



Mapping Lithuania's analytical ecosystem



Introduction	3
Chapter 1.	
Ecosystem of Lithuania's analytical sector	4
1.1 Public-civil partnership	4
1.2 Legal framework and ethics	4
Chapter 2.	
Segmented mapping of organisations' activities	5
2.1 Military OSINT and GEOINT	5
2.2 Countering disinformation and Infosec	11
2.3 Investigation of sanctions evasion and economic crimes	17
2.4 Extended catalogue	19
Chapter 3.	
Lithuanian OSINT tools	21
3.1 Specialised bots and parsers in the volunteer sector	21
3.2 Public licenses and Open Source	22
3.3 Conditions for regulatory and commercial access and opportunities for Ukraine	25
3.4 Detailed financial formats for Ukraine	26
Chapter 4.	
Analysis of cooperation between Ukraine and Lithuania	27
4.1 Security and intelligence level	27
4.2 Journalism and OSINT level	28
4.3 Lithuania's experience of cooperation with other countries	28
4.4 Challenges and barriers	29
4.5 Prospective areas for cooperation for 2026-2028	30
Methodology	32

Introduction

Lithuania, a country of approximately 2.8 million people¹, illustrates how a society can build a systematic defence against external information threats. Its geopolitical position next to Russia and Belarus gives local OSINT communities and organisations a clear focus: real-time monitoring of hybrid threats, tracking covert schemes to evade sanctions, and countering disinformation, among other activities.

Russia's full-scale invasion of Ukraine in 2022 significantly reshaped the work of Lithuanian researchers and analysts. They reallocated resources, drew increasingly on Ukraine's defence experience, and launched large-scale investigations into financial flows supporting Russia. In Lithuania, open-source intelligence (OSINT) is not confined to intelligence services or journalists. Instead, it operates through a broad network of cooperation between the state and civil society.

Currently, independent think tanks, teams of investigative journalists, and volunteer networks play a key role in this work. Their experience is already being adopted in neighbouring countries.

The document covers 14 organisations that form Lithuania's OSINT ecosystem as of 2024-2026. The study is structured around four functional areas, each with its own tools, data sources, and end users of analytical materials: military OSINT and geospatial intelligence, countering disinformation and information security, investigations into sanctions evasion, and strategic OSINT.

The need for this study emerged from the lack of a systematic overview of Lithuania's OSINT community in Ukrainian-language sources. While references to individual organisations exist, they lack coherent structure. This document fills that gap by providing a practical reference point: it maps potential Lithuanian partners, outlines their areas of activity in detail, and identifies opportunities for both grant-based and operational cooperation with Ukraine.

This report was prepared with the support of the non-governmental organisation Terrecon.

Authors:

Daria Verbytska, CEO of Terrecon.

Kateryna Saienko, OSINT analyst at Terrecon.

Consultant:

Yevheniia Fedotova, Vice President of the Liberal-Democratic League of Ukraine.

¹ https://european-union.europa.eu/principles-countries-history/eu-countries/lithuania_en

Chapter 1.

Ecosystem of Lithuania's analytical sector

1.1 Public-civil partnership

In the Lithuanian context, state institutions such as the Ministry of National Defence, the Strategic Communications Department of the Lithuanian Armed Forces (hereafter StratCom), and the intelligence services view civilian investigators not as external observers, but as a “civilian wing” of intelligence work.

Since 2023, the National Crisis Management Centre has been the key institution coordinating responses to hostile information operations. LTU AF StratCom is part of this ecosystem, along with other 10 institutions (and additional ones, depending on the issue). This cooperation works in both directions²: volunteer networks (such as the Lithuanian “elves”) and think tanks (such as Debunk.org) carry out initial monitoring of hostile narratives, while military structures analyse this data within a broader security context, verify threats, and use the findings to inform the public and support defence decision-making.

Cooperation with intelligence services, in particular the State Security Department, is more closed in nature, but no less effective, especially in the areas of economic intelligence and monitoring of sanctions evasion.

1.2 Legal framework and ethics

The activities of Lithuanian OSINT investigators operate within the European Union's legal framework, where the General Data Protection Regulation (hereafter GDPR³) serves as an important regulatory instrument. The implementation of this regulation has significantly reshaped open-source investigation methodologies, forcing analysts to balance the public interest in investigations with individuals' right to privacy. In Lithuania, GDPR requires organisations to clearly justify the collection and storage of personal data on ethical grounds. As a result, the sector has evolved in a way that places strong emphasis on source legitimacy and strict anonymisation practices, helping investigators avoid legal risks that could undermine trust in the OSINT field as a whole.

The implementation of the NIS 2⁴ cybersecurity directive has become a key factor reshaping the operations of Lithuanian technology hubs. Organisations providing threat monitoring or data analysis services to the public sector are now categorised as entities subject to enhanced cybersecurity requirements. This includes mandatory audits of data storage systems, incident reporting protocols, and verification of software supply chains.

² <https://www.propastop.org/en/2019/11/01/lithuanias-attitude-to-propaganda-forcefully-against-lies/>

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

⁴ <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

Chapter 2.

Segmented mapping of organisations' activities

Lithuanian OSINT organisations can be divided into three operational segments, each employing different methods of collecting information:

Segment	Activities / end users
Military OSINT / GEOINT	Analysis of combat operations, movements of military equipment, and satellite images. End users: Lithuania's Ministry of Defence, NATO, analysts.
Countering disinformation	Monitoring narratives, identifying bot networks, and fact-checking. End users: media, government institutions, and general public.
Sanctions evasion and financial schemes	Investigations into supply chains and covert schemes. End users: customs authorities, the prosecutor's office, and journalists.

2.1 Military OSINT and GEOINT

This is the least publicly accessible segment of open-source intelligence is shaped by veterans, former officers, special forces specialists, and state institutions.

The technological foundation of defence-related initiatives relies heavily on commercial satellite intelligence. Regional analysis increasingly draws on high-resolution images from providers such as Planet or Maxar, enabling real-time monitoring of the construction of military facilities in Belarus and the movement of equipment along the Suwałki Corridor.

A distinct part of the country's analytical landscape is its state security sector, which functions as a closed system. Despite its high level of secrecy and limited public access, these institutions set the key direction for the broader civilian OSINT ecosystem, serving as its main beneficiaries and ultimate end users.

The Second Investigation Department under the Ministry of National Defence (AOTD⁵) is considered the successor to Lithuania's interwar intelligence tradition, although in its present form it was re-established in 1990. Its work focuses on military intelligence and counterintelligence, with particular attention paid to assessing Russia's military capabilities.

The State Security Department (hereafter VSD⁶) serves as Lithuania's main civilian intelligence service, focusing on a broad range of threats, including economic security, counterintelligence, and the protection of the constitutional order.

⁵ <https://www.aotd.lt/>

⁶ <https://www.vsd.lt/>

Its responsibilities include monitoring foreign investment in relation to strategic assets, counterterrorism, and countering disinformation operations that may undermine public stability.

The organisations jointly publish an annual report titled “Assessment of Threats to National Security,” which serves as a key resource for the OSINT community. It helps shape and validate the priorities of civilian investigators by identifying the most vulnerable sectors and key geographic areas of concern.

Organisations:

Lietuvos šaulių sąjunga (Lithuanian Riflemen's Union)



The organisation has around 17,000 members. It brings together civilian specialists in IT, linguistics, and data analysis who use their professional expertise to support military intelligence tasks within the territorial defence system.

It is led by a military officer, Colonel Linas Idzelis⁷.



“The Riflemen” operate within specialised information resistance units. Their OSINT work is mainly split into two core areas: information operations (InfoSec) and geospatial intelligence (GEOINT), including drone-based reconnaissance.

In military OSINT and GEOINT, specialised Riflemen units analyse commercial satellite images, integrate data from open-source mapping platforms, and coordinate civilian drone operators to produce tactical reports in support of the regular armed forces.

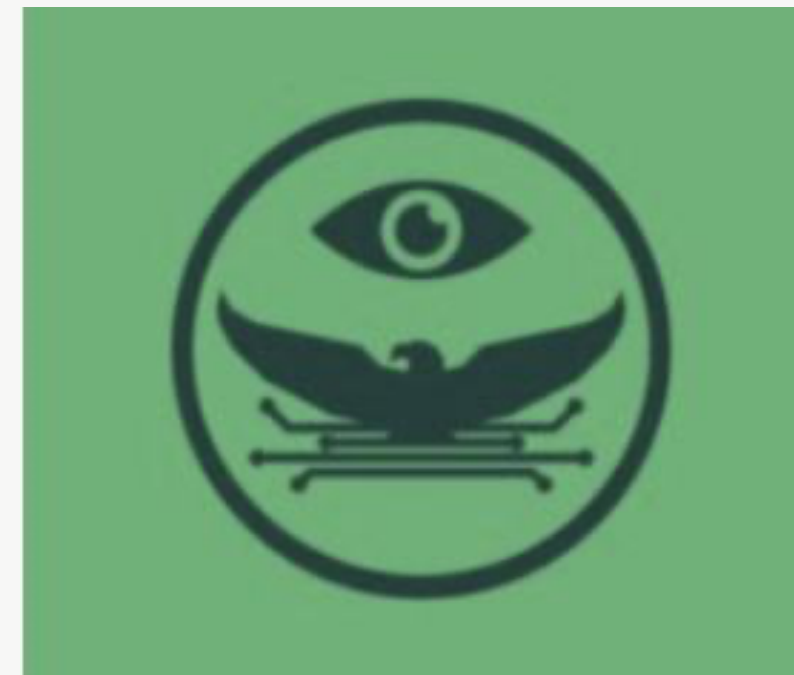
In cooperation with the Mobilisation Department, the Riflemen's Union trains residents of border regions (particularly around the Suwałki Corridor) in basic OSINT and GEOINT skills.

⁷ <https://lt.linkedin.com/in/linas-idzelis-b18588197>

Civilians are taught how to verify the authenticity of images, geolocate suspicious objects, and report unusual activity or military movements near the border through secure government channels.

Cases:

Lizdeika⁸ Cyber Unit



An internal cyber and technology team that develops digital training environments designed to simulate conditions as close as possible to real-world threats. Within these “virtual training grounds,” participants practise incident response, digital forensics, and elements of OSINT analysis under simulated scenarios of information attacks. The platform integrates practical modules in cyber defence, drone reconnaissance, and data analysis, creating a closed training ecosystem used to prepare for hybrid threats and support coordination with Lithuania's defence structures.

Locked N' Loaded



A Lithuanian civil defence and security analysis centre officially registered as a non-governmental organisation in Vilnius. The platform is headed by Paulius Stonis⁹.



The organisation's main platform is the website parakomanai.lt, where it publishes detailed tactical analysis, with Lithuanian as the primary language of communication. The project is aimed at military personnel, conscripts, and civilians who want a clearer understanding of the security situation in the Baltic region and the dynamics of the war in Ukraine.

⁸ <https://lizdeika.education/en/>

⁹ <https://lt.linkedin.com/in/paulius-stonis?trk=org-employees>

The analytical core of Locked N' Loaded is made up of armed forces veterans and seasoned experts with many years of military experience. The team's main mission is to turn complex military developments into clear, practical insights. The organisation produces detailed tactical analyses based on GEOINT, verification of satellite images, and in-depth open-source intelligence. It tracks movements of Russian troops, shifts in assault tactics, and studies Russian military operations directly in the Ukrainian war theatre, drawing lessons for Lithuania's own defence.

In addition to its daily monitoring of the front line, Locked N' Loaded develops specialised training programmes for both the public and private sectors. The team has also demonstrated its responsiveness and willingness to share expertise by taking part as speakers at the KITE 2025¹⁰ International Defence Technology Forum in Kyiv. At this specialised conference focused on innovation in security and intelligence, Lithuanian analysts presented their own GEOINT monitoring methods and approaches to tactical analysis of enemy force movements.

Cases:

Wargaming exercises¹¹

In these simulations, the centre's experts model the actions of an aggressor state, based on real military doctrine, operational planning, and tactical practices of Russian or Belarusian forces. Participants, including government officials, managers of critical infrastructure facilities, and members of the Riflemen's Union, must respond to evolving crisis scenarios in real time.



Locked N' Loaded enjoys a strong international reputation.

¹⁰ <https://nako.org.ua/en/direct/transparency-vs-secrecy/konferenciya-kite-dlya-ekspertiv-u-rozvidci-vikonavca-direktorka-nako-moderuvala-diskusiyu-pro-rol-socmerez-v-osint-en/>

¹¹ <https://lt.linkedin.com/in/paulius-stonis?trk=org-employees>

The centre is a member of both the Royal United Services Institute (RUSI) in the United Kingdom and the Lithuanian Defence and Security Industry Association, while also maintaining close ties with the Eastern Europe Studies Centre (EESC) and the Civic Resilience Initiative (CRI).

VISA



The Public Information Security Agency is a specialised analytical centre led by Mindaugas Sėjūnas ¹².



The work of Public Information Security Agency (VšĮ Visuomenės informacinio saugumo agentūra) is closely integrated into the analysis of real-world security challenges and threats in the Baltic region.

The agency specialises in advanced GEOINT methods and the systematic assessment of military and hybrid threats. Its analytical team focuses on collecting and verifying data from open sources and commercial satellite images. Specialists closely track logistics chains, the movement of military equipment, and the construction of military infrastructure along border areas.

A key feature of VISA's operating model is its non-public nature and direct cooperation with the state sector. Unlike organisations that produce content for public audiences or investigative journalism, it operates within a closed, collaborative framework.

BPTI & Digital Defense Competence Centre



Baltic Institute of Advanced Technology and the Digital Defence Competence Centre form a technological partnership specialising in research and development in the fields of algorithmic warfare and intelligence.

¹² <https://www.facebook.com/mindaugas.sejunas>

The centre develops advanced mathematical methods and AI models capable of automatically analysing vast volumes of geospatial data. The institute is founded and headed by Tomas Žalandauskas¹³.



Main GEOINT areas of specialisation include:

- * automating the detection of objects in satellite images and processing complex signal data;
- * developing computer vision algorithms that can automatically identify military equipment, detect concealed fortifications, assess infrastructure damage, and track changes in logistics networks;
- * improving AI systems so they can function effectively in conditions of enemy electronic warfare, as well as under heavy cloud cover or battlefield smoke.

Cases

Deployment of SAR-based systems for analysing critical infrastructure

In its analytical projects, BPTI uses synthetic aperture radar (SAR) satellite data to monitor railway, logistics, and energy infrastructure. The team detects changes in infrastructure assets regardless of weather conditions or time of day, models traffic loads on transport corridors, and analyses bottlenecks in critical supply chains.

BPTI is a key Lithuanian participant in European Defence Fund programmes. It is part of the ARMADA¹⁴ project consortium, funded by the European Defence Agency. Within this project, Lithuanian specialists are developing a roadmap and algorithms for applying artificial intelligence in the systems for automated analysis of Earth observation data.

¹³ <https://lt.linkedin.com/in/tomas-zalandauskas>

¹⁴ <https://www.bulletprove.com/armada.html>

2.2 Countering disinformation and Infosec

Civic Resilience Initiative (CRI)



Civic Resilience Initiative (CRI) is a Lithuanian non-governmental organisation founded in 2018 by security experts Linas Skirius, Lukas Andriukaitis¹⁵ and Tomas Kazulėnas¹⁶. It develops an information environment aimed at countering information threats.



The organisation develops programmes in gamified learning for young people, OSINT investigations, and security initiatives. In its security work, Civic Resilience Initiative takes a proactive approach to learning from Ukraine's experience for the development of Baltic and NATO defence strategy. It also hosts an annual international conference "Defending Baltics: War Lessons from Ukraine" in Vilnius, which brings together more than 500 military personnel, experts, and journalists¹⁷.



The team has a strong track record of getting harmful content removed, but cooperation with global platforms remains challenging. Requests to Google to take down toxic content are often ignored. Analysts attribute this to shifts in the company's internal policies in response to political changes in the United States.

¹⁵ <https://x.com/LAndriukaitis>

¹⁶ <https://www.facebook.com/tomas.kazulenas/>

¹⁷ <https://cri.lt/projects/challenges-of-the-contemporary-disinformation/>

In their work, analysts do not rely on a single universal software solution; however, for monitoring social media and analysing large volumes of video content, they actively recommend the Lithuanian platform RepSense¹⁸, which is capable of detecting emotional tone in data.

In its cooperation with the state, CRI mainly operates through grants and competitive programmes in the field of media literacy. The organisation says it develops project ideas independently and submits them to state institutions, rather than working on direct government contracts.

In an interview conducted for this study, the organisation's representatives highlighted key trends in their field, particularly the growing use of artificial intelligence in the information environment. At the same time, a significant share of influence campaigns is still carried out using traditional methods. A particular challenge remains the use of bot networks, including those linked to Russian information operations. The rise of generative technologies is making it increasingly difficult to detect automated content due to its high degree of personalisation. The interviewees also pointed to a lack of research on bot networks and information manipulation in Lithuania's information space.

Cooperation with Ukrainian colleagues

The interviewees expressed a strong interest in identifying partners for educational projects aimed at strengthening young people's resilience to information threats. Of particular interest are gamified learning formats, the experience of Ukrainian OSINT organisations in monitoring and analysing Russian and Belarusian content, and the involvement of Ukrainian experts in educational programmes and public events.

However, cooperation with Ukrainian organisations can at times be challenging. One of the main difficulties is the verification of local OSINT communities. A key reason is the lack of a reliable directory or registry that could be used to assess credibility of potential partners, their financial stability, and protect themselves against potential fraud. In addition, CRI also highlights other challenges, including language barriers (particularly limited English proficiency for direct communication), as well as frequent discrepancies in budgeting, often driven by inflated rates in Ukrainian project proposals.

Cases

GEOINT quests for school students

CRI developed several gamified formats for countering disinformation, ranging from street-based AR games (students use smartphones to identify disinformation in real urban settings) to a video game featuring a "fake expert," in which players must detect and debunk false claims¹⁹.

¹⁸ <https://repsense.io/>

¹⁹ [Kaip interaktyvus kompiuterinis žaidimas „Dezinformacijos Medžioklė“ ugdo kritinį mąstymą ir atsparumą dezinformacijai?](#)

CRI's flagship project is a GEOINT quest²⁰ in Vilnius, which brings together around 1,000 school and university students. Participants compete in teams representing their schools and complete tasks at designated locations, with NATO personnel from deployed contingents also involved.

A pilot project is also running on a separate platform in five schools. It is a dedicated AI-powered chatbot that helps students carry out independent investigations, points out logical errors, and guides their analysis.

"Lithuanian Elves"

The movement emerged in 2014 in response to Russian aggression against Ukraine and the accompanying information warfare. It began as a small group of around 20 enthusiasts, but by 2022 the "Elves" had expanded into an international network of approximately 22,000 volunteers across 13 countries in Central and Eastern Europe.



The movement's main mission is to counter disinformation by monitoring online comments, identifying bot farms, and amplifying counter-narratives to help protect ordinary users from propaganda. In their approach, volunteers focus on fact-checking and exposing anonymous trolls, while explicitly avoiding any form of cyber espionage or hacking tools. Given the security risks involved, members carefully conceal their identities and operate as a closed, anonymous expert community.

The "Elves" have become a source of expertise for international security institutions, including NATO's Strategic Communications Centre of Excellence in Riga. These volunteer groups complement existing NATO and EU structures, strengthening links between government institutions and active civil society.

The movement is integrated with the analytical platform Debunk.org²¹, which functions as an OSINT hub for analysing disinformation. Volunteers collect and carry out initial identification of suspicious information campaigns on social media. The "Elves" themselves are also explicitly described as a volunteer community that works with Debunk.org to detect and counter disinformation.

²⁰ Disinformation Challenge

²¹ <https://www.debunk.org/about-elves>

Established in 2018, Elves Academy has become an international platform for training hundreds of specialists in countering hybrid threats, contributing to the standardisation of OSINT methodologies across the Alliance.

Cases

“Bust-AD” campaign²²

The operation was launched in response to the rise of generative AI, which pro-Russian hackers and financial scammers began using to bypass moderation on Facebook and Instagram. Volunteers found that over the course of a year (from September 2023 to September 2024), this malicious advertising reached nearly 6 million users across Europe. The “Elves” traced the campaign to Russian servers and passed the evidence directly to Meta, prompting the platform to block hundreds of fraudulent advertising accounts.

Debunk.org



A technological and analytical organisation combining automated AI-driven monitoring with a network of volunteer analysts known as the “Elves.” The organisation evolved from the Demaskuok platform, founded by the major Baltic news portal Delfi.

Debunk.org monitors more than 2,500 web domains in 26 languages, processing around 30,000 articles daily²³. Its own platform, DebunkReach, measures the reach of each piece of disinformation by tracking backlinks and social media engagement²⁴.

The organisation systematically publishes weekly and monthly overviews of the disinformation landscape in the Baltic states, focusing on narratives that undermine military support for Ukraine, promote anti-sanctions messaging, and frame such assistance as “unnecessary.” These reports serve as a valuable open resource for partners studying Kremlin influence in Central and Eastern Europe.

Sprinter network²⁵

A large-scale mapping of a network of websites and accounts spreading pro-Russian narratives across the Baltic region and Poland in a coordinated manner. The investigation identified structural links between ostensibly independent media outlets and state-run propaganda channels in Russia and Belarus.

²² <https://www.debunk.org/bust-ad-russian-backed-deepfake-of-a-lithuanian-3-plus-news-reporter-appears-on-facebook-urging-s>

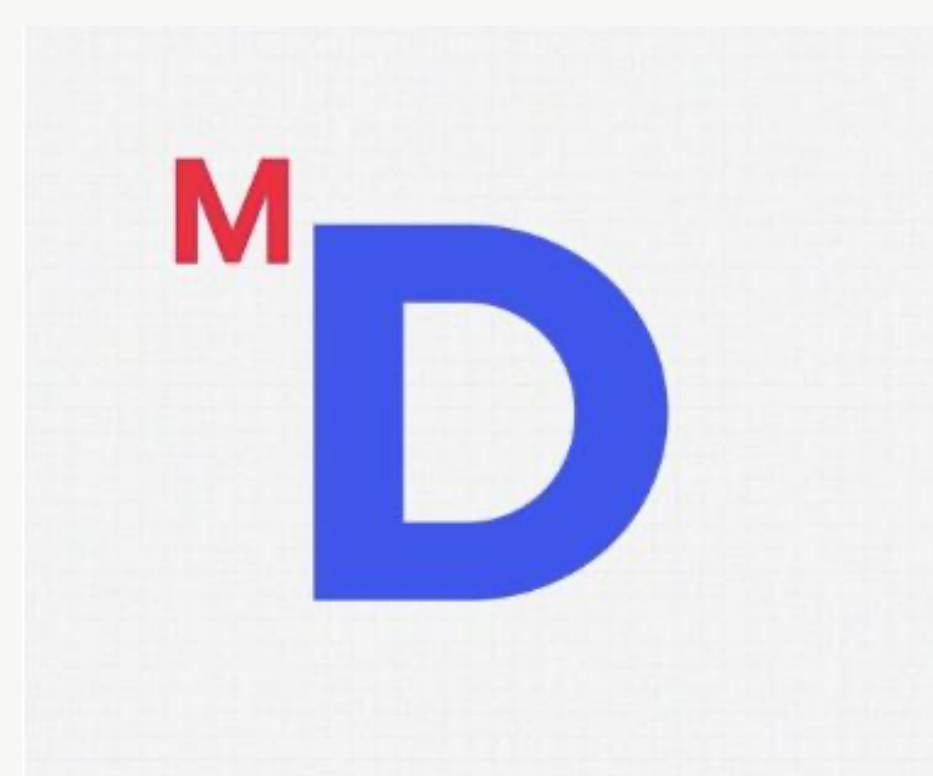
²³ https://books.google.se/books?id=wD-MEAAAQBAJ&redir_esc=y

²⁴ <https://www.debunk.org/methodology>

²⁵ <https://www.debunk.org/the-sprinter-network-unmasking-the-disinformation-web>

Belarusian “security content” on X²⁶

An analysis of how content from Belarusian security agencies is spread through a network of accounts on X. The investigation revealed mechanisms of coordinated amplification of Belarusian information influence, directed against Lithuanian society and support for Ukraine.

Media initiatives**DELFI Melagiu Detektorius**

Launched in 2018 by editor Aistė Meidutė, the project is integrated into the news ecosystem of the Lithuanian media outlet Delfi.



It helps debunk disinformation as soon as it appears. The content is published in three languages: Lithuanian, Polish, and Russian. The focus on national minorities helps protect vulnerable groups from external influence and maintain social unity.

The topics covered range from health-related disinformation to complex Russian geopolitical narratives. The project is officially certified by the International Fact-Checking Network and the European Fact-Checking Standards Network.

In its work, “Detector of Lies” uses OSINT tools to verify visual content, identify manipulated edits, and trace the origins of fake news through metadata and digital footprints.

The project is run by professional investigative journalists who specialise in analysing complex information operations. It also collaborates with technology partners, including Debunk.org. Their tools help detect suspicious content at an early stage of its dissemination.

²⁶ <https://www.debunk.org/disinformation-without-borders-how-belarusian-silovik-content-spreads-across-x>

Cases

Debunking the fake claim about “a NATO and European plan to occupy Moldova”²⁷

Ahead of important elections in Moldova, Russia's Foreign Intelligence Service launched a large-scale information operation through bot networks and pro-Kremlin accounts in Lithuania. Analysts traced the original sources of the manipulation and proved that Russian intelligence had completely distorted information about routine NATO defensive exercises.

Media4Change



An international movement bringing together more than 640²⁸ journalists, experts, and civil society representatives from different countries.

Founded by Neringa Jurčiukonytė²⁹, the organisation focuses on three interconnected areas: human rights, investigative journalism, and media literacy.



It serves as a coordinating hub for many initiatives, including the open-data platform Karštos Pėdos. Over the past six years, the team has analysed more than 143,000 materials about stigmatised groups in the Lithuanian media outlets. The organisation has also delivered more than 200 training sessions for journalists, journalism students, and volunteer educators³⁰.

Media4Change plays an active role in analysing coverage of Ukraine across Lithuanian and Baltic media, documenting anti-Ukrainian rhetoric, and developing counter-narratives.

²⁷ <https://becid.eu/facts/rusijai-paskelbus-apie-europos-plana-okupuoti-moldova-jav-analitikai-ispeja-del-kremliaus-keslu-po-moldovos-rinkimu/>

²⁸ <https://www.media4change.co/>

²⁹ <https://lt.linkedin.com/in/neringa-jurciukonyte>

³⁰ <https://www.media4change.co/project/>

³¹ <https://karstospedos.lt/index.html>

Cases

Creation and evolution of “Karštos Pėdos” open data ecosystem³¹

Media4Change coordinated the development of an interactive open data platform that has become an essential resource for investigative journalism. The platform is widely used by both leading national media outlets and regional reporters as a starting point for their investigations.

2.3 Investigations of sanctions evasion and economic crimes

Siena



Founded in 2019 by journalists Šarūnas Černiauskas³² and Miglė Krancevičiūtė³³, the organisation publishes one major investigation every month.



Siena's investigations focus on sanctions evasion, corruption in the public sector, the misuse of EU funds, financial crime, and criminal networks linked to Russia and Belarus.

After 2022, the organisation significantly shifted its operational focus towards tracking sanctions evasion – the schemes through which money and goods continue to flow in support of Russia's wartime economy. According to the organisation itself, its investigations published since the full-scale invasion have directly led to fines and asset freezes worth more than 12 million euros, as well as the dismantling of smuggling networks³⁴.

Siena is an official partner of OCCRP, an international network of investigative journalists from around the world. This status gives the team access to global databases and enables it to collaborate on cross-border investigations with more than 100 media organisations across over 60 countries.

³² <https://www.icij.org/journalists/sarunas-cerniauskas/>

³³ <https://lt.linkedin.com/in/migle-kranceviciute>

³⁴ <https://www.siena.lt/>

Cases

Cryptocurrency flows to the Wagner Group and the Rusich Sabotage Assault Reconnaissance Group³⁵

As part of an international investigation, Siena documented how the Russian paramilitary group Rusich, which has been accused of war crimes in Ukraine, raised hundreds of thousands of euros through cryptocurrency donations channelled via Baltic companies. The investigation also identified links between Estonian and Lithuanian crypto firms and Russia's Sberbank.

LRT Tyrimų skyrius



The LRT investigative team is a journalism unit of Lithuania's public broadcaster. It was established as a separate division in 2018. The unit is led by Indrė Makaraitytė³⁶.



The team's core operational focus is national security in its broadest sense. It specialises in exposing schemes to circumvent EU sanctions on Russia and Belarus, mapping Russian business influence in the Baltic region, and dismantling legal manoeuvres that Kremlin-linked actors attempt to deploy within Lithuania. Most of the content is published in Lithuanian, reflecting its focus on a domestic audience; however, key investigations are translated into English and Russian to reach international audiences.

³⁵ vsquare.org/tales-from-the-crypto-money-laundering-fraud-sanctions-estonia-lithuania-russia/

³⁶ <https://www.m100potsdam.org/en/participants/colloquium/indre-makaraityte/index.html>

³⁷ <https://www.occrp.org/en/investigation/traders-are-sneaking-banned-russian-and-belarusian-wood-into-the-eu-by-pretending-its-from-central-asia>

Cases

The “Kazakhstan and Kyrgyz express” (circumventing sanctions via Central Asia)³⁷

A series of international investigations in which the team analysed customs databases, transport invoices and registers of European companies after strict sanctions were imposed on Belarusian timber and Russian oil products. The investigation found that sanctioned goods from Belarus and Russia were being widely imported into the EU as supposedly originating in Central Asia, using falsified certificates.

2.4 Extended catalogue

Laisvės TV OSINT Unit



Laisvės TV is an independent online media outlet founded by journalist Andrius Tapinas³⁸. It combines the capabilities of a media platform with the flexibility of an investigative community.



It focuses on uncovering hidden links between Lithuanian politicians and business figures and pro-Kremlin networks, as well as directly contributing to defence-related initiatives (including raising 6 million euros in just three days to purchase Bayraktar for Ukraine). It also works closely with the volunteer fact-checking group “Lithuanian Elves” to verify information on social media. Findings from Laisvės TV investigations regularly trigger inquiries by Lithuania’s Financial Crime Investigation Service (FNTT) and the Special Investigation Service (STT)³⁹.

³⁸ <https://lt.linkedin.com/in/andrius-tapinas-51b169152>

³⁹ <https://www.15min.lt/naujiena/aktualu/lietuva/pradetas-ikiteisminis-tyrimas-del-garnis-gautos-lengvatines-paramos-is-nacionalinio-pletros-banko-ilte-56-2467120>

Patikrinta (15min.lt)

A fact-checking project launched in 2016 by journalist Liepa Želnienė⁴⁰ within the newsroom of 15min. It is now led by Eglė Zicare.



Patikrinta became the first project in the Baltic states to receive certification from the International Fact-Checking Network.

What sets it apart is its focus on domestic politics and the ways in which local populist or radical groups use manipulation. The team is also directly integrated into the news feed of one of the country's most visited websites.

DIGIRES

A science and technology project focused on strengthening information security in society. It was launched in 2021 at the Faculty of Public Communication of Vytautas Magnus University, in cooperation with the media company Delfi Lietuva and partners from the civic sector. The project was initiated and is led by Aukšė Balčytienė⁴¹.

⁴⁰ <https://www.facebook.com/liepa.zelniene/>

⁴¹ <https://lt.linkedin.com/in/aukse-balcytiene-678858211>



It brings together university researchers who develop AI algorithms for the early detection of propaganda, as well as practising journalists. Its model is focused on long-term analysis of how disinformation spreads, particularly how it reaches vulnerable groups such as ethnic minorities in border regions.

Chapter 3.

Lithuanian OSINT tools

3.1 Specialised bots and parsers in the volunteer sector

* The “Trusted Flagger” reporting automation tool

When a researcher identifies fake news or a disinformation campaign, the system builds a standardised evidence package based on the Berkeley Protocol. It captures verified screenshots, logs URLs and pulls relevant metadata. The report is then sent via a secure API straight to moderation teams at platforms such as Meta, TikTok or Google, bypassing the normal review queue.

* Parsers of customs declarations and rail shipment data

Scripts and AI tools automatically extract and structure cargo data from customs declarations, transit systems and rail shipment data across EU and Central Asian countries. This process may involve platforms such as MUJ⁴² and Rava⁴³, as well as logistics parsing systems like 8devices.⁴⁴

The data can also be aggregated through European rail documentation systems such as ORFEUS and CIM/SMGS, as well as digital logistics ecosystems used by carriers and integrators (Transporeon and LTG Cargo), helping to build analytics on trade flows and supply chains.

⁴² <https://www.muji.lt/en>

⁴³ <https://rava.lt/en/metro-program/>

⁴⁴ <https://www.8devices.com/>

* “Skaidrinam Extractor” OCR financial reporting parser

During a volunteer audit of MPs’ use of public funds, IT volunteers built a system based on Tesseract/EasyOCR, integrated with local LLM models. The software automatically reads and digitises hundreds of thousands of messy scans of fuel receipts, invoices and financial reports into a single structured table, while instantly flagging anomalies and possible fraud.

3.2 Public licenses and Open Source

All tools and databases developed as part of the civic audit are released under the international Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

* Lietuvos atvirų duomenų portalas (data.gov.lt)⁴⁵

A single access point consolidating more than 2,500 datasets from all ministries, municipalities and public agencies. The platform provides direct access to raw data in CSV, JSON, XML and GML formats via open APIs. It also enables large-scale parsing of data on public assets, transport flows, procurement, environmental conditions and infrastructure, serving as a foundation for detecting systemic anomalies.

* Valstybės įmonė Registrų centras⁴⁶

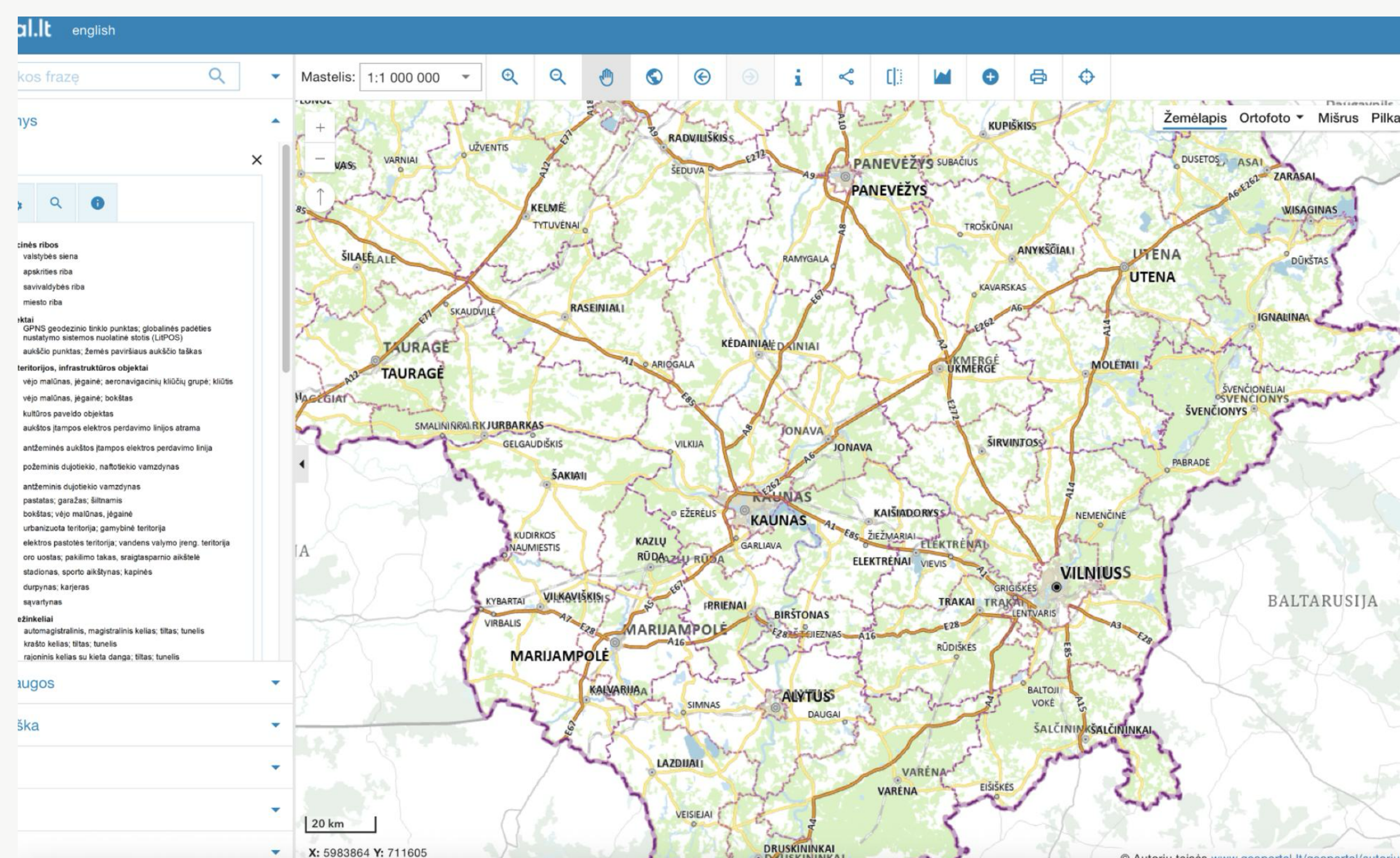
It maintains the country’s core national registers. Under its open data policy, it provides monthly raw extracts from the Register of Legal Entities, the Beneficial Ownership Database, the Real Estate Register and the Address Register. It is a key tool for financial intelligence and sanctions monitoring. It allows users to trace ownership structures, identify European assets linked to Russian oligarchs, and uncover shell companies.

⁴⁵ <https://data.gov.lt/>

⁴⁶ <https://www.registrucentras.lt/>

* Geoportal.lt⁴⁷

A centralised GIS platform providing open geospatial data in line with the strict standards of the EU INSPIRE Directive. The datasets are available in Shapefile (.shp) and GeoPackage (.gpkg) formats. It provides precise cadastral boundaries of land parcels, ultra-high-resolution orthophoto maps, forest and water management layers, as well as historical topographic maps. These materials are used to cross-reference commercial satellite images with official cartographic data and to verify the boundaries of assets.



* Karštos Pėdos⁴⁸

A national transparency tool that functions as a database but also includes an integrated network map. It allows users to visualise overlaps between the interests of politicians, officials and businesses, with geographic links to specific companies or border hubs.

* Balticdisinfo.eu⁴⁹

An open platform for weekly monitoring of disinformation narratives in Lithuania, Latvia and Estonia, developed by the Civic Resilience Initiative. It publishes structured reports detailing the channels of dissemination, the origin of narratives, and links to Kremlin influence operations. Among the verified cases is documentation of a coordinated campaign in late 2025, when pro-Russian outlets systematically reframed Lithuanian language requirements for public servants as “total discrimination against Russian speakers,” while ignoring the security context behind the legislative changes.

⁴⁷ <https://www.geoportal.lt/geoportal/>

⁴⁸ <https://karstospedos.lt/en/home.html>

⁴⁹ <http://Balticdisinfo.eu>

Tools for financial intelligence and sanctions monitoring

* AMLYZE⁵⁰

Built by a team of leading experts and former regulators with experience at the Central Bank of Lithuania, the European Central Bank (ECB) and the Financial Crime Investigation Service (FNTT), the platform provides 24/7 transaction monitoring, customer risk scoring and screening of real-time payments. Its key feature is the Sanctions Screening Performance Test module, which uses a database of more than 50,000 controlled names to test banking systems for hidden errors in detection.

* Salv Bridge⁵¹

Developed by an Estonian-Lithuanian consortium of RegTech innovators and deployed in Lithuania with the participation of major fintech companies, the tool enables real-time data sharing across participants of the financial sector on suspicious profiles and indicators of money laundering, improving the detection of financial crime.

Computer vision models based on the NAS-MACU architecture⁵²

BPTI's own neural network algorithms. Instead of standard object recognition, the AI automatically adapts its parameters to a specific satellite, enabling it to identify military equipment (such as T-72 tanks or air defence systems) under challenging conditions like fog, cloud cover, battlefield smoke or deep shadows from trees.

Software for automated analysis of coherent changes⁵³

Developed by VILNIUS TECH, this system can quickly identify where heavy vehicles have moved and where new trenches or shelters have been dug, even after the equipment has left and the area has been concealed.

Інтеграційні екосистеми Data Fusion⁵⁴

Platforms developed with funding from the European Defence Fund. They automatically combine satellite data into a single digital layer, along with inputs from civilian maritime and airborne radars, tactical drones, and social media posts with geotags. This infrastructure also enables a joint AI “feedback loop” with Ukraine, where models are continuously improved using real battlefield experience.

⁵⁰ <https://amlyze.com/>

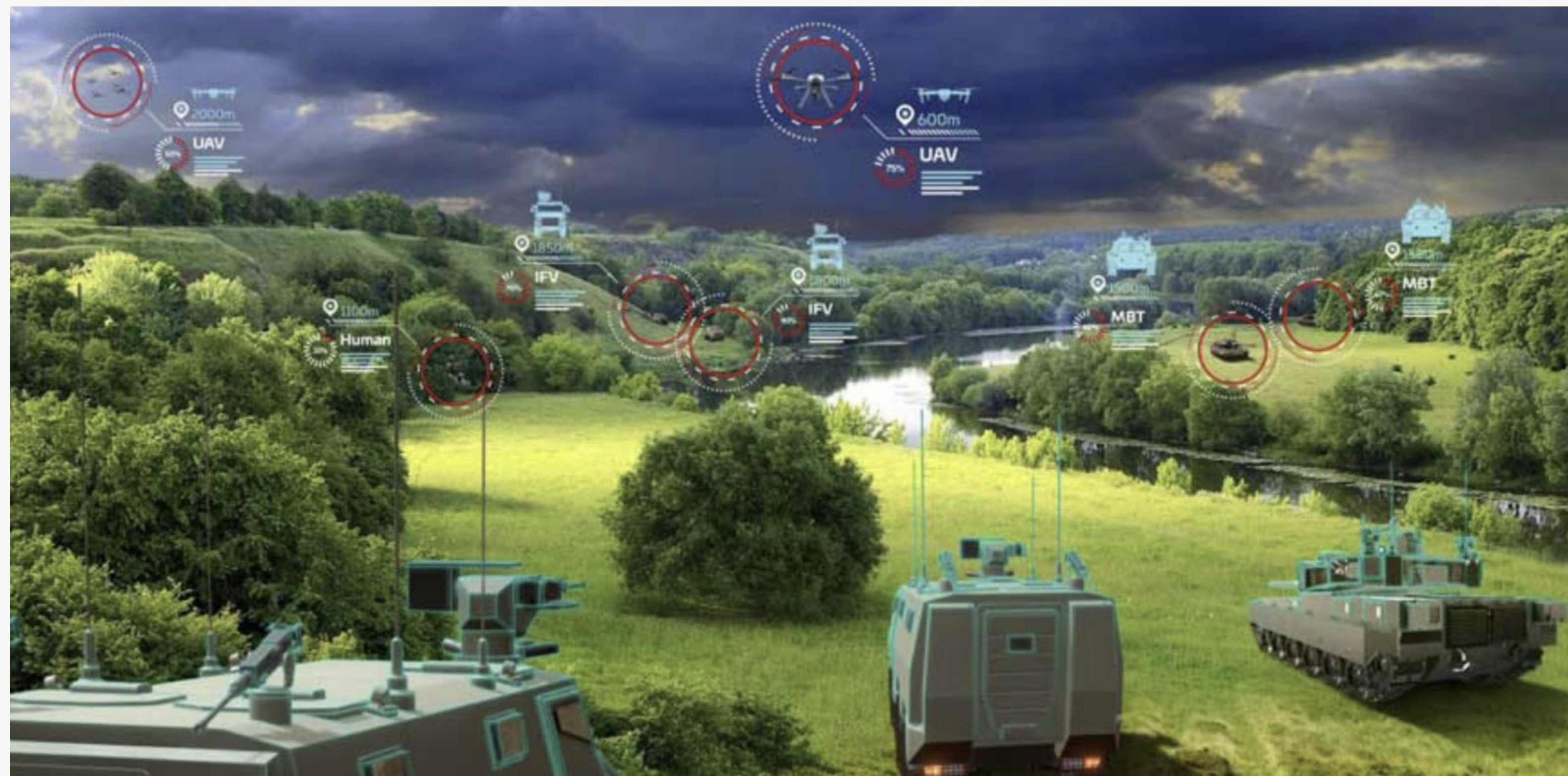
⁵¹ <https://salv.com/product/salv-bridge/>

⁵² <https://www.mdpi.com/2072-4292/15/1/91>

⁵³ Софт, який порівнює два радарні знімки однієї й тієї ж ділянки, зроблені в різний час, і автоматично підсвічує навіть найменші зміни на поверхні.

⁵⁴ <https://www.joint-forces.com/ew-and-cyber/72799-edf-funds-store-ai-assisted-optronics-project>

Ukraine provides up-to-date frontline data (such as radio signals, new camouflage techniques, or examples of Russian equipment) the AI has not previously seen. The system processes these materials, corrects recognition errors, updates the models, and returns improved versions of the software to analysts and military users.



3.3 Conditions for regulatory and commercial access and opportunities for Ukraine

As part of the development of a unified Lithuanian Open-Source Intelligence Centre and an innovation-focused defence hub in Kaunas, a two-tier cooperation model has been established, balancing NATO national security priorities with allied commitments to Ukraine.

Access to restricted volunteer-led and semi-commercial tools is carried out in accordance with clear security protocols. These set out how data is handled, ensure compliance with legal requirements, and reduce the risk of unauthorised access by hostile intelligence services.

Standardisation under Berkeley Protocol⁵⁵

Any civilian or military specialist granted access to data collection and processing tools (for example, Kiberšauliai scrapers or BPTI satellite modules) must complete certification in maintaining the “chain of custody” for evidence. Digital materials collected using the software may be formally used in international courts (ICC) or in United Nations reports.

Memoranda for security clearance:

Lithuania's OSINT architecture works closely with military intelligence and the State Security Department, and direct access to analytical data requires a tripartite memorandum (Government of Lithuania - NGO/Developer - Recipient). Access to military AI models requires Ukrainian situation centres to be verified through the Ministry of Defence.

Data protection regulations:

Civilian and journalistic platforms provide access to their OSINT dashboards subject to compliance with European cybersecurity standards.

⁵⁵ <https://www.law.berkeley.edu/research/berkeley-human-rights-center/programs/berkeley-protocol-on-digital-open-source-investigations/>

Users must complete two-factor authentication and verify their digital signature to help prevent leaks of logistical or personal data. The ecosystem's funding model is based on diversification: commercial users support development, while military and human rights missions are given priority access and free-of-charge support.

Consolidated commercial access matrix for Ukraine

Tool category	Commercial cost in the EU	Conditions for Ukraine's Armed Forces and Defence Forces	Conditions for Ukrainian NGO and media
Military AI and GEOINT (BPTI, VILNIUS TECH)	High (commercial contracts / EDF)	Free under a tech barter arrangement (Data Fusion Loop)	Not available (strict military restrictions)
Disinformation analytics (Debunk.org platform)	Under B2B / B2G subscription licensing	Free (direct government access)	Free (via BECID/EDMO grant quotas)
Logistics parsers and financial databases (Siena, Open Data)	Free (Open Source / CC BY 4.0)	Free (open-source on GitHub)	Free (OCCRP's joint investigations)

3.4 Detailed financial formats for Ukraine

“Joint R&D” format

The Armed Forces of Ukraine do not pay licensing fees for the use of intellectual property of Lithuanian institutions. Instead, the Ukrainian side provides real, verified frontline datasets. In practice, Ukraine's battlefield experience serves as a form of contribution in exchange for Lithuanian high-tech solutions, enabling the development of jointly built, world-class software products⁵⁶.

Grant-funded support for the civilian sector

For Ukrainian fact-checkers and investigative journalists, access to paid tools for automated monitoring of the information space is funded through European grant programmes.

The Lithuanian side covers the costs of server infrastructure and API integrations within the budgets of the European Digital Media Observatory (EDMO), BECID projects and Horizon Europe programmes.



⁵⁶ <https://thedefensepost.com/2024/11/05/ukraine-lithuania-unmanned-electronic-warfare/>

Chapter 4.

Analysis of cooperation between Ukraine and Lithuania

The most institutionalised form of Ukrainian-Lithuanian cooperation currently operates through formal international criminal justice mechanisms, most notably the Joint Investigation Team (JIT)⁵⁷, which was established under the auspices of Eurojust following Russia's full-scale invasion of Ukraine⁵⁸.



The JIT was set up in the first weeks following Russia's full-scale invasion to enable rapid coordination among countries investigating war crimes in parallel. It initially included Ukraine, Lithuania and Poland, with other European countries joining it over time.

The key advantage of the Joint Investigation Team lies in its ability to facilitate the direct exchange of criminal evidence. Investigators and prosecutors from different countries can share evidence, coordinate investigative activities, align their approaches to the legal qualification of crimes, and avoid duplicating efforts across multiple jurisdictions.

4.1 Security and intelligence level

A key instrument of Ukrainian-Lithuanian cooperation is the bilateral Security Cooperation Agreement signed in June 2024⁵⁹. It formally commits Lithuania to providing Ukraine each year with a fixed level of support for defence and security, amounting to no less than 0.25% of Lithuania's GDP.

In addition to the guaranteed financial and military-technical support, the agreement also establishes the legal and technical foundation for direct and deeper cooperation between the military intelligence services of both countries.

⁵⁷ <https://www.eurojust.europa.eu/judicial-cooperation/practitioners-networks/joint-investigation-teams-jits>

⁵⁸ <https://www.eurojust.europa.eu/news/eurojust-supports-joint-investigation-team-alleged-core-international-crimes-ukraine>

⁵⁹ <https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-91809>

4.2 Journalism and OSINT level

A clear example of cooperation between the countries is the “Mapping Russia’s War Machine” project⁶⁰ – a major international GEOINT investigation carried out by a consortium of journalists including Lithuania’s public broadcaster LRT, the VSquare network, Eesti Ekspress, Frontstory.pl, and the volunteer platform OSINT for Ukraine. Analysts mapped Russian military bases along NATO’s entire north-western border, from Murmansk to Kaliningrad.

4.3 Lithuania’s experience of cooperation with other countries

Baltic-Nordic cooperation

The Northern European and Baltic countries work closely together on security and technology through coordination between national cyber police units, CERT organisations, and European agencies such as Europol and ENISA.

Law enforcement agencies across the region also run regular practical workshops, such as the OSINT Workshop for Nordic and Baltic Countries⁶¹, to align digital forensic tools and improve cyber threat analysis.

In parallel, the countries have launched a major intergovernmental initiative, the Baltic AI Giga Factory⁶² – a project to develop AI computing hubs whose algorithms will support regional GEOINT operations, monitor satellite images along border areas, and enable automated language analysis for InfoSec.

Western Balkans and Georgia

Recognising that the Kremlin uses similar destabilisation tactics in other vulnerable parts of Europe, Lithuania has begun scaling its OSINT capabilities to the Western Balkans and the South Caucasus. The Debunk.org analytical hub is expanding⁶³ its regional counter-disinformation work through partner OSINT initiatives in these regions, bringing together local media and analytical organisations to jointly monitor information operations.

Lithuanian experts share their custom web scrapers with local civil society organisations and journalists, train them to build network graphs to expose “troll farms”, and introduce counter-narrative methodologies to help protect the local media space ahead of elections.

⁶⁰ <https://osintforukraine.com/publications/mapping-russias-war-machine>

⁶¹ <https://www.vp.gov.lv/en/article/state-police-strengthens-international-cooperation-field-digital-investigations>

⁶² <https://www.migam.ai/migam-ai-among-key-participants-of-the-baltic-ai-gigafactory-partner-assembly/>

⁶³ <https://debunk.org/projects/>



4.4 Challenges and barriers to cooperation

Structural barrier No. 1: Information isolation

Information isolation arises from differences in operational culture and technical incompatibility. Lithuanian GEOINT specialists may track the movement of a specific military unit using satellite images, Ukrainian OSINT volunteers may identify social media profiles linked to soldiers from that unit, and state investigative bodies may document the on-the-ground consequences of their actions. However, without a unified protocol, these datasets are not combined into a single evidentiary chain.

Each organisation uses its own standards for storing metadata and hashing video material. As a result, different groups of analysts often end up duplicating work on the same case (for example, an attack on a specific civilian site) without being aware of each other's findings. This creates an impression of high activity, while overall system efficiency remains low.

In the Lithuanian context, where OSINT is closely linked to the defence sector, excessive classification often becomes a barrier to cooperation with civilian investigators, even when the information comes entirely from open sources.

Structural barrier No. 2: Language barrier

The language barrier in Lithuanian-Ukrainian cooperation creates a clear divide between information and professional environments. Most Lithuanian organisations, including LRT Tyrejų Grupė, Patikrinta 15min and Debunk.org, primarily work in Lithuanian, so their investigations and analytical outputs are largely aimed at a domestic audience and remain available mostly within the country.

As a result, even important research on disinformation or security threats often does not reach Ukrainian partners without translation, which limits how effectively information can circulate between the communities.

Structural barrier No. 3: Financial instability in the civil society sector

Most private and non-governmental organisations at the core of Lithuania's transparency ecosystem (including independent fact-checking groups, investigative media outlets and volunteer OSINT teams) operate under ongoing financial strain. Unlike state security institutions, the civil society sector remains heavily reliant on short-term grants, donations and sponsorships.

The most damaging tool used to pressure independent investigators is so-called SLAPP lawsuits. This legal tactic sees large businesses, corrupt officials or covert pro-aggressor lobby groups target small NGOs and newsrooms with multimillion-euro defamation claims under the guise of "protecting honour and business reputation".

These cases can drain an organisation's resources for years, forcing analysts to divert funds from investigative work to costly legal defence.

4.5 Prospective areas for cooperation for 2026-2028

Direction 1: Investigating sanctions evasion

Lithuania serves as a key transit and compliance hub between Russia/Belarus and the EU internal market. As a result, it often becomes a jurisdiction where sanctions-evasion schemes are formally legitimised through re-exports, intermediary companies, and logistics chains broken up across multiple legal entities.

The adoption of Lithuania's national sanctions list in June 2025⁶⁴ adds an extra layer of screening on top of EU sanctions regimes, helping to more precisely flag local beneficiaries, logistics intermediaries and shell companies that may not appear on EU-wide lists but are still involved in transit schemes.



⁶⁴ <https://www.urm.lt/en/news/928/lithuanian-parliament-approved-amendments-to-the-law-enabling-lithuania-to-impose-national-individual-and-economic-sanctions-against-russia-and-belarus%3A44394>

The potential for cooperation between Lithuania's Siena and Ukrainian investigative teams lies in combining Lithuania's local regulatory visibility with OCCRP's international analytical infrastructure. This not only helps document individual cases of sanctions evasion, but also reconstruct full end-to-end networks, from beneficial owners to end users.

Direction 2: ICPA as a structural platform for OSINT

The International Centre for the Prosecution of the Crime of Aggression (ICPA) should be viewed as a layer of evidentiary infrastructure for future prosecutions, operating both as an investigative body and as a mechanism for ensuring that materials are procedurally admissible.

It can also act as a standards-setting body for evidentiary protocols, defining unified requirements for authenticating digital materials, time-stamping events, verifying geolocation, and maintaining the chain of custody. This would ensure that OSINT data can be used in international courts without losing its legal validity.

Direction 3: AI monitoring of narratives – scaling the model of Debunk.org

A practical extension of the Debunk.org model could move it from analytical monitoring towards a fully integrated, inter-institutional early warning system. This would involve a shared data exchange layer between Debunk.org and Ukrainian partners via secure APIs, feeding in content streams from social media, Telegram channels and news sources across the Baltic region.

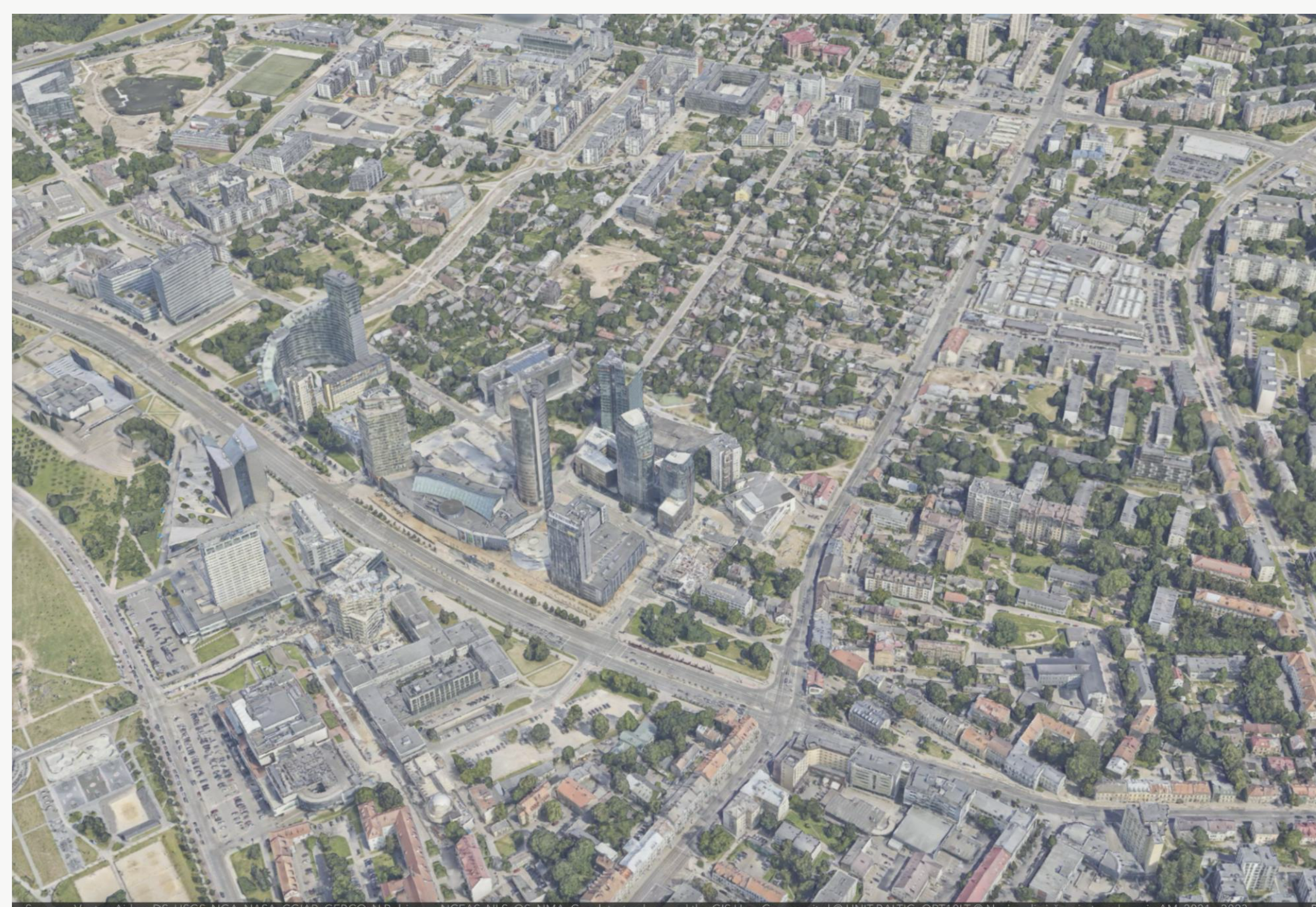
In practical terms, this could be complemented by trigger-based alerts for Ukrainian analytical centres and government bodies, so they receive not just reports, but real-time signals of sudden spikes or coordinated information campaigns. An important part of the setup would also be a shared data governance model that complies with GDPR and national restrictions, while still allowing the exchange of aggregated indicators and metadata without compromising privacy.

Direction 4: GEOINT – expanding the model of “Eyes on Russia”

The next step in developing the GEOINT model based on “Eyes on Russia” is moving from ad hoc OSINT analysis to a continuous, multi-source monitoring infrastructure.

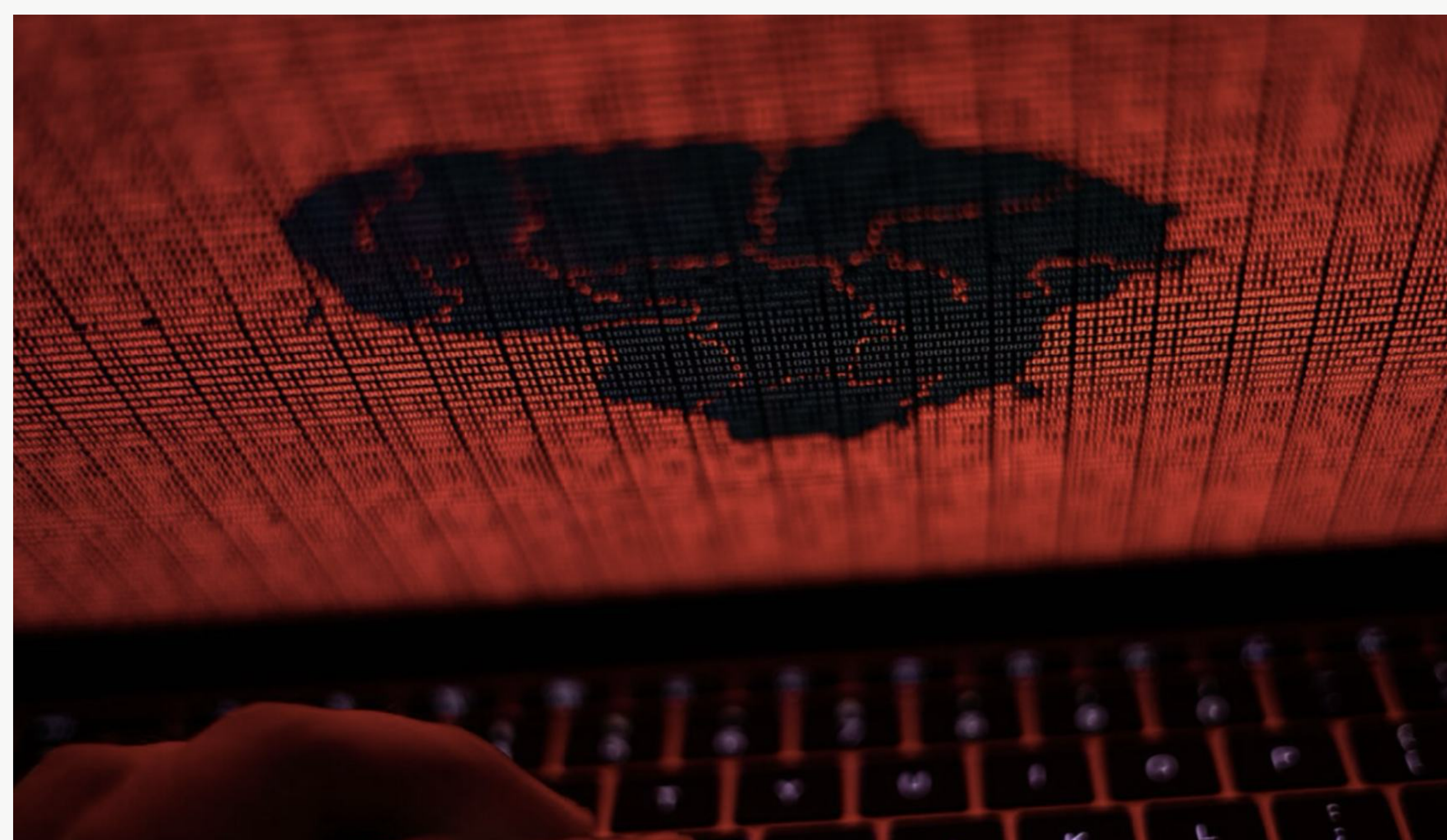
With the rapid growth of video and geospatial data, the key priority is standardising how it is processed: automatically integrating satellite images, geolocation analysis of videos, social media content and open registers into a single spatiotemporal model of events.

⁶⁴ <https://www.urm.lt/en/news/928/lithuanian-parliament-approved-amendments-to-the-law-enabling-lithuania-to-impose-national-individual-and-economic-sanctions-against-russia-and-belarus%3A44394>



Direction 5: Post-war transparency – the Karštos Pėdos model for Ukraine

The model of Karštos Pėdos transparency platform could be highly relevant for post-war Ukraine in the context of reconstruction and anti-corruption efforts. Media4Change and Siena have hands-on experience in building such systems, including defending them against regulatory pressure framed as GDPR compliance issues.



Methodology

The main objective of this analysis is to structure information on Lithuanian OSINT and analytical organisations and to help Ukrainian counterparts find relevant partners.

The study prioritises organisations that systematically work on investigations related to Russia and Belarus, as well as those with proven public track records in tracking military equipment, countering disinformation, or investigating economic crimes, including sanctions evasion.

The study is based on systemic, historical and comparative approaches. The systemic approach treats Lithuania's analytical ecosystem as a network of interconnected organisations and initiatives.

The historical approach examines how the sector has developed and the factors that have shaped it over time. The comparative approach is used to assess organisations across their areas of work, specialisations and modes of cooperation.

Data was collected through open-source intelligence (OSINT), including official websites of organisations, public reports, analytical publications, social media profiles, and mentions in specialised media.

To clarify and verify the information, interviews were conducted with representatives of selected organisations mentioned in the report. This selective approach was driven by time constraints during the author's field visit to Lithuania. Some organisations were identified only during meetings with sector representatives, which made it impossible to conduct additional interviews within the same trip. In addition, certain initiatives do not have permanent representatives or publicly available contact details. Given this, the interviews covered only part of the organisations, and the findings should be seen as a mapping of the ecosystem that can be further expanded through additional research and expanding the network of contacts.

The collected data were organised and categorised by organisation type, areas of activity, thematic focus, and potential for cooperation with Ukrainian partners. The sector was then visualised using an ecosystem mapping approach.