LiSMI

Live Social Media Intelligence

A powerful platform designed to track, analyze, and interpret public information to uncover trends, threats, and audience sentiment.

2025

Agenda

Information Space as a Battlefield

Modern Information Threats

Strategic Blind Spots

Our Solution

Key Capabilities

Deep Dive Investigation

Technologies

Security & Compliance

Who is this for?

Case Study

Romania, 2025 Elections

Next Steps

Information Space as a Battlefield

Modern Information Threats

The digital information space is increasingly used as a tool of geopolitical influence. Foreign actors exploit social media, news platforms, and online communities to manipulate opinions, undermine elections, and destabilize democratic societies.

Foreign state-sponsored propaganda and manipulation

Attempts to sway elections through disinformation, etc.

Recruitment of extremists and foreign intelligence assets

Spread of fake narratives used to destabilize societies

Erosion of trust in democratic institutions and the media

Strategic Blind Spots

Threats often go undetected until damage is done

In Slovakia (2023), anti-Ukrainian Telegram narratives surged two months before the elections. Their impact on public discourse was only recognized by OSINT activists after the narratives had already shaped public opinion.

OSINT efforts are manual, fragmented, and reactive

Government monitoring teams rely on manual workflows (PDF reports, Excel links, human reading). This makes it nearly impossible to detect trends at scale or trace coordinated behavior across platforms. By the time one analyst reviews 200 messages, bot networks have pushed out 2,000 more.

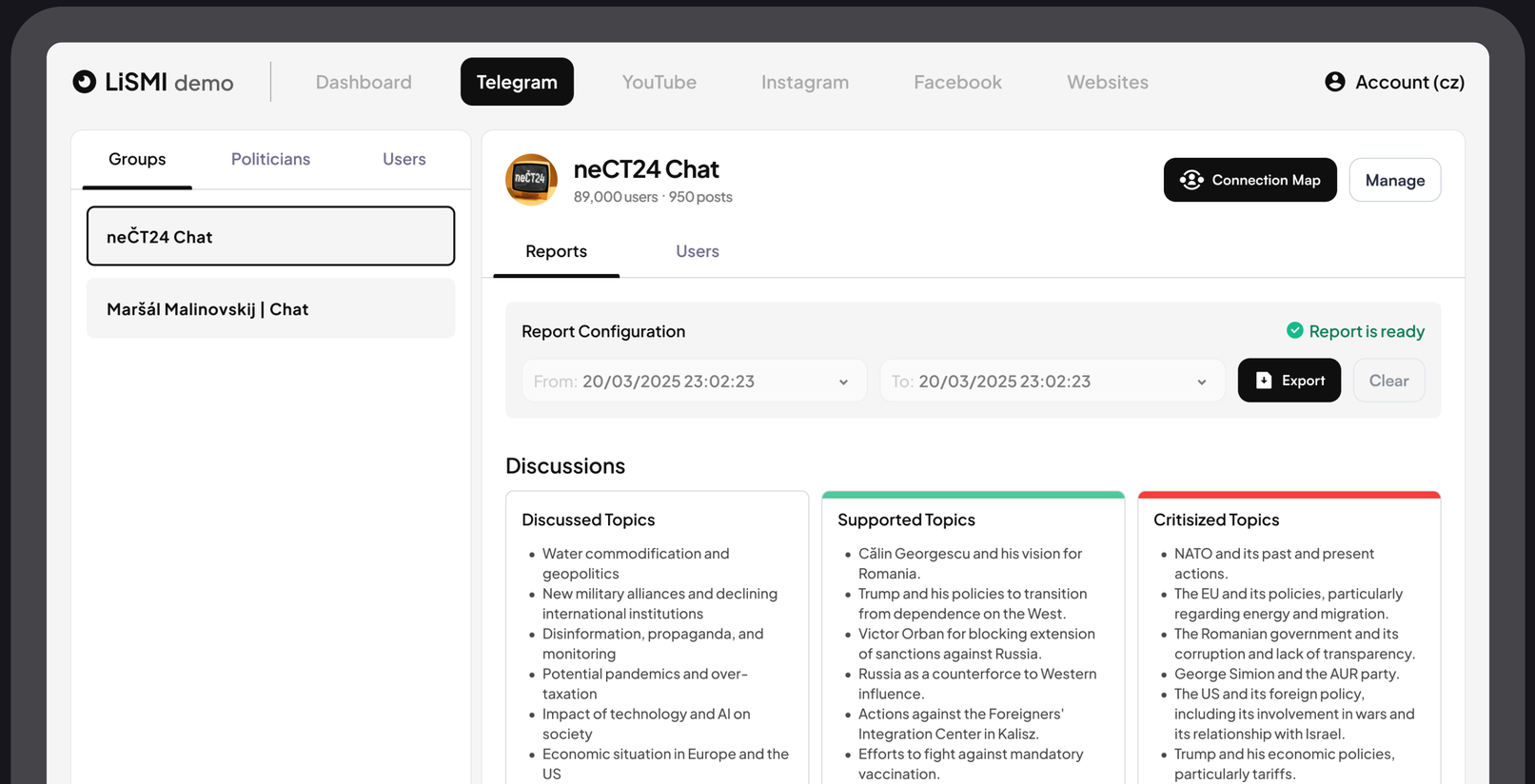
Covert campaigns adapt faster than detection systems

When a Russian-linked Facebook page was banned, the associated network migrated to Telegram and TikTok within 24 hours. Without cross-platform surveillance, the shift went unnoticed — until it surfaced in the press.

Our Solution

LiSMI

A platform for real-time monitoring of critical online ecosystems. Built for live insights, not post-factum reports.



Track Social Media Sources

We currently monitor Telegram, Instagram, YouTube, and X (Twitter) — key platforms where influence campaigns and radical content often emerge. Additional sources can be integrated upon request, depending on specific targeting needs.

Instagram

Influencers shaping public opinion

Telegram

Channels, groups, and public chats

YouTube

Political and radical content creators

X (Twitter)

Real-time conversations and trending topics

Track Your Own Sources

Add and monitor sources relevant to your tasks

Key Capabilities – Monitoring & Reports

Timely insights and alerts from multilingual data — helping detect emerging threats, track influence campaigns, and respond faster.

Daily Intelligence Reports

Automatically generated from multilingual source data — fully language-agnostic.

Live Trend Monitoring

Track emerging topics, narrative shifts, and influence operations as they unfold.

Personalised Alerts

Custom alerts on fake news, disinformation, propaganda, terrorism-linked content, and more.

Deep Dive Investigation

From individuals to ecosystems, everything you need to investigate who is saying what, and why it matters.

Track Influence and Reach

Monitor how narratives around public figures and politicians evolve and detect surges in popularity or sudden attacks before they go mainstream.

Spot Manipulation Patterns

Uncover bot accounts and copy-paste operators. Identify signs of inauthentic behavior and content flooding.

Profile Key Individuals

Understand user behavior: what they post, how they speak, how often they engage. Spot emotional tone, political leaning, and signs of radicalization.

Understand the Media Landscape

See what topics are being discussed, promoted, or attacked and identify which users are most active and influential in a given channel.

Map the Network

Visualize connections between users, channels, and influencers. Detect coordinated campaigns or influence groups.

Technology & Data

Open-Source Intelligence (OSINT)

- We collect and analyse publicly available content: articles, posts, comments, channels

Custom Analytics Engine

- In-house tech stack for data collection, processing, and presentation
- Modular, scalable, and adaptable to evolving information spaces

AI-Powered Analysis

- AI/NLP models used to extract insights, classify content, detect anomalies, and summarise narratives
- Optimised pipelines for near real-time results

Secure & Controlled Access

- Protected, role-based platform access
- Supports on-premise or sovereign cloud deployments for sensitive environments

Security & Compliance

Legally Compliant by Design

We collect and process only publicly available information from open online sources, including social media platforms, messaging apps, websites, and forums. No private communications, personal identifiers, or restricted-access data are ever accessed or stored.

European Infrastructure

All data is stored and processed within the European Union, using Google Cloud Platform with regional residency controls and compliant subprocessors (e.g., Gemini AI).

On-Prem Deployment Ready

The platform is fully compatible with on-premise and air-gapped environments.

Who is this for?

Security & Intelligence Teams

Detect and counter information warfare, foreign influence, and terrorist propaganda.

Track election interference and covert recruitment operations in real time.

OSINT & Media Analysts

Monitor public sentiment, narrative shifts, and propaganda trends.

Conduct deep research using structured open-source intelligence.

Case Study

Romania, 2025 Elections – Monitoring

A two-phase analysis of 50 top users in Romania's major pro-Russian Telegram channels (@DanDiaconu, @sputnecenzurat) was conducted using an advanced monitoring platform.

Phase one established a behavioral baseline; phase two , ahead of national elections, applied enhanced algorithms for deeper user-level insights.

Jan 2025 – Mar 2025

Baseline Phase

Behavioral baseline analysis of top 50 active users.

Apr 2025 – May 2025

Pre-election Phase

Enhanced analysis with upgraded algorithms and user-level insights.

May 2025

Elections

Romania, 2025 Elections – Outcome

Clear evidence of intensified coordinated propaganda efforts in the run-up to Romania's presidential elections.

Escalation of Narrative Spread	• Activity from accounts promoting pro-Russian narratives has gone up six times. • Noticeable shift toward more aggressive and confrontational messaging.
Emergence of Bot-Like Behavior	• Surge in suspicious activity with clear automation patterns, including: repetitive messaging, slogan-heavy language, high-volume reposting from coordinated sources.

Purtator de cuvant MAE Romania/ MFA spokesperson
@PdCMAERO

During Romania's ongoing presidential elections yet again we see the hallmarks of Russian interference. A viral campaign of fake news on Telegram & other social media platforms is aimed to influence the electoral process. This was expected & 🇷🇴 authorities debunked the fake news.

5:27 PM · May 18, 2025 · **614** Views

Next Steps

1. **Try the demo**
   Explore the platform’s core capabilities in action.
2. **Run pilot together**
   We’ll deploy a tailored test setup with your selected sources and objectives.
3. **Scale to full deployment**
   Flexible feature set, custom workflows, and infrastructure adapted to your operational needs

Contact Us

info@eigengrau.world