sensitive parts

- And here is the interesting part of the work of a cartographer or a GIS specialist – how to fulfill the obligation stated by the state law and:
  - Not make the omission too obvious
  - Not create a contradiction with other datasets
  - Depict the reality one can see in the field or in satellite imagery – which everyone can check

Editing the data to exclude sensitive parts

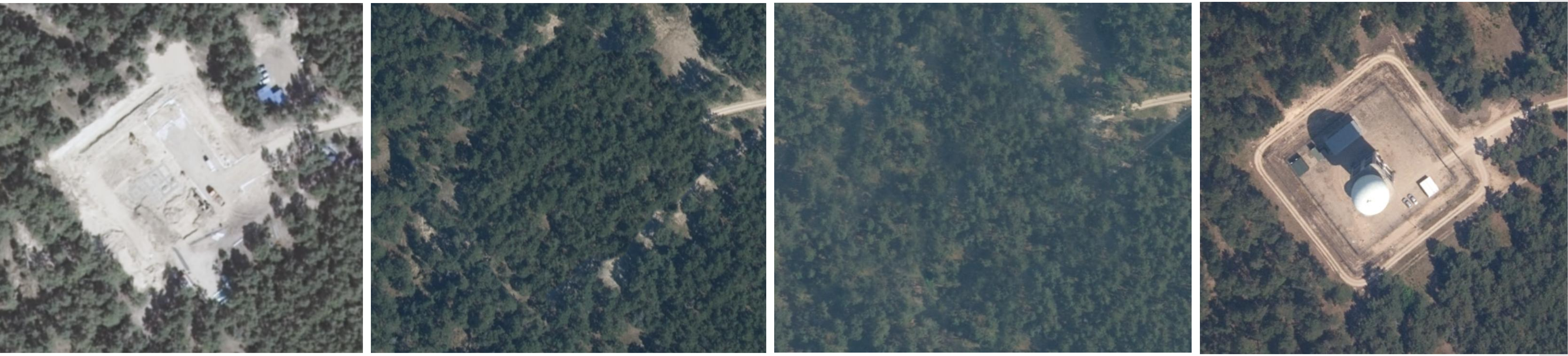
- This obviously leads to creation of two types of maps – for military purposes and civilian maps, that exclude not only certain symbols, but also certain objects

- As for the civilian data, there are not only maps, but also orthophotos and LiDAR data – both point clouds and digital models, that all must be consistent with each other and compliant with the rules for the objects that can and cannot be shown in the data



Editing the data to exclude sensitive parts

- No point in hiding information in orthophotos and digital models, that can be seen on satellite imagery – publicly available orthophotos from 4 successive cycles of the same place:



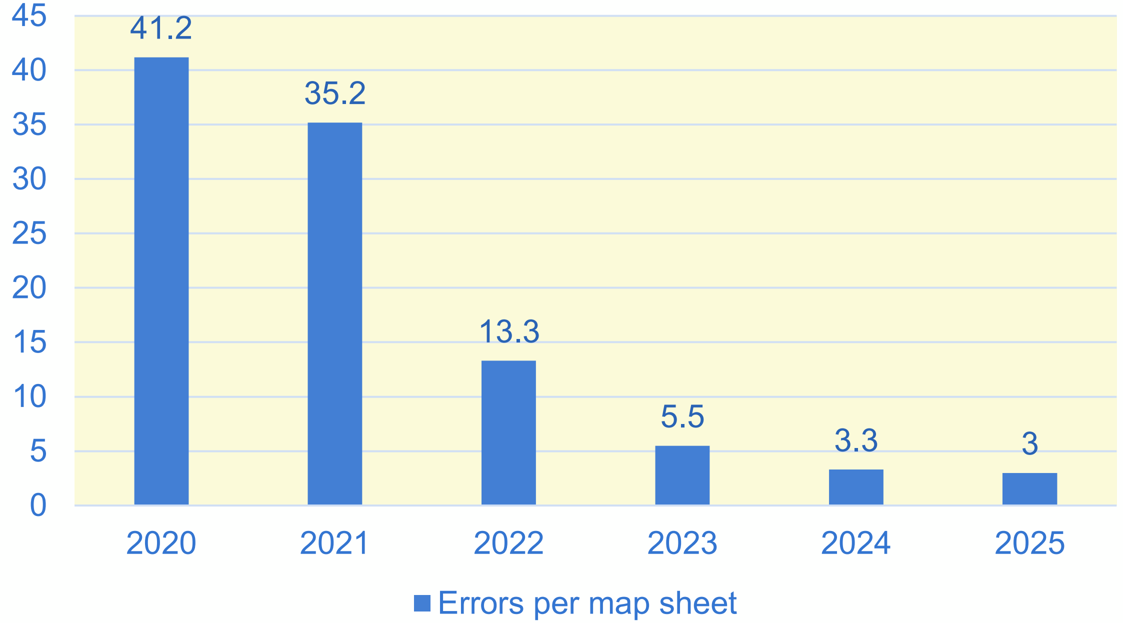
Editing the data to exclude sensitive parts

- Inclusion by omission - sometimes trying to hide too much can leave a glaring hole, that identifies objects of interest more than hides them
- Lot of specialists involved in editing the data to exclude sensitive parts/military objects which obviously make the data less accurate and introduce the human factor of error
- The characteristics of spatial data quality is a broad term, but it can be argued that among the main are these four: consistency, completeness, conformance and currency

The characteristics of the spatial data quality

- Consistency – even if the checks on exclusion of sensitive data are integrated into the data flow from the start of the data production and all of the personnel is trained equally, there can be a lot of inconsistencies in the data, therefore LGIA has independent unit for data validation that checks all the data before it’s final acceptance and shares the feedback with the data producers so that most errors can be eliminated during the data production

- In the table there can be seen the improvement of the data quality during the final validation process for the Topographic basemap of Latvia in scale 1:10 000



The characteristics of the spatial data quality

- Completeness – this one measure is probably the most affected by a decision to mask or hide something as such actions reduce the data completeness

- There is a known number of objects, that fall under the restrictions, but this data is not reported in metadata

- So, while representing 100% area of a certain territory, a dataset can still be incomplete due to masking or editing of the data, for example, by redactors of topographic maps

The characteristics of the spatial data quality

- Conformance – how well the data align with the predefined standards, formats and rules

- The customer usually should be the one defining the criteria for the data conformance, but in case of the EU level data, it hasn’t always been the case, as the data from different countries need to be harmonized

- The aim of several EU directives and initiatives has been to improve the harmonization of the spatial data among the member states, some have been less successful, some are just recently coming in force

The characteristics of the spatial data quality

- Currency – we all know that a map is obsolete as soon as it is finished, as the changes in the «real» world never stop, but a map represents a snapshot in time
- The same rule is valid as well for a topographic map, as for an orthophoto, satellite image, digital model – anything that is not updated constantly
- The more time passes, the worse is the temporal quality or the currency of the data and obviously there comes a point when the data is too old to be suitable for user needs
- When there is an event to get a user feedback, the data users always ask for a better data currency or faster updates

Conclusion

- While preparing presentation on this topic I've found out that not only GIS professionals in Latvia see the need of opening more datasets to the public and companies to generate innovation while maintaining the highest security standards

- The impression I got from my research was, that currently the main driving force is the need for security, and the EU member states have the final say, which of their authoritative data and how much of it can be open and reusable on Pan-European level, far from perfect situation for the businesses hoping to get more access to the data

- There are several EU level directives that drive the opening and sharing of the data, but even these documents recognize the need for the data security

Conclusion

- In the last 3 years there has been a huge shift in regional security that has forced to rethink strategies going forward both on national and European level, the main risks changing from environmental to man-made military and economic risks, and it is not easy to adopt these changes to existing directives

- As Europe strives to compete globally with other regions, we need the data to drive our development, as the AI age is rapidly expanding and AI relies on the availability of the data for its growth

- The aim of this presentation was not finding a way of opening more data and improving its security, but one thing is for sure - as the global landscape keeps changing, we'll have to be creative to navigate it successfully

Thank you for listening!