



# Мапування аналітичної екосистеми Литви





|                                                                       |           |
|-----------------------------------------------------------------------|-----------|
| <b>Вступ</b>                                                          | <b>3</b>  |
| <b>Розділ 1.</b>                                                      |           |
| <b>Екосистема аналітичного сектору Литви</b>                          | <b>4</b>  |
| 1.1 Державно-громадське партнерство                                   | 4         |
| 1.2 Правове поле та етика                                             | 4         |
| <b>Розділ 2.</b>                                                      |           |
| <b>Сегментоване мапування діяльності організацій</b>                  | <b>5</b>  |
| 2.1 Мілітарний OSINT та GEOINT                                        | 5         |
| 2.2 Протидія дезінформації та Infosec                                 | 11        |
| 2.3 Розслідування обходу санкцій та економічних злочинів              | 17        |
| 2.4 Розширений каталог                                                | 19        |
| <b>Розділ 3.</b>                                                      |           |
| <b>Литовські OSINT-інструменти</b>                                    | <b>22</b> |
| 3.1 Спеціалізовані боти та парсери волонтерського сектору             | 22        |
| 3.2 Публічні ліцензії та Open Source                                  | 22        |
| 3.3 Регламентні та комерційні умови доступу та можливості для України | 25        |
| 3.4 Деталізація фінансових форматів для України                       | 27        |
| <b>Розділ 4.</b>                                                      |           |
| <b>Аналіз співпраці: Україна та Литва</b>                             | <b>28</b> |
| 4.1 Безпековий та розвідувальний рівень                               | 28        |
| 4.2 Журналістський та OSINT-рівень                                    | 29        |
| 4.3 Досвід співпраці Литви з іншими країнами                          | 29        |
| 4.4 Виклики та бар'єри                                                | 30        |
| 4.5 Перспективні напрямки співпраці на 2026-2028                      | 31        |
| <b>Методологія аналізу</b>                                            | <b>33</b> |



## Вступ

Литва, країна з населенням близько 2,8 мільйона осіб<sup>1</sup>, ілюструє, як суспільство розбудовує системний захист від зовнішніх інформаційних загроз. Геополітичне розташування поруч із Росією та Білоруссю формує чіткий фокус для місцевих OSINT-спільнот та організацій: моніторинг гібридних загроз у реальному часі, відстеження тіньових схем обходу санкцій, блокування дезінформації тощо.

Повномасштабне вторгнення Росії в Україну у 2022 році мало значний вплив на вектор розвитку для литовських дослідників. Вони перерозподілили свої ресурси, почали переймати український досвід оборони та розгортати масштабні розслідування про фінансові потоки, що живлять Росію.

Розвідка на основі відкритих даних (OSINT) у Литві не є виключною компетенцією спецслужб та журналістів. Тут вона працює на широку мережу взаємодії між державою та громадянським суспільством.

Наразі ключову роль в дослідженнях відіграють незалежні аналітичні центри, команди журналістів-розслідувачів та волонтерські рухи. Їхній досвід вже активно впроваджується і в сусідніх країнах.

Документ охоплює 14 структур, що формують литовську OSINT-екосистему станом на 2024-2026 роки. Дослідження побудоване за чотирма функціональними напрямками, кожен із яких має власний інструментарій, джерела даних і кінцевого споживача аналітики: мілітарний OSINT та геопросторова розвідка, протидія дезінформації та інформаційна безпека, розслідування обходу санкцій, а також стратегічний OSINT.

Потреба в дослідженні виникла через нестачу систематизованого огляду литовської OSINT-спільноти в україномовному просторі. Розрізнені згадки про окремі організації існують, але без єдиної логічної структури. Документ заповнює цю прогалину як практичний орієнтир та аналізує потенційних литовських партнерів, деталізує нішу їхньої діяльності та шукає способи для масштабування співпраці.

**Звіт підготовлено за підтримки громадської організації "Terrecon".**

### Авторки:

Дар'я Вербицька, CEO Terrecon.

Катерина Саєнко, OSINT-аналітикиня ГО "Terrecon".

### Консультантка:

Євгенія Федотова, віце-президентка ГО "Ліберально-демократична ліга України".

---

<sup>1</sup> [https://european-union.europa.eu/principles-countries-history/eu-countries/lithuania\\_en](https://european-union.europa.eu/principles-countries-history/eu-countries/lithuania_en)



## Розділ 1.

### Екосистема аналітичного сектору Литви

#### 1.1 Державно-громадське партнерство

У литовському контексті державні органи, такі як Міністерство національної оборони, Департамент стратегічних комунікацій Збройних сил (далі – СтратКом) та спецслужби, розглядають цивільних розслідувачів не як сторонніх спостерігачів, а як «цивільне крило» розвідки.

З 2023 року Національний центр управління кризами є ключовою установою, що координує реагування на ворожі інформаційні операції. До цієї системи також входить Департамент стратегічних комунікацій Збройних сил Литви (СтратКом) разом із ще десятима установами, а за потреби – й іншими, залежно від характеру загрози.

Особлива роль у цій екосистемі належить Департаменту стратегічних комунікацій (далі – СтратКом) Литовської армії, який координує протидію інформаційним операціям агресора. Ця взаємодія є двосторонньою<sup>2</sup>: наприклад, волонтерські мережі (на зразок «литовських ельфів») та аналітичні центри (такі як Debunk.org) роблять первинний моніторинг ворожих наративів, а військові структури, зі свого боку, аналізують ці дані в ширшому контексті безпеки, верифікують загрози та використовують отримані висновки для інформування суспільства й ухвалення оборонних рішень.

Співпраця зі спецслужбами, зокрема з Департаментом державної безпеки, має більш закритий, але не менш ефективний характер, особливо у сферах економічної розвідки та моніторингу обходу санкцій.

#### 1.2 Правове поле та етика

Діяльність литовських OSINT-розслідувачів розгортається у межах правового поля Європейського Союзу, де важливим регулятором виступає Загальний регламент про захист даних (далі – GDPR<sup>3</sup>). Впровадження цього регламенту суттєво трансформувало методику роботи з відкритою інформацією, змусивши аналітиків балансувати між суспільною значущістю розслідування та правом особи на приватність. У литовському контексті GDPR вимагає від кожної організації чіткого етичного обґрунтування збору та зберігання персональних даних. Це призвело до росту сектору, де розслідувачі приділяють особливу увагу легітимності джерел та дотриманню процедур анонімізації, щоб уникнути юридичних претензій, які можуть підірвати довіру до всієї OSINT-сфери.

Впровадження директиви про кібербезпеку NIS 2<sup>4</sup> стало ключовим фактором, що змінив роботу литовських технологічних організацій. Тепер організації, які надають послуги з моніторингу загроз або аналізу даних для державного сектору, класифікуються як суб'єкти, що мають відповідати підвищеним стандартам кібербезпеки.

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

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

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



Це означає обов'язковий аудит систем зберігання даних, протоколи звітності про інциденти та перевірку ланцюжків постачання софту.

**Розділ 2.**  
**Сегментоване мапування діяльності організацій**

Литовські OSINT-організації можна поділити на три сегменти діяльності з різними методами збору інформації:

| Сегмент                                       | Що роблять / Хто споживає                                                                                   |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Мілітарний OSINT / GEOINT                     | Аналіз бойових дій, переміщення техніки, супутникові знімки.<br>Споживачі: МО Литви, НАТО, аналітики.       |
| Протидія дезінформації                        | Моніторинг наративів, виявлення ботоферм, фактчекінг.<br>Споживачі: медіа, держструктури, широка аудиторія. |
| Дослідження обходу санкцій та фінансових схем | Розслідування ланцюгів постачання, тіньових схем.<br>Споживачі: митниця, прокуратура, журналісти.           |

**2.1 Мілітарний OSINT та GEOINT**

Цей найбільш закритий сегмент розвідки з відкритих джерел формується навколо ветеранів, колишніх офіцерів, фахівців-спецпризначенців та державних структур.

Технологічний фундамент оборонних ініціатив значною мірою спирається на використання комерційної супутникової розвідки. Регіональний аналіз дедалі частіше базується на високоточних знімках від провайдерів рівня Planet або Maxar – завдяки цьому будівництво військових об'єктів у Білорусі та переміщення техніки вздовж Сувальського коридору фіксуються в режимі реального часу.

Окреме місце в аналітичній архітектурі країни посідає її державний безпековий сегмент, який функціонує як закритий простір. Попри високу засекреченість та обмежений публічний доступ, саме ці інституції визначають ключові вектори розвитку для всього цивільного OSINT-середовища, виступаючи його головними бенефіціарами та кінцевими споживачами.

Другий департамент оперативних служб при Міністерстві національної оборони (далі – AOTD<sup>5</sup>) є правонаступником розвідувальних традицій міжвоєнної Литви, хоча в сучасному вигляді він був відновлений у 1990 році. Сфера його діяльності зосереджена на військовій розвідці та контррозвідці, де особлива увага приділяється мілітарному аналізу потенціалу агресора.

Департамент державної безпеки (далі – VSD<sup>6</sup>) виконує роль головної цивільної спецслужби Литви, фокусуючись на ширшому спектрі викликів, що охоплюють економічну безпеку, контррозвідку та захист конституційного ладу.

<sup>5</sup> <https://www.aotd.lt/>

<sup>6</sup> <https://www.vsd.lt/>



Сфера інтересів VSD включає моніторинг іноземних інвестицій у взаємодії зі стратегічними об'єктами, боротьбу з тероризмом, а також протидію дезінформаційним операціям, що загрожують суспільній стабільності.

Обидві структури щороку випускають спільний документ «Оцінка загроз національній безпеці», який є ключовим матеріалом для всіх організацій, що працюють у векторі національної безпеки. Цей звіт фактично легітимізує напрямки роботи для цивільних розслідувачів, вказуючи на найбільш вразливі сектори та пріоритетні географічні напрямки.

#### Організації:

##### **Lietuvos šaulių sąjunga (Спілка стрільців Литви)**



Організація об'єднує близько 17 тисяч осіб. Її учасники – цивільні фахівці з ІТ, лінгвістики та аналізу даних, які застосовують свої професійні компетенції для виконання завдань військової розвідки в системі територіальної оборони.

Організацією очолює військовий – полковник Лінас Ідзеліс<sup>7</sup>.



“Стрільці” діють у межах спеціалізованих підрозділів інформаційного опору. Основний фокус їхньої розвідки з відкритих джерел розподілений між двома ключовими напрямками: інформаційними операціями (InfoSec) та геопросторовій аналітиці (GEOINT) разом із розвідкою за допомогою безпілотників.

У сфері мілітарного OSINT та GEOINT спеціалізовані загони стрільців аналізують комерційні супутникові знімки, інтегрують дані з відкритих картографічних сервісів та координують роботу цивільних операторів БПЛА для підготовки тактичних звітів на користь регулярних Збройних сил.

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



Спілка стрільців спільно з Департаментом мобілізації навчає мешканців прикордонних районів (зокрема навколо Сувалкського коридору) базовим навичкам OSINT і GEOINT. Цивільних громадян навчають верифікувати автентичність фотографій, фіксувати геолокацію підозрілих об'єктів та повідомляти про аномальну активність або переміщення техніки біля кордонів через захищені державні канали.

**Кейси:**

**Кіберпiгрознiк Lizdeika<sup>8</sup>**



Внутрішня кібер- та технологічна команда, яка створює навчальні цифрові середовища для тренування в умовах, максимально наближених до реальних загроз. У “віртуальних полігонах” учасники відпрацьовують реагування на інциденти, роботу з цифровими слідами та елементи OSINT-аналізу в умовах змодельованих інформаційних атак. Платформа інтегрує практичні модулі з кіберзахисту, дрон-розвідки та аналізу даних, формуючи замкнене тренувальне середовище, яке використовується для підготовки до гібридних загроз і координації з оборонними структурами Литви.

**Locked N' Loaded**



Литовський цивільний центр аналізу оборони та безпеки офіційно зареєстрований як неурядова організація у Вільнюсі. Керівником платформи є Паулюс Стоніс<sup>9</sup>.



<sup>8</sup> <https://lizdeika.education/en/>

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



Головним інформаційним майданчиком організації є сайт [parakomanai.lt](http://parakomanai.lt), де публікуються ґрунтовні тактичні аналізи, а основною мовою комунікації є литовська. Проект орієнтований на військовослужбовців, призовників та цивільних громадян, які прагнуть розуміти реальний стан безпеки в Балтійському регіоні та логіку бойових дій в Україні.

Аналітичне ядро Locked N' Loaded складається з ветеранів збройних сил та експертів із багаторічним досвідом служби. Головна місія команди полягає в тому, щоб перекладати складні військові процеси на зрозумілу мову практичних висновків. Організація надає конкретні тактичні розбори на основі GEOINT, верифікації супутникових знімків та детального аналізу відкритих джерел. Команда оцінює переміщення техніки РФ, зміни у штурмовій тактиці росіян та вивчає російські військові операції безпосередньо в зоні бойових дій в Україні для формування уроків оборони для самої Литви.

Окрім щоденного моніторингу фронту, Locked N' Loaded розробляє спеціалізовані навчальні програми для державного та приватного секторів. Свою високу мобільність та готовність ділитися досвідом команда безпосередньо підтвердила участю в ролі спікерів на Міжнародному форумі оборонних технологій KITE 2025<sup>10</sup> у Києві. У межах цієї спеціалізованої конференції, присвяченої інноваціям у сфері безпеки та розвідки, литовські аналітики презентували власні методики GEOINT-моніторингу та тактичного аналізу переміщення ворожих сил.

#### Кейси:

##### Проведення настільних військових ігор<sup>11</sup>

У цих симуляціях експерти центру виступатимуть у ролі умовного агресора, використовуючи реальну військову доктрину, штабну логіку та тактичні шаблони армій Росії чи Білорусі. Учасники гри – цивільні посадовці, керівники підприємств критичної інфраструктури або представники Спілки стрільців – мають реагувати на кризові сценарії в режимі реального часу.



<sup>10</sup> <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/>

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

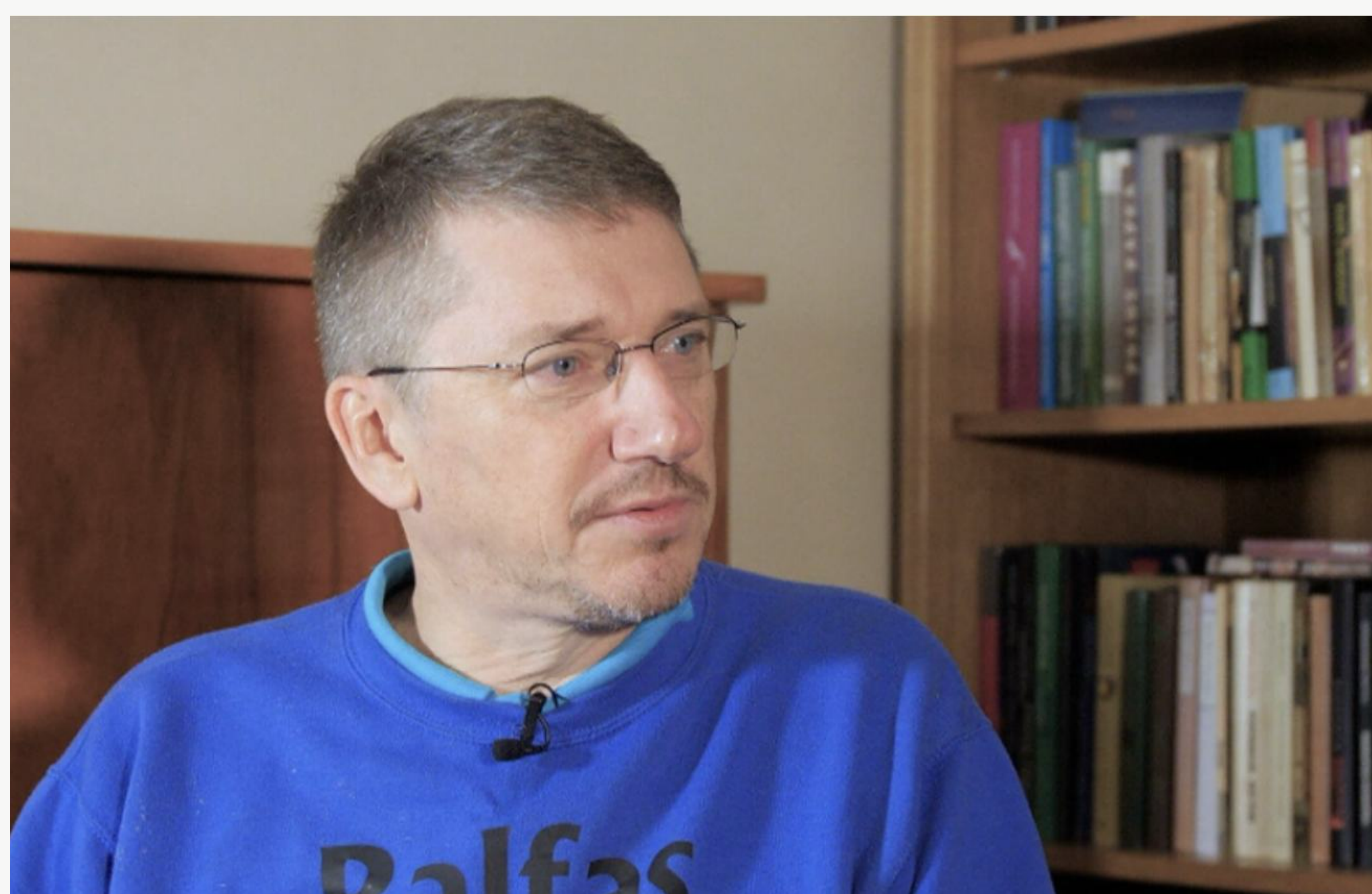


У професійному плані Locked N' Loaded має міжнародну репутацію: центр є офіційним членом Королівського інституту оборонних досліджень (RUSI) у Великій Британії та Литовської асоціації оборонної та безпекової промисловості. Команда тісно співпрацює з Центром досліджень Східної Європи (EESC) та Ініціативою громадянської стійкості (CRI).

## VISA



Агентство суспільної інформаційної безпеки діє як спеціалізований аналітичний центр під керівництвом Міндаугаса Сєюнаса<sup>12</sup>.



Діяльність агенції максимально інтегрована у процеси аналізу реальних безпекових викликів і загроз Балтійського регіону.

Головна спеціалізація агентства VISA полягає у роботі зі складними методами GEOINTу та системній оцінці воєнних і гібридних загроз. Команда аналітиків зосереджена на зборі та верифікації даних із відкритих і комерційних супутникових джерел. Фахівці детально відстежують логістичні ланцюжки, динаміку переміщення техніки та будівництво військової інфраструктури на кордонах.

Ключова особливість моделі роботи VISA – її непублічний характер та пряма співпраця з державним сектором. На відміну від організацій, що створюють контент для широкого загалу або журналістських розслідувань, агенція орієнтується на закритий формат взаємодії.

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



## **BPTI & Digital Defense Competence Centre**



Балтійський інститут передових технологій спільно з Центром компетенцій цифрової оборони утворюють технологічне партнерство, яке спеціалізується на дослідженнях та розробках у сфері алгоритмічної війни та розвідки. Центр розробляє складні математичні методи та ШІ-моделі, здатні автоматично аналізувати величезні масиви геопросторової інформації. Засновником і директором інституту є Томас Жаландаускас<sup>13</sup>.



Головна спеціалізація команд у контексті GEOINT:

- \* автоматизація розпізнавання об'єктів на супутникових знімках та обробка складних сигналів;
- \* створення алгоритмів комп'ютерного зору, які здатні самостійно ідентифікувати військову техніку, знаходити приховані лінії фортифікацій, оцінювати руйнування інфраструктури та відстежувати зміни в логістичних ланцюжках;
- \* розвиток роботи ШІ в умовах радіоелектронних перешкод противника, щільної хмарності або задимлення поля бою.

### **Кейси**

#### **Впровадження систем аналізу критичної інфраструктури на основі SAR-знімків**

В аналітичних проєктах BPTI застосовуються радарні супутникові дані із синтезованою апертурою (SAR) для моніторингу стану залізничної, логістичної та енергетичної інфраструктури. Команда виявляє зміни в інфраструктурних об'єктах, незалежно від погодних умов і часу доби, моделює навантаження на транспортні коридори й аналізує проблемні ділянки у критичних логістичних ланцюгах.

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



ВРТІ є ключовим представником Литви у програмах Європейського оборонного фонду. Інститут входить до складу консорціуму проєкту ARMADA<sup>14</sup>, який фінансується Європейським оборонним агентством. У межах цього проєкту литовські фахівці розробляють дорожню карту та алгоритми застосування штучного інтелекту в системах автоматичного аналізу даних спостереження Землі.

## 2.2 Протигія дезінформації та Infosec

### Civic Resilience Initiative (CRI)



Литовська громадська організація Civic Resilience Initiative (CRI), заснована у 2018 році експертами з безпеки Лінасом Скіріусом, Лукасом Андрюкайтисом<sup>15</sup> та Томасом Казуленасом<sup>16</sup>, створює інформаційне середовище для протидії інформаційним загрозам.



Організація розвиває напрями гейміфікованого навчання для молоді, OSINT-розслідувань та безпекових заходів. Стосовно останнього напрямку, CRI займає проактивну позицію щодо вивчення українського досвіду для оборонної стратегії Балтії та НАТО. Вони щорічно збирають у Вільнюсі понад 500 військових, експертів та журналістів на міжнародній конференції «Defending Baltics: War Lessons from Ukraine»<sup>17</sup>.

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

<sup>15</sup> <https://x.com/LAndriukaitis>

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

<sup>17</sup> [Defending Baltics: War Lessons from Ukraine](#)





Команда має успішні кейси блокування шкідливих матеріалів, проте взаємодія з глобальними платформами є проблематичною. Запити на видалення токсичного контенту з боку Google часто ігноруються. Аналітики пов'язують це зі зміною внутрішньої політики корпорації на тлі політичних змін у США.

У своїй роботі аналітики не використовують єдиного універсального софту, проте для моніторингу соціальних медіа та аналізу великих масивів відеоконтенту активно рекомендують литовську платформу RepSense<sup>18</sup>, яка вміє розпізнавати емоційне забарвлення даних.

У співпраці з державою CRI переважно працює через грантові та конкурсні програми у сфері медіаграмотності. Представники організації повідомили, що команда CRI самостійно розробляє проєктні ідеї та пропонує їх державним інституціям, а не виконує прямі урядові замовлення.

Під час інтерв'ю представники організації підкреслили ключові тенденції у сфері їхньої роботи – зростання використання штучного інтелекту в інформаційному середовищі. Водночас значна частина кампаній впливу досі здійснюється традиційними методами. Окремим викликом залишається застосування ботомереж, зокрема пов'язаних із російськими інформаційними операціями. Розвиток генеративних технологій ускладнює розпізнавання автоматизованого контенту через високий рівень персоналізації. Також співрозмовники звертають увагу на нестачу досліджень, присвячених ботомережам та маніпуляціям в інформаційному просторі Литви.

### Співпраця з українськими колегами

Співрозмовники насамперед зацікавлені у пошуку партнерів для освітніх проєктів, спрямованих на розвиток стійкості молоді до інформаційних загроз. Особливий інтерес викликають ігрові формати навчання, досвід українських OSINT-організацій у роботі з російським і білоруським контентом, а також залучення профільних українських експертів до освітніх та публічних заходів.

<sup>18</sup> <https://repsense.io/>



Проте партнерство з українськими організаціями періодично може ускладнюватись. Головною проблемою часто є саме верифікація локальних OSINT-спільнот. Одна з причин – відсутність якісного довідника чи реєстру, на який можна було б спиратися для перевірки надійності партнерів, їхньої фінансової стабільності та захисту від потенційного шахрайства. Крім того, CRI відзначають й інші виклики, наприклад мовні труднощі, а саме брак знань англійської мови для прямої комунікації або ж часті розбіжності в бюджетуванні через завищені ставки в українських проєктних заявках.

## Кейси

### GEOINT-квести для школярів

CRI розробила кілька ігрових форматів протидії дезінформації: від вуличних AR-ігор (учні шукають дезінформацію у реальному місті зі смартфонами) до відеогри з «фейковим експертом», де гравці мають виявити та спростувати неправдиві твердження<sup>19</sup>.

Основним успішним проєктом CRI є GEOINT-квест<sup>20</sup> у Вільнюсі, який збирає близько тисячі школярів та студентів. Учасники змагаються між школами та виконують завдання на спеціальних локаціях, до яких обов'язково залучають військових із контингенту НАТО.

На окремій платформі працює пілотний проєкт у п'яти школах – це спеціальний чат-бот із технологією штучного інтелекту, який допомагає школярам самостійно проводити розслідування, вказує на логічні помилки та спрямовує їхній аналіз.

### “Литовські ельфи”

Рух зародився у 2014 році як відповідь на російську агресію проти України та пов'язану з нею інформаційну війну. Спочатку рух був групою з 20 ентузіастів, а до 2022 року «Ельфи» масштабувалися у міжнародну мережу, що налічує близько 22 000 волонтерів у 13 країнах Центральної та Східної Європи.



<sup>19</sup> Kaip interaktyvus kompiuterinis žaidimas „Dezinformacijos Medžioklė“ ugdo kritinį mąstymą ir atsparumą dezinformacijai?

<sup>20</sup> Disinformation Challenge



Головна місія руху полягає у протидії дезінформації через моніторинг коментарів, виявлення ботоферм та поширення контрнарративів для захисту пересічних користувачів від пропаганди. У своїй методології волонтери фокусуються на фактчекінгу та деанонімізації тролів, повністю уникаючи інструментів кібершпигунства чи хакінгу. Через високі безпекові ризики учасники руху ретельно приховують свої особисті дані, діючи як закрита й анонімна експертна спільнота.

«Ельфи» перетворилися на джерело експертизи для міжнародних безпекових інституцій, включаючи Центр стратегічних комунікацій НАТО у Ризі. Волонтерські групи доповнюють існуючі структури НАТО та ЄС, посилюючи зв'язки між державними органами та активним громадянським суспільством.

Рух інтегрований із аналітичною платформою Debunk.org<sup>21</sup>, яка виконує роль OSINT-центру для аналізу дезінформації. Волонтери працюють над збором та первинним виявленням підозрілих інформаційних кампаній у соцмережах. Сам рух “Elves” також прямо визначається як волонтерська спільнота, яка співпрацює з Debunk.org у виявленні та протидії дезінформації.

Створена у 2018 році Elves Academy стала міжнародним майданчиком для підготовки сотень фахівців із боротьби з гібридними загрозами, що сприяє уніфікації OSINT-методик у межах Альянсу.

## Кейси

### Кампанія «Bust-AD»<sup>22</sup>

Операція стала відповіддю на появу генеративного ШІ, який проросійські хакери та фінансові шахраї почали використовувати для обходу модерації Facebook та Instagram. Волонтери виявили, що за рік (з вересня 2023 по вересень 2024) ця шкідлива реклама встигла охопити майже 6 мільйонів користувачів у Європі. «Ельфи» довели зв'язок кампанії з російськими серверами та передала зібрані докази безпосередньо представникам Meta, що змусило платформу заблокувати сотні рекламних кабінетів шахраїв.

### Debunk.org



Технологічна та аналітична структура, що поєднує автоматизований ШІ-моніторинг з мережею волонтерів-аналітиків, відомих під назвою «ельфи».

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

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



Організація виросла з платформи Demaskuok, яку заснував найбільший балтійський новинний портал Delfi.

Debunk.org моніторить понад 2 500 веб-доменів на 26 мовах, обробляючи близько 30 000 статей щодня<sup>23</sup>. Власна платформа DebunkReach вимірює охоплення кожного дезінформаційного матеріалу з урахуванням зворотних посилань і взаємодій у соцмережах<sup>24</sup>.

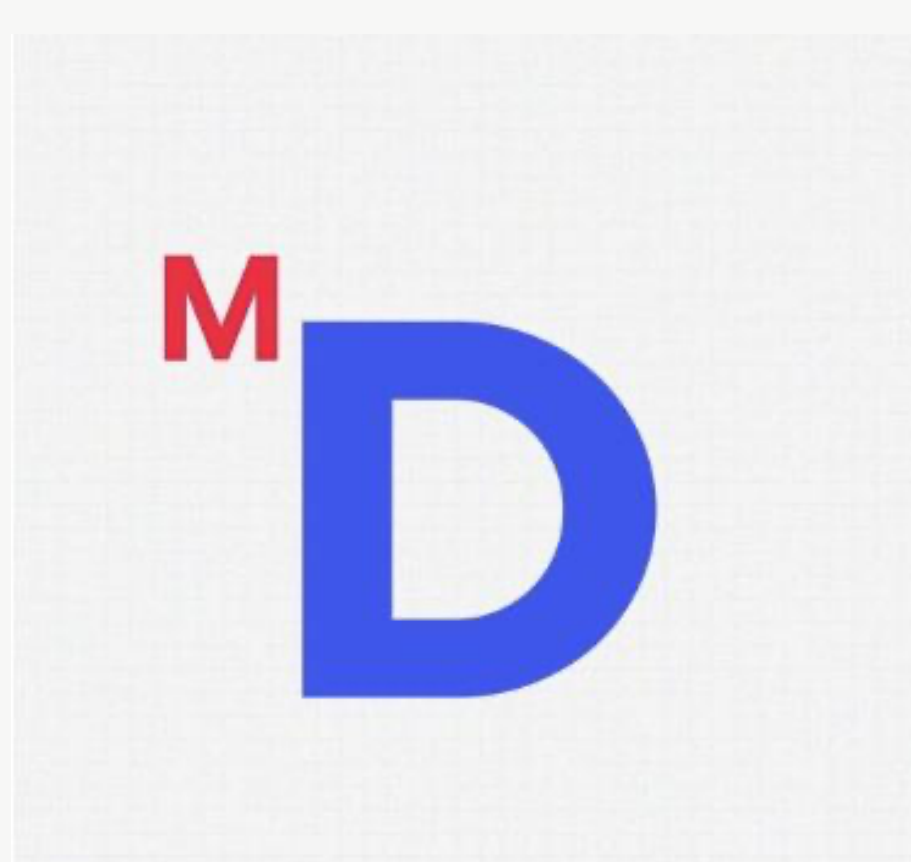
Організація систематично публікує щотижневі та щомісячні огляди дезінформаційного ландшафту Балтійських держав з фокусом на наративах, що дискредитують воєнну допомогу Україні, поширюють «антисанкційні» меседжі та формують образ «непотрібної» підтримки. Публікація таких оглядів є цінним відкритим ресурсом для партнерів, що досліджують кремлівський вплив у Центрально-Східній Європі.

### **Білоруський «силовий контент» на X<sup>26</sup>**

Аналіз поширення контенту білоруських силових структур через мережу акаунтів на платформі X. Розслідування показало механізми координованого підсилення інформаційного впливу з боку Білорусі, орієнтованого проти литовського суспільства та підтримки України.

### **Мегійні ініціативи**

#### **DELFI Melagių Detektorius**



Запущений у 2018 році редакторкою Аїсте Мейдуте, проєкт інтегрований в новинну екосистему литовського мовника Delfi.



<sup>23</sup> [https://books.google.se/books?id=wD-MEAAAQBAJ&redir\\_esc=y](https://books.google.se/books?id=wD-MEAAAQBAJ&redir_esc=y)

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

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

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



Він допомагає спростовувати дезінформацію в момент її появи. Матеріали випускають трьома мовами: литовською, польською та російською. Такий фокус на національних меншинах допомагає захистити вразливі групи від зовнішнього впливу та підтримувати єдність у суспільстві.

Теми розборів варіюються від дезінформації про здоров'я до складних російських геополітичних наративів. Проєкт офіційно сертифікований Міжнародною та Європейською мережами фактчекінгу.

У своїй роботі «Детектор брехні» використовує OSINT-інструментарій для верифікації візуального контенту, виявлення маніпулятивних монтажів та відстеження походження фейкових новин через метадані та цифрові сліди.

Над проєктом працюють професійні журналісти-розслідувачі, які займаються дослідженням складних інформаційних операцій. Проєкт також співпрацює з технологічними партнерами, зокрема Debunk.org. Їхні інструменти допомагають виявляти підозрілий контент ще на початкових етапах його поширення.

#### Кейси

##### Розвінчання фейку про “план НАТО та Європи окупувати Молдову”<sup>27</sup>

Перед важливими виборами в Молдові російська Служба зовнішньої розвідки запустила через мережу ботів та прокремлівські акаунти в Литві масштабний вкид. Аналітики розібрали першоджерела маніпуляції та довели, що російська розвідка повністю перекурила інформацію про планові оборонні навчання НАТО.

#### Media4Change



Міжнародний рух, що об'єднує понад 640<sup>28</sup> журналістів, експертів та громадських представників з різних країн.

Заснована Нерінгою Юрчюконіте<sup>29</sup>, організація зосереджена на трьох взаємопов'язаних напрямках: правах людини, розслідувальній журналістиці та медіаграмотності.

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

<sup>28</sup> <https://www.media4change.co/>

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





Вона є координаційним хабом для багатьох ініціатив, серед яких open-data платформа Karštos Pėdos. Упродовж шести років команда проаналізувала понад 143 000 матеріалів про стигматизовані групи в литовських медіа. Організація провела понад 200 навчальних сесій для журналістів, майбутніх журналістів та педагогів-волонтерів<sup>30</sup>.

Media4Change активно бере участь в аналізі висвітлення України у литовських та балтійських медіа, документуванні антиукраїнської риторики та розробці контрнарративів.

## Кейси

### Створення та еволюція екосистеми відкритих даних „Karštos Pėdos“<sup>31</sup>

Media4Change виступила координатором розробки інтерактивної платформи відкритих даних. Інструмент став базовою платформою для проведення розслідувань для великих національних медіа та для регіональних репортерів.

## 2.3 Розслідування обходу санкцій та економічних злочинів

### Siena



Заснована у 2019 році журналістами Шарунасом Черняускасом<sup>32</sup> і Мігле Кранцевічюте<sup>33</sup>, організація публікує одне велике розслідування на місяць.

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

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

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

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





Робота Siena охоплює обхід міжнародних санкцій, корупцію у публічному секторі, нецільове використання коштів ЄС, фінансові злочини та кримінальні мережі, пов'язані з Росією та Білоруссю.

Після 2022 року переорієнтувала значну частину своєї операційної потужності на відстеження обходу санкцій – схем, через які гроші та товари продовжують надходити на підтримку російської воєнної економіки. За даними самої організації, розслідування, опубліковані після повномасштабного вторгнення, безпосередньо призвели до накладення штрафів і заморозки активів на суму понад 12 мільйонів євро, а також до демонтажу контрабандних мереж<sup>34</sup>.

Siena є офіційним партнером OCCRP – міжнародної організації, що об'єднує журналістів-розслідувачів з багатьох країн світу. Цей статус відкриває команді доступ до глобальних баз даних для проведення міжнародних розслідувань разом із сотнею інших редакцій у понад 60 держав.

## Кейси

### Криптовалютні потоки до ПВК “Вагнер” та ДШРГ “Русич”<sup>35</sup>

У межах міжнародного розслідування Siena документувала, як російське приватне воєнне угруповання «Русич», відповідальне за воєнні злочини в Україні, залучало сотні тисяч євро через криптовалютні пожертви через балтійські компанії. Розслідування встановило зв'язки між естонськими та литовськими криптофірмами та Ощадбанком Росії.

### LRT Tyrimų skyrius



<sup>34</sup> <https://www.siena.lt/>

<sup>35</sup> [vsquare.org/tales-from-the-crypto-money-laundering-fraud-sanctions-estonia-lithuania-russia/](https://vsquare.org/tales-from-the-crypto-money-laundering-fraud-sanctions-estonia-lithuania-russia/)



Розслідувальна команда LRT є журналістським підрозділом національного мовника. Як окремий спеціалізований напрям розслідувальної журналістики вона сформувався у 2018 році. Підрозділ очолює Індре Макарятіте<sup>36</sup>.



Основним операційним фокусом команди є національна безпека у найширшому сенсі. Вони спеціалізуються на викритті схем обходу європейських санкцій проти РФ та РБ, мапуванні російського бізнес-впливу в Балтійському регіоні та деконструкції юридичних диверсій, які кремлівська агентура намагається реалізувати всередині Литви. Більшість матеріалів виходить литовською мовою, що зумовлено фокусом на внутрішнього глядача, проте ключові розслідування перекладаються англійською та російською для міжнародного резонансу.

#### Кейси

##### **Схема «Казахстанського та Киргизького експресу» (Обхід санкцій через Центральну Азію)<sup>37</sup>**

Серія міжнародних розслідувань, де команда аналізувала митні бази даних, транспортні накладні та реєстри європейських компаній після введення жорстких санкцій проти білоруської деревини та російських нафтопродуктів. Команда довела, що під виглядом товарів із Центральної Азії до ЄС масово везли підсанкційну продукцію з Білорусі та Росії за підробленими сертифікатами.

#### 2.4 Розширений каталог

##### **Laisvės TV OSINT Unit**



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

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



Laisvės TV – незалежний інтернет-канал, заснований журналістом Андрюсом Тапінасом<sup>38</sup>. Поєднує можливості медіаплатформи з гнучкістю розвідувальної спільноти.



Організація фокусується на виявленні прихованих зв'язків литовських політиків та бізнесменів із прокремлівськими структурами, а також на прямому забезпеченні оборонних потреб (саме вони зібрали €6 млн на Bayraktar для України за три дні). Працює з волонтерським рухом «Литовських ельфів» для верифікації інформації в соцмережах. Результати розслідувань Laisvės TV регулярно стають приводом для перевірок з боку Служби розслідування фінансових злочинів (FNTT) та Спеціальної слідчої служби (STT) Литви<sup>39</sup>.

#### **Patikrinta (15min.lt)**



Фактчекінговий проєкт був започаткований у 2016 році журналісткою Лєпа Желнене<sup>40</sup> у складі редакції 15min, а нині командою керує Егле Зікарі.



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

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

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



Patikrinta став першим проектом у країнах Балтії, який отримав сертифікацію International Fact-Checking Network.

Їхня унікальність полягає у фокусі на внутрішньополітичному полі та маніпуляціях, які використовують місцеві популісти або радикальні групи. Команда інтегрована безпосередньо в стрічку новин одного з найбільш відвідуваних сайтів країни.

### **DIGIRES**



Науково-технологічний проект, який працює над інформаційною безпекою суспільства. Він був започаткований у 2021 році на базі факультету публічної комунікації Vytautas Magnus University спільно з медіакомпанією Delfi Lietuva та партнерами з громадського сектору. Ініціаторкою та керівницею проекту є Ауксе Бальчитене<sup>41</sup>.



Організація об'єднує університетських науковців, які розробляють ШІ-алгоритми для раннього виявлення пропаганди, з практикуючими журналістами. Модель орієнтована на довгостроковий аналіз того, як саме дезінформація проникає у вразливі групи населення (зокрема, етнічні меншини на кордонах).

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



## Розділ 3.

### Литовські OSINT інструменти

#### 3.1 Спеціалізовані боти та парсери волонтерського сектору

##### \* Інструмент автоматизації звітності «Trusted Flagger»

Коли дослідник виявляє фейк або дезінформаційну атаку, скрипт автоматично пакує доказову базу відповідно до міжнародних стандартів Берклівського протоколу (робить верифіковані знімки екрана, фіксує URL, зчитує метадані) та через захищений API-канал надсилає скаргу командам модерації Meta, TikTok або Google, миттєво минаючи стандартну загальну чергу розгляду.

##### \* Парсери митних декларацій та залізничних накладних

Скрипти та AI-інструменти автоматично витягують і структурують дані про вантажі з митних декларацій, транзитних систем і залізничних накладних країн ЄС та Центральної Азії. У процесі можуть використовуватись платформи типу MUJ<sup>42</sup>, Rava<sup>43</sup>, а також системи логістичного парсингу на кшталт 8devices<sup>44</sup>.

Дані можуть агрегуватись через європейські системи залізничних накладних (ORFEUS, CIM/SMGS) та цифрові логістичні екосистеми перевізників і інтеграторів (Transporeon, LTG Cargo), що будує аналітику торгових потоків і ланцюгів постачання.

##### \* OCR-парсер фінансової звітності «Skaidrinam Extractor»

Під час волонтерського аудиту використання бюджетних коштів депутатами, IT-волонтери розробили систему на основі Tesseract/EasyOCR та інтеграції з локальними LLM-моделями. Програмне забезпечення автоматично розпізнає та оцифровує в єдину таблицю сотні тисяч хаотичних сканів паливних чеків, квитанцій та звітів, миттєво підсвічує аномалії та випадки шахрайства.

#### 3.2 Публічні ліцензії та Open Source

Усі інструменти та бази даних, створені в межах громадського аудиту, поширюються за міжнародною ліцензією Creative Commons Attribution 4.0 International (CC BY 4.0).

##### \* Lietuvos atvirų duomenų portalas (data.gov.lt)<sup>45</sup>

Єдина точка доступу, яка консолідує понад 2 500 наборів даних від усіх міністерств, муніципалітетів та державних служб. Платформа надає прямий доступ до сирих даних у форматах CSV, JSON, XML та GML через відкриті API-інтерфейси.

<sup>42</sup> <https://www.muji.lt/en>

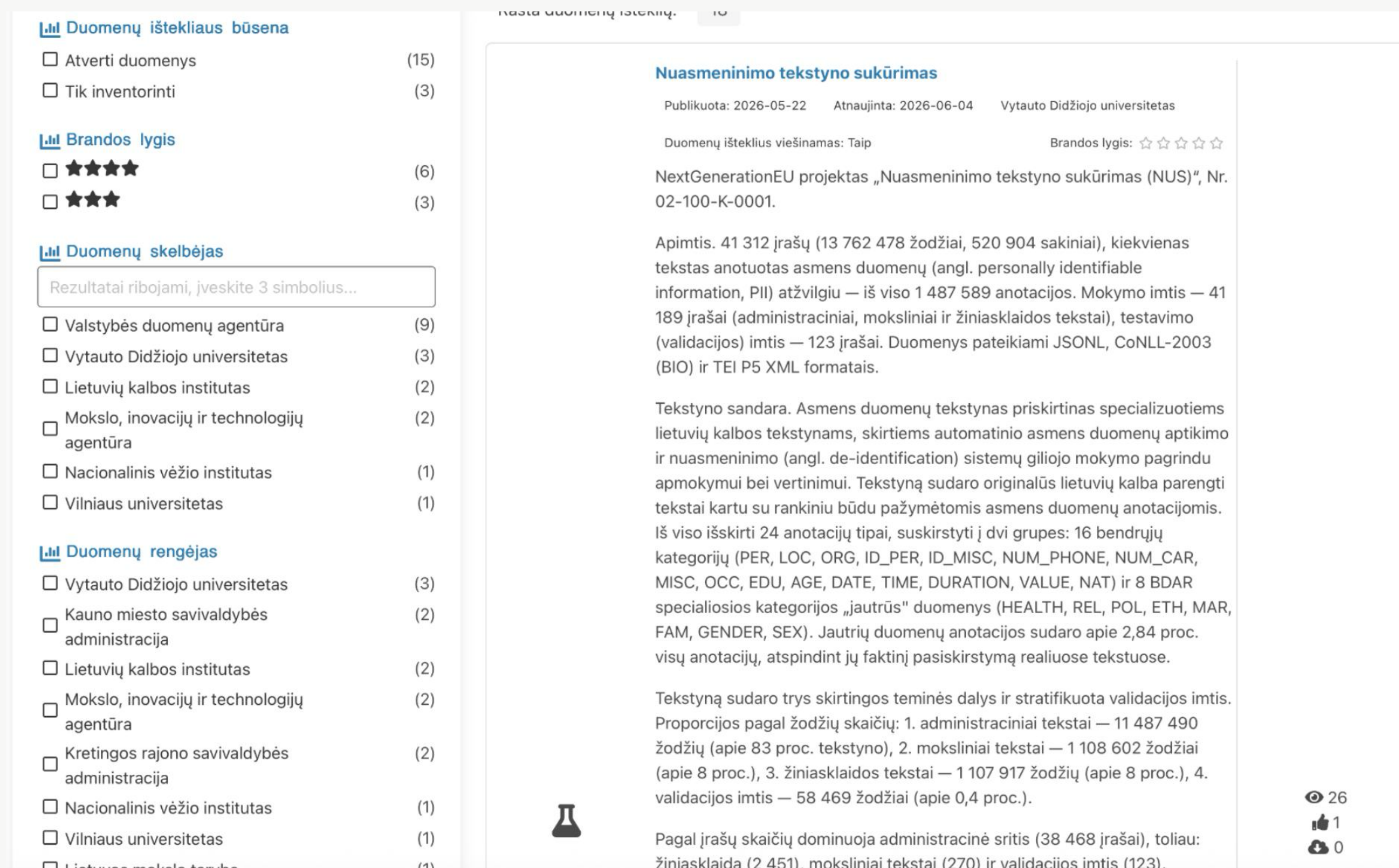
<sup>43</sup> <https://rava.lt/en/metro-program/>

<sup>44</sup> <https://www.8devices.com/>

<sup>45</sup> <https://data.gov.lt/>



Також система здійснює масовий парсинг даних про державні ресурси, транспортні потоки, закупівлі, екологічний стан та інфраструктурні об'єкти, виступаючи базою для виявлення системних аномалій.

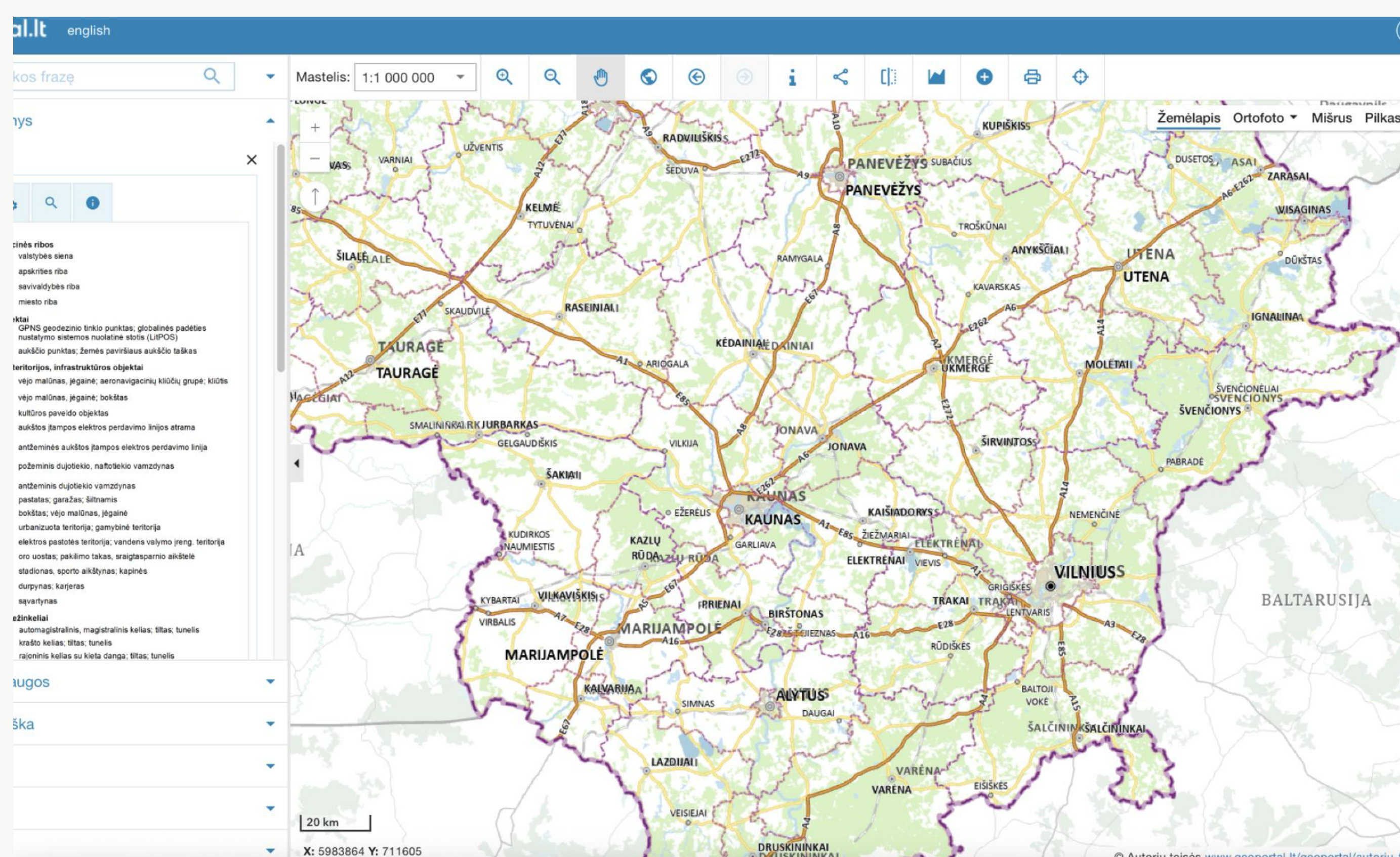


### \* Valstybės įmonė Registrų centras<sup>46</sup>

Веде головні базові реєстри країни. У межах політики відкритих даних надає щомісячні первинні вивантаження Реєстру юридичних осіб, системи даних про бенефіціарів, Реєстру нерухомості та Адресного реєстру. Головний інструмент фінансової розвідки та моніторингу санкцій. Дозволяє безкоштовно деанонімізувати ланцюжки власності, знаходити європейські активи російських олігархів та викривати компанії-прокладки.

### \* Geoportal.lt<sup>47</sup>

Централізована ГІС-платформа, яка надає відкриті геопросторові дані за суворими стандартами європейської директиви INSPIRE. Набори поширюються у форматах Shapefile (.shp) та GeoPackage (.gpkg). Надає точні кадастрові межі земельних ділянок, ортофотоплани надвисокої чіткості, карти лісових та водних господарств, а також історичні топографічні шари. Ці матеріали використовують для зіставлення комерційних супутникових знімків з офіційними картографічними даними та перевірки меж об'єктів.



<sup>46</sup> <https://www.registrucentras.lt/>

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



#### \* **Karštos Pėdos**<sup>48</sup>

Національний інструмент прозорості, який хоч і є базою даних, але має інтегровану карту зв'язків. Він дозволяє візуалізувати перетинання інтересів політиків, чиновників і бізнесу з географічною прив'язкою до конкретних підприємств чи прикордонних хабів.

#### \* **Balticdisinfo.eu**<sup>49</sup>

Відкрита платформа щотижневого моніторингу дезінформаційних наративів у Литві, Латвії та Естонії, розроблена Civic Resilience Initiative. Публікує структуровані звіти: канал поширення, джерело наративу, зв'язок із кремлівськими операціями впливу. Серед верифікованих кейсів – документування координованої кампанії кінця 2025 року, коли проросійські ресурси системно переформатовували литовські мовні вимоги для службовців як «тотальну дискримінацію російськомовних», ігноруючи безпековий контекст законодавчих змін.

### **Інструменти для фінансової розвідки та моніторингу санкцій**

#### \* **AMLYZE**<sup>50</sup>

Створена командою провідних експертів і експертів із досвідом роботи в Центробанку Литви, Європейському центральному банку (ECB) та Службі розслідування фінансових злочинів (FNTT), платформа здійснює цілодобовий моніторинг транзакцій, оцінку ризиків клієнтів (Customer Risk Scoring) та миттєвий скринінг платежів. Її унікальність – модуль Sanctions Screening Performance Test, який за допомогою бази з понад 50 000 контрольованих імен тестує банківські системи на наявність прихованих помилок.

#### \* **Salv Bridge**<sup>51</sup>

Розробка естонсько-литовського консорціуму RegTech-інноваторів, розгорнута у Литві за участю найбільших фінтех-гігантів. Інструмент передбачає оперативний обмін даними між учасниками фінансового сектору щодо підозрілих профілів та ознак відмивання коштів, що підвищує ефективність виявлення фінансових правопорушень.

#### **Моделі комп'ютерного зору на архітектурі NAS-MACU**<sup>52</sup>

Власні нейромережеві алгоритми BPTI. Замість стандартного розпізнавання ШІ автоматично підлаштовує параметри під конкретний супутник, щоб розпізнавати техніку (наприклад, Т-72 чи ППО) в умовах туману, хмарності, задимлення поля бою чи глибоких тіней від дерев.

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

<sup>49</sup> <http://Balticdisinfo.eu>

<sup>50</sup> <https://amlyze.com/>

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

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



### Софт автоматичного аналізу когерентних змін<sup>53</sup>

Розробка VILNIUS TECH, яка миттєво фіксує, де пройшла важка техніка, де з'явився новий окоп чи укриття, навіть якщо техніка вже поїхала, а сама територія замаскована.

### Інтеграційні екосистеми Data Fusion<sup>54</sup>

Платформи, що розробляються за фінансування Європейського оборонного фонду. Вони автоматично об'єднують дані з космосу в один цифровий шар, цивільних морських та повітряних радарів, тактичних дронів та геоприв'язаних повідомлень із соцмереж. Саме через цю інфраструктуру реалізується спільна з Україною «петля донавчання» ШІ – процес автоматичного вдосконалення алгоритмів на основі реального бойового досвіду. Україна передає до системи актуальні дані з поля бою (наприклад, специфічні радіосигнали, нові типи маскування чи зразки техніки РФ), які штучний інтелект раніше не бачив. Система аналізує ці нові матеріали, виправляє свої помилки розпізнавання, оновлюється та одразу повертає аналітикам і військовим уже точнішу версію софту.



### 3.3 Регламентні та комерційні умови доступу та можливості для України

У межах розбудови єдиного Lithuanian Open-Source Intelligence Centre та інноваційного оборонного хабу в Каунасі, сформовано дворівневу архітектуру взаємодії, яка поєднує інтереси національної безпеки НАТО та союзницькі зобов'язання перед Україною.

Доступ до закритих волонтерських і напівкомерційних інструментів здійснюється відповідно до встановлених безпекових протоколів. Вони регламентують порядок роботи з даними, забезпечують дотримання правових вимог та знижують ризики несанкціонованого доступу з боку ворожих розвідувальних структур.

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

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



**Стандартизація за Берлінгерським протоколом (Berkeley Protocol)<sup>55</sup>**

Будь-який цивільний або військовий фахівець, який отримує доступ до інструментів збору та обробки даних (наприклад, скраперів Kiberšauliai або супутникових модулів BPTI), зобов'язаний пройти сертифікацію щодо дотримання «ланцюжка зберігання доказів». Цифрові матеріали, зібрані за допомогою софту, можуть бути офіційно використані у міжнародних судах (МКС) або у звітах ООН.

**Меморандуми про безпековий допуск:**

Оскільки литовська OSINT-архітектура тісно взаємодіє з військовою розвідкою та Департаментом держбезпеки, прямий доступ до аналітичних даних вимагає підписання тристороннього Меморандуму (Уряд Литви – ГО/Розробник – Одержувач). Для доступу до мілітарних ШІ-моделей українські ситуаційні центри проходять верифікацію через систему Міноборони.

**Регламент захисту даних:**

Цивільні та журналістські платформи надають доступ до своїх OSINT-панелей за умови дотримання європейських стандартів кібербезпеки. Користувачі проходять обов'язкову двофакторну аутентифікацію та верифікацію цифрового підпису для запобігання витоку логістичних або персональних баз даних.

Фінансова модель екосистеми побудована на принципі диверсифікації: комерційний сектор фінансує розробку, тоді як військові та правозахисні місії отримують пріоритетні безкоштовні преференції.

**Зведена матриця комерційного доступу для України**

| Категорія інструменту                                   | Комерційна вартість у ЄС              | Умови для ЗСУ та Сил оборони                         | Умови для українських ГО та медіа                     |
|---------------------------------------------------------|---------------------------------------|------------------------------------------------------|-------------------------------------------------------|
| Мілітарний ШІ та GEOINT (BPTI, VILNIUS TECH)            | Висока (комерційні контракти / EDF)   | Безкоштовно за умови tech-бартеру (Data Fusion Loop) | Недоступно (суворі мілітарні обмеження)               |
| Аналітика дезінформації (Debunk.org platform)           | За ліцензійною підпискою B2B / B2G    | Безкоштовно (прямий урядовий доступ)                 | Безкоштовно (через грантові квоти програм BECID/EDMO) |
| Логістичні парсери та фінансові бази (Siena, Open Data) | Безкоштовно (Open Source / CC BY 4.0) | Безкоштовно (відкритий код на GitHub)                | Безкоштовно (спільні розслідування OCCRP)             |

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



### 3.4 Деталізація фінансових форматів для України

#### Формат «Joint R&D»

Сили оборони України не сплачують ліцензійні платежі за використання інтелектуальної власності литовських інститутів. Замість грошей українська сторона надає реальні верифіковані датасети з лінії фронту. По суті, український бойовий досвід є платою за литовські високі технології, що дає можливість створювати спільні програмні продукти світового рівня<sup>56</sup>.

#### Грантове субсидіювання для цивільного сектору

Для українських фактчекерів та журналістів-розслідувачів доступ до платних інструментів автоматичного моніторингу інформаційного простору покривається за рахунок європейських фондів.

Фінансування використання серверних потужностей та API-інтеграцій бере на себе литовська сторона в межах бюджетів Європейської обсерваторії цифрових медіа (EDMO), проєктів BECID та програм Horizon Europe.



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



## Розділ 4.

### Аналіз співпраці: Україна та Литва

Найбільш інституціоналізована форма україно-литовської співпраці сьогодні відбувається через офіційні міжнародні механізми кримінального переслідування, насамперед Спільну слідчу групу (далі – JIT<sup>57</sup>), створену під егідою Eurojust після початку повномасштабного вторгнення Росії в Україну<sup>58</sup>.



Ця група була сформована протягом перших тижнів повномасштабного вторгнення як інструмент швидкої координації між державами, які почали паралельно розслідувати військові злочини на своїх рівнях. Спочатку до неї увійшли Україна, Литва та Польща, а згодом приєдналися інші європейські країни.

Практичність Спільної слідчої групи полягає в обміні кримінальними матеріалами: слідчі та прокурори з різних країн можуть напряму передавати докази, координувати слідчі дії, синхронізувати підходи до кваліфікації злочинів і уникати дублювання розслідувань у різних юрисдикціях.

#### 4.1 Безпековий та розвідувальний рівень

Інструментом співпраці між Україною та Литвою стала двостороння Угода про безпекову співпрацю, укладена в червні 2024 року<sup>59</sup>. Цей документ юридично зафіксував непорушне зобов'язання Вільнюса щорічно виділяти на оборонні та безпекові потреби України фіксовану суму у розмірі не менше 0,25% від національного ВВП Литви.

Окрім гарантованого фінансового та військово-технічного потоку, угода заклала правову та технічну основу для прямої та глибокої взаємодії між структурами воєнної розвідки обох держав.

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

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

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



## 4.2 Журналістський та OSINT-рівень

Наочним кейсом співпраці країн є проект «Mapping Russia's War Machine»<sup>60</sup> – велике міжнародне GEOINT-розслідування, реалізоване консорціумом журналістів у складі литовського національного мовника LRT, аналітичних центрів VSquare, Eesti Ekspress, Frontstory.pl та волонтерської платформи OSINT for Ukraine. Аналітики провели мапування російських військових баз вздовж усього північно-західного кордону НАТО – від Мурманська до Калінінграда.

## 4.3 Досвід співпраці Литви з іншими країнами

### Балтійсько-скандинавська співпраця

Країни Північної Європи та Балтії тісно співпрацюють у сфері безпеки та технологій через взаємодію національних кіберполіцій, CERT-структур та європейських агентств, таких як Europol та ENISA.

Правоохоронні органи регіону проводять регулярні практичні семінари, як-от OSINT Workshop for Nordic and Baltic Countries<sup>61</sup> для синхронізації інструментів цифрового криміналістичного аналізу та дослідження кіберзагроз.

Паралельно країни запустили масштабну міжурядову ініціативу Baltic AI Giga Factory<sup>62</sup> – проект зі створення обчислювальних хабів штучного інтелекту, алгоритми яких обслуговуватимуть потреби регіонального GEOINT, моніторингу супутникових знімків прикордоння та автоматизованої мовної аналітики InfoSec.

### Західні Балкани та Грузія

Усвідомлюючи, що Кремль використовує ідентичні методи дестабілізації в інших вразливих регіонах Європи, Литва почала масштабувати свої OSINT-технології на Західні Балкани та Південний Кавказ. Аналітичний хаб Debunk.org розширює<sup>63</sup> свої регіональні проекти протидії дезінформації через партнерські OSINT-ініціативи у країнах Західних Балкан та Південного Кавказу, залучаючи місцеві медіа та аналітичні організації до спільного моніторингу інформаційних операцій.

Литовські фахівці передають місцевим громадським організаціям та журналістам свої кастомні веб-скрапери, вчать будувати графи зв'язків для викриття “фабрик тролів” та впроваджують методологію контрнарративів для захисту локального медіапростору перед виборами.

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

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

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

<sup>63</sup> <https://debunk.org/projects/>





#### 4.4 Виклики та бар'єри співпраці

##### Структурний бар'єр №1: Інформаційна ізоляція

Інформаційна ізоляція виникає через відмінності в операційній культурі та технічну несумісність. Литовські GEOINT-фахівці можуть ідентифікувати переміщення конкретної військової частини за супутниковими знімками, українські OSINT-волонтери – знаходити профілі солдатів цієї частини в соцмережах, а державні слідчі органи – документувати наслідки їхніх дій на місцях. Проте через відсутність єдиного протоколу ці масиви даних не зливаються в єдиний доказовий ланцюжок.

Кожна організація використовує власні стандарти збереження метаданих та хешування відеоматеріалів. Через ізолюваність різні групи аналітиків витрачають ресурси на розслідування одного і того ж кейсу (наприклад, обстрілу конкретного цивільного об'єкта), не знаючи про напрацювання колег. Це створює ілюзію активності при низькій загальній продуктивності системи.

У литовському контексті, де OSINT тісно переплетений з оборонним сектором, надмірна класифікація даних часто стає бар'єром для співпраці з цивільними розслідувачами, навіть коли інформація отримана виключно з відкритих джерел.

##### Структурний бар'єр №2: Мовний бар'єр

Мовний бар'єр у литовсько-українській взаємодії означає розділення інформаційних і професійних середовищ. Більшість литовських організацій, зокрема такі як LRT Tytėjų Grupė, Patikrinta 15min чи Debunk.org, орієнтуються насамперед на литовськомовну аудиторію, тому їхні розслідування та аналітичні матеріали залишаються доступними переважно всередині країни.

Це створює ситуацію, коли навіть важливі дослідження про дезінформацію чи безпекові загрози не доходять до українських партнерів без перекладу, через що інформація часто не поширюється між спільнотами.



**Структурний бар'єр №3: Фінансова нестійкість громадянського сектора**

Більшість приватних і неурядових організацій, які формують ядро литовської екосистеми прозорості, включаючи незалежні фактчекінгові агенції, розслідувальні медіа та волонтерські OSINT-колективи, функціонують в умовах хронічної фінансової вразливості. На відміну від державних безпекових інституцій, цивільний сектор критично залежить від короткострокових грантів, донатів та спонсорської допомоги.

Найбільш руйнівним інструментом тиску на незалежних розслідувачів є так звані SLAPP-позови. Це юридична практика, коли великий бізнес, корумповані чиновники або приховані лобісти агресора засипають малі ГО та редакції багатомільйонними судовими позовами про «захист честі та ділової репутації».

Судові процеси роками зв'язують усі наявні ресурси ГО, змушуючи аналітиків витрачати кошти на дорогих адвокатів замість проведення розслідувань.

**4.5 Перспективні напрямки співпраці на 2026-2028****Напрямок 1: Розслідування обходу санкцій**

Литва виконує функцію критичного транзитного та комплаєнс-хабу між РФ/Білоруссю та внутрішнім ринком ЄС, тому її юрисдикція стає місцем, де санкційні схеми часто формально легалізуються через реекспорт, посередницькі компанії та логістичні ланцюги, розбиті на кілька юридичних пунктів.

Прийняття у червні 2025 року<sup>64</sup> національного санкційного списку Литви створює додатковий рівень фільтрації, який доповнює санкційні режими ЄС і дозволяє точніше «підсвічувати» локальних бенефіціарів, логістичних посередників та компанії-прокладки, що не потрапляють у загальноєвропейські списки, але беруть участь у транзитних схемах.



<sup>64</sup> <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>



Потенціал співпраці між литовською Siena та українськими розслідувальними командами полягає саме в можливості поєднати локальну регуляторну видимість Литви з міжнародною аналітичною інфраструктурою OCCRP, що не лише допомагає фіксувати окремі випадки обходу санкцій, а й відновлювати повні схеми від бенефіціара до кінцевого споживача.

#### **Напрямок 2: ICRA як структурна платформа для OSINT**

Міжнародний центр кримінального переслідування за злочин агресії (далі – ICRA) слід розглядати як шар доказової інфраструктури для майбутнього переслідування, який працює одночасно в режимі розслідування і підготовки процесуальної придатності матеріалів.

ICRA може виступати як стандартизатор доказових протоколів – визначати єдині вимоги до аутентифікації цифрових матеріалів, часової синхронізації подій, геолокаційної прив'язки та ланцюга збереження доказів, щоб зібрані OSINT-дані могли бути використані в міжнародних судах без втрати юридичної валідності.

#### **Напрямок 3: ШІ-моніторинг наративів – масштабування моделі Debunk.org**

Практичне розширення моделі Debunk.org може виглядати як перехід від аналітичного моніторингу до повноцінної міжінституційної системи раннього попередження. Йдеться про створення спільного контуру обміну даними між Debunk.org та українськими партнерами через захищені API, які передають потоки контенту з соцмереж, Telegram-каналів і новинних ресурсів у Балтії.

Для практичного використання це варто доповнити системою тригерних сповіщень для українських аналітичних центрів і державних структур, щоб вони отримували не просто звіти, а оперативні сигнали про різкі сплески або координацію кампаній. Важливою частиною стає також узгоджена модель управління даними, яка враховує GDPR та національні обмеження, але дозволяє обмін агрегованими індикаторами та метаданими без порушення приватності.

#### **Напрямок 4: GEOINT – розширення моделі «Eyes on Russia»**

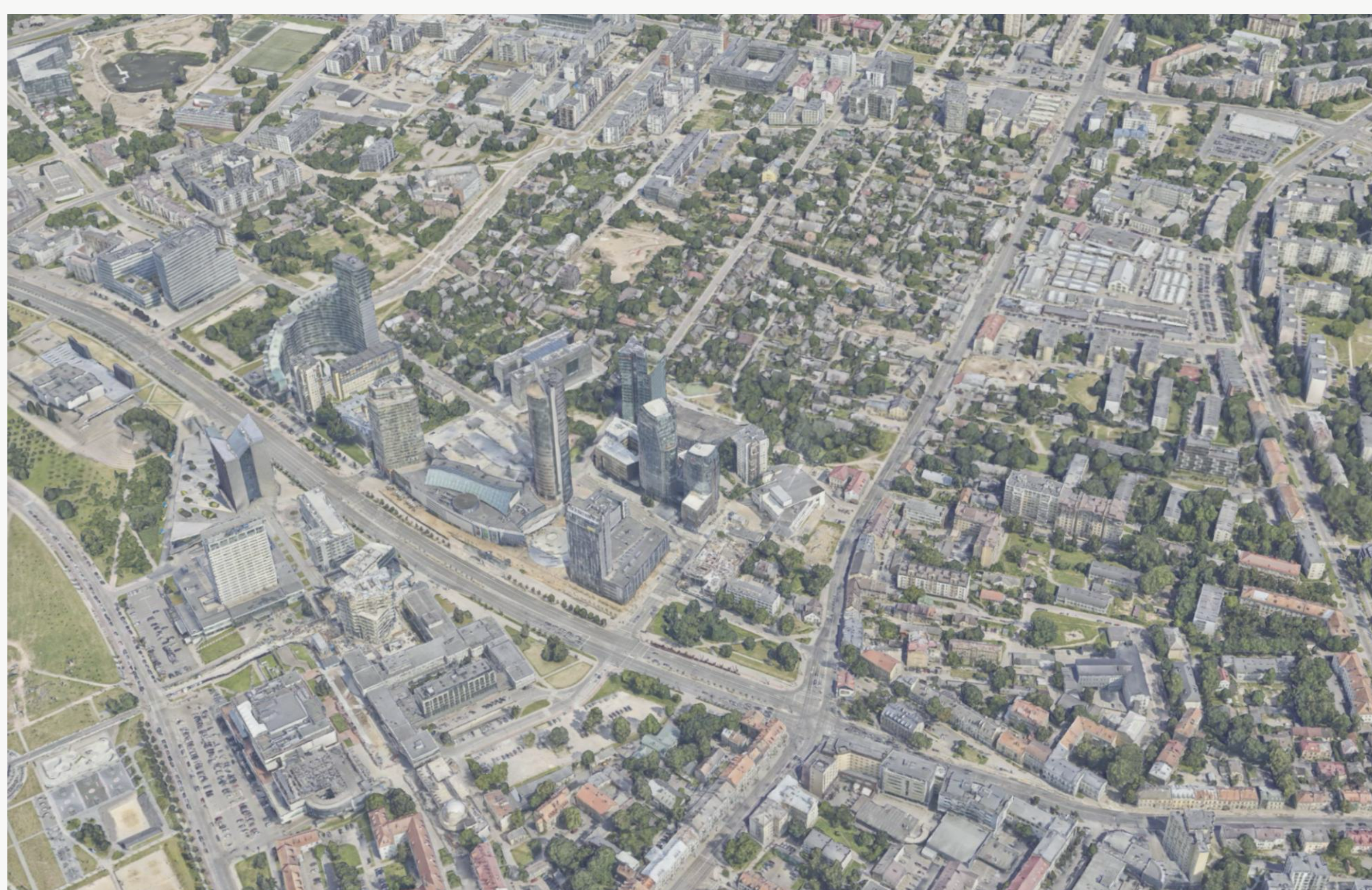
Наступним кроком у розвитку GEOINT-моделі на базі “Eyes on Russia” є перехід від ситуативного OSINT-аналізу до безперервної багатоджерельної інфраструктури спостереження.

З огляду на швидке збільшення кількості відео- та просторових даних, ключовим стає стандартизація їхньої обробки: автоматичне поєднання супутникових знімків, геолокаційного аналізу відео, даних з соціальних мереж і відкритих реєстрів у єдину часово-просторову модель подій.

---

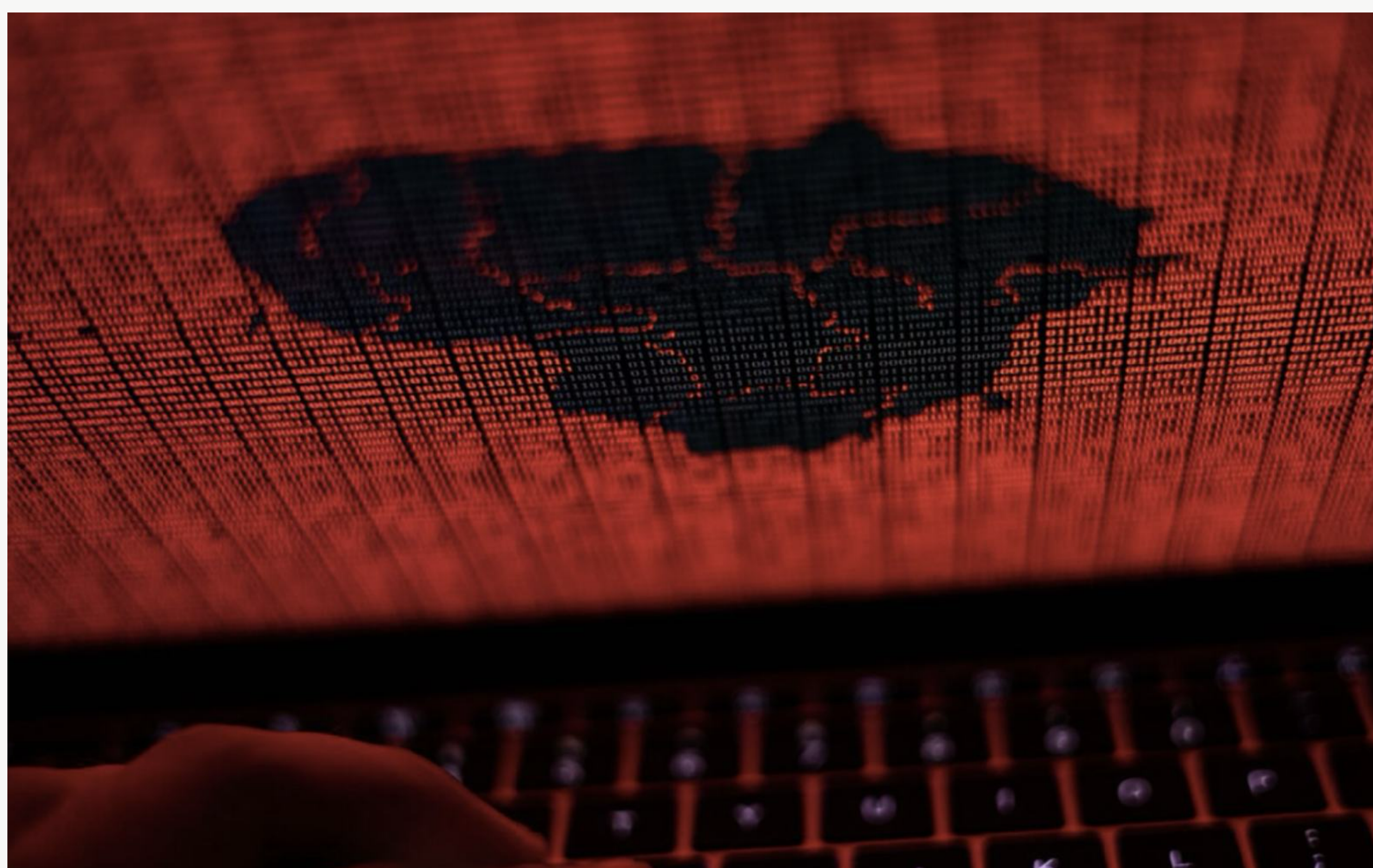
64 <https://www.urm.lt/en/news/928/lithuanian-parliament-approved-amendments-to-the-law-enabling-lithuania-to-impose-national-individual-and-economic-sanctions-against-russia-and-belarus%3A44394>





### Напрямок 5: Повоєнна прозорість – модель Karštos Pėdos для України

Модель платформи прозорості Karštos Pėdos буде корисною для повоєнної України в контексті відновлення та протидії корупції. Media4Change та Siena мають практичний досвід побудови такої системи, зокрема її захисту від регуляторних атак під виглядом GDPR.



### Методологія аналізу

Головна мета аналізу – впорядкувати інформацію про литовські OSINT та аналітичні організації і допомогти українським колегам знайти партнерів.

Пріоритетом дослідження стали організації, які системно працюють з розслідуваннями проти Росії та Білорусі, а також мають успішні публічні кейси у відстеженні військової техніки, боротьбі з дезінформацією чи розслідуванні економічних злочинів (у тому числі обхід санкцій).

Дослідження базувалося на системному, історичному та порівняльному підходах. Системний підхід допоміг розглянути аналітичну екосистему Литви як сукупність взаємопов'язаних організацій та ініціатив. Історичний підхід використовувався для аналізу розвитку сектору та чинників, що вплинули на його формування. Порівняльний підхід – для зіставлення організацій за напрямками діяльності, спеціалізацією та форматами співпраці.



Для збору даних використовувався аналіз відкритих джерел (OSINT), зокрема офіційних вебсайтів організацій, публічних звітів, аналітичних матеріалів, профілів у соціальних мережах та згадок у профільних медіа.

Для уточнення та верифікації інформації були проведені інтерв'ю з представниками деяких організацій, згаданих у звіті. Причина вибіркості – проведення дослідження в умовах обмеженого часу під час фізичного візиту авторки до Литви. Частина організацій була ідентифікована вже під час зустрічей з представниками сектору, що унеможлиблює проведення додаткових інтерв'ю в межах цієї поїздки. Крім того, окремі ініціативи не мають постійних представників або публічно доступних контактів для комунікації. З огляду на це, інтерв'ювання охопило лише частину організацій, а результати дослідження слід розглядати як карту екосистеми, яка може бути доповнена під час подальшої роботи та розширення контактів.

Зібрані дані були систематизовані та класифіковані за типами організацій, напрямками діяльності, тематичною спеціалізацією та потенціалом для співпраці з українськими партнерами. Для візуалізації сектору застосовувався метод мапування організаційної екосистеми.