

Exposing the architecture of FIMI operations

3rd Report on FIMI Threats

EEAS Stratcom - Data Team

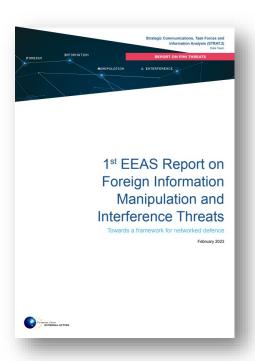
August 2025

3rd EEAS Report on FIMI Threats

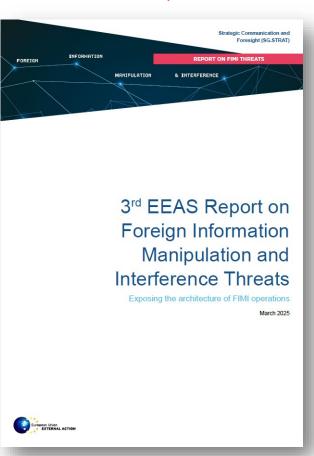
How to analyse?

How to respond?

How to expose?

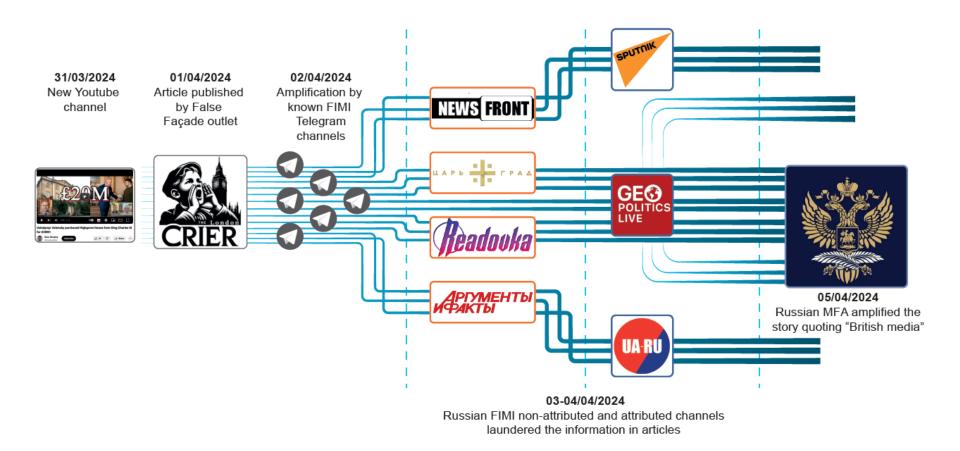






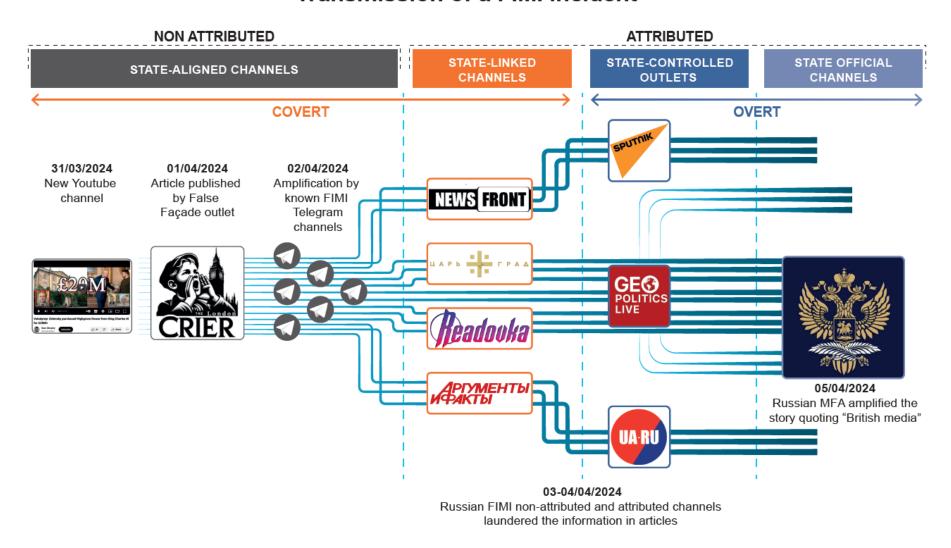


Transmission of a FIMI incident





Transmission of a FIMI incident





Four blocks of the FIMI Architecture

OFFICIAL STATE CHANNELS

Official communication channels directly operated by a government and its representatives, openly reflecting the state's official voice.

 Examples: Government accounts, MFA representatives. STATE-CONTROLLED OUTLETS

Media outlets funded, managed, and editorially controlled by state-appointed bodies or the ruling party. These outlets deliver the editorial line set by the state.

> Examples: RT, Sputnik, CGTN, and their official mirror sites.

OVERT

COVERT

STATE-LINKED CHANNELS

Channels that operate under state oversight without publicly disclosing their affiliation. Uncovering their connection to the state requires a combination of evidence to reveal hidden patterns of influence or indirect control.

 Examples: Channels run by intelligence services, controlled by individuals with strong ties to the government or ruling party, or media outlets editorially directed or overseen by state actors. ATTRIBUTED
NON ATTRIBUTED

STATE-ALIGNED CHANNELS

Channels that cannot be directly attributed to state control or funding and therefore remain unattributed but show systematic signs of alignment with a state entity. They fall into this category until more evidence emerges to confirm attribution to state infrastructure.

 Examples: Portal Kombat, False Façade, Paperwall.







TECHNICAL EVIDENCE

Public affiliation

· Direct statements or self-attribution

Financial records

· Documentation of financial or operational links

Shared infrastructure

- □ Backend data
- □ IP addresses
- Hosting services
- Domain ownership
- Metadata analysis of files
- ☐ Geolocation
- ☐ Ad networks
- Cryptocurrency wallets and unique identifiers for commercial services
- Matching patterns in accounts creation dates and names
- Use of same code/templates
- Autonomous System Numbers
- Social Credit Numbers
- Indexed or archived internet content

BEHAVIOURAL EVIDENCE

Systematic interaction and amplification patterns

- Persistent backlinking, automated republishing, mirroring content and information laundering using copy-pasting or automated translations
- Reiterated engagement using cross references, reshares, likes and comments

Reiterated use of inauthentic media assets

 Patterns of impersonation or inauthentic accounts, such as Al-generated accounts

Coordinated messaging

- Linguistic patterns such as similar phrasing or terminology
- Synchronised publication time and alignment with specific time zones
- Agenda-setting and aligned cross-posting across multiple platforms at similar timestamps
- Systematic use of AI tools to generate content
- Recurrent use of certain hashtags
- Branding and visual similarities

Historical consistency and interaction with other operations

□ Repeated playbooks. Activity aligned with known patterns from other campaigns

CRITERIA: INDICATORS PER CATEGORY

State official channels

Channels attributed to a state based on technical evidence of funding, ownership and editorial control based on Open Source indicators.

· Self-attributed channels to the Government

State-controlled outlets

Channels attributed to a state based on technical evidence of funding, ownership and editorial control based on Open Source indicators.

- · Self-attributed channels to state media
- Alternative domains used by state-controlled media sharing infrastructure with the original channel (such as IP addresses, hosting services, or domain ownership)

State-linked channels

Channels attributed to a Threat Actor based on access to high-confidence indicators (mostly from proprietary or classified sources) and combined with medium-level Open Source indicators.

- Financial records providing state funding
- Shared infrastructure detected through proprietary and classified information
- Combination of technical and behavioural indicators linking new channels to previously attributed state-linked infrastructure (e.g., shared infrastructure, systematic interaction and amplification, coordinated messaging and historical consistency with attributed operations)

State aligned channels

Channels aligned with Threat Actors' activity according to a combination of medium-level indicators (mostly based on Open Source information).

- Combination of technical and behavioural indicators showing strong, repetitive patterns of alignment with FIMI-attributed infrastructure:
- Shared infrastructure
- Systematic interaction and amplification
- Reiterated use of inauthentic media assets
- Coordinated messaging
- Historical consistency and interaction with other operations



N-ATTRIBUTED

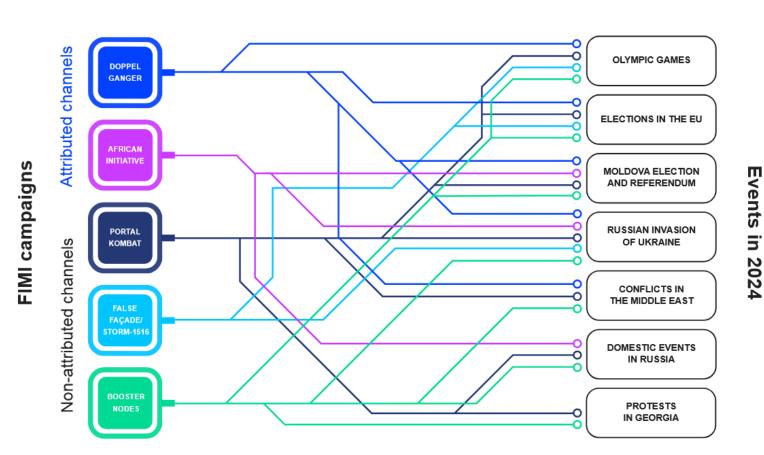
Entities in the FIMI Architecture





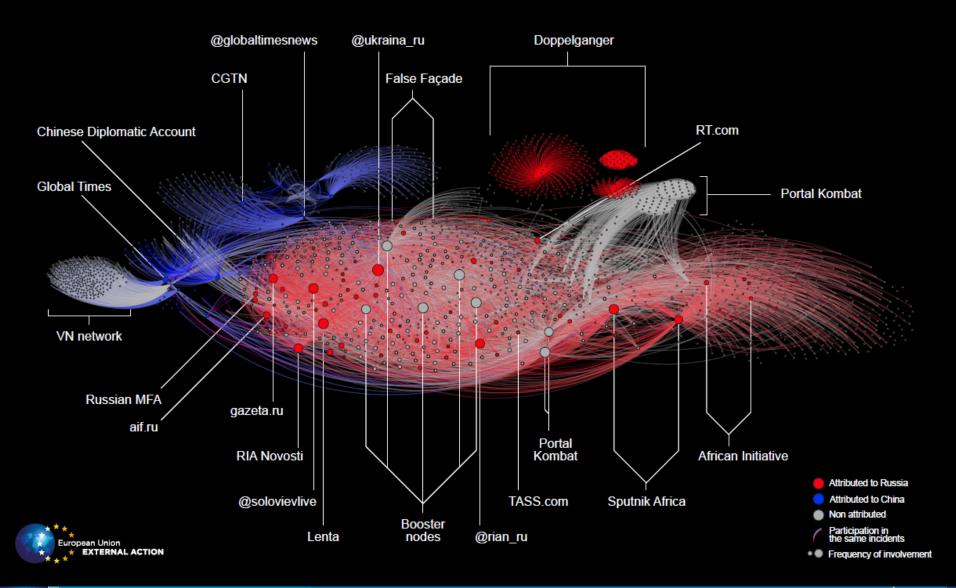
FIMI activities in 2024

Covert FIMI operations exploiting events in 2024

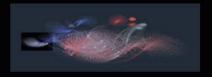




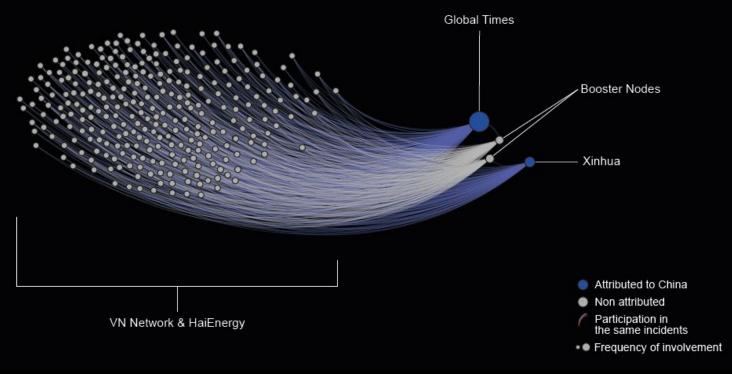
The galaxy of FIMI operations







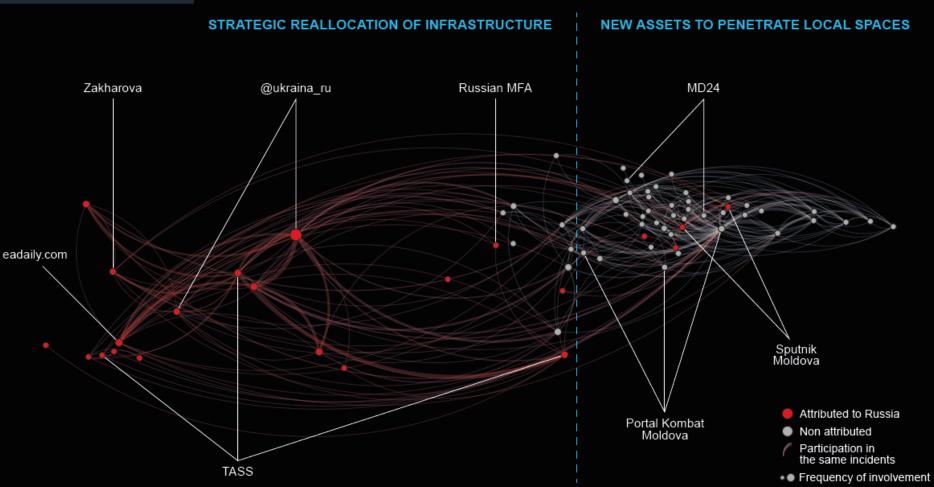
Chinese influence-for-hire operations



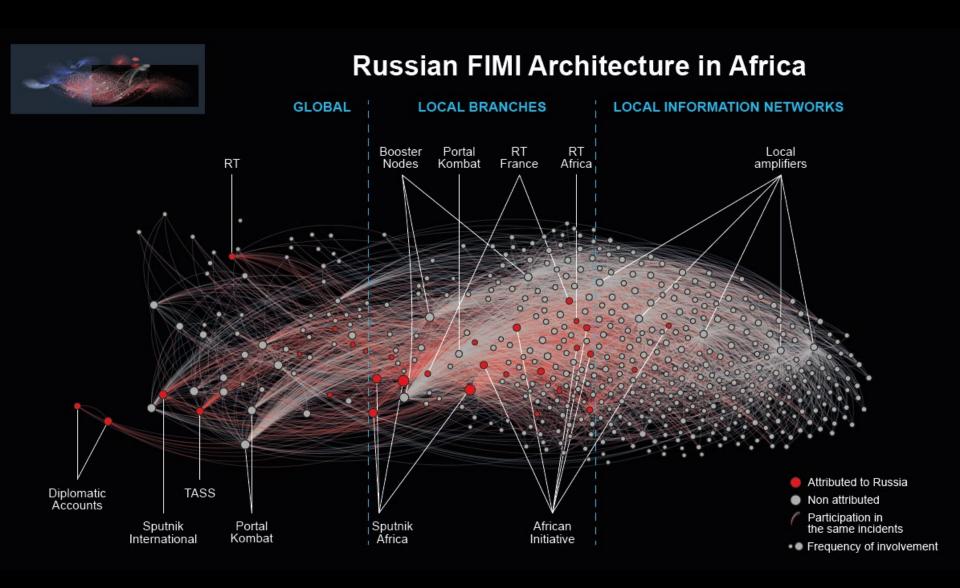




FIMI Architecture in the Moldovan elections









STRAT-DATA-ANALYSIS@eeas.europa.eu