PRESS RELEASE

December 2024

INSIGHTS FROM ATHENA LANDMARK STUDY ON FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

The ATHENA consortium of 14 partners from 11 countries has responded to the European Democracy Shield initiative. Based on the analysis of 32 case studies of foreign information manipulation and interference (FIMI) and analysis of the tactics, techniques and procedures (TTPs) used by attackers, the consortium provided policy recommendations. A landmark report with The ATHENA report on manifestations of FIMI was more than a year in the drafting, has 1,400 footnotes - an indicator of the numerous articles, newspaper stories, blogs, reports, speeches consulted by partners - including in-depth interviews with more than 20 experts making original contributions in the European fight against FIMI.

Key insights

Adapting to evolving tactics: vigilance against the FMI actors

FIMI actors use a wide range of TTPs and platforms to evade detection and to spread their messages. Defenders need constant vigilance and adaptation of countermeasures as malicious actors' tactics evolve.

- The range of case studies indicates a proliferation and inventiveness of TTPs employed by FIMI attackers. Consequently, attribution is a challenge. Some attackers cover their tracks well or engage in deniability. FIMI analysis requires an understanding of the different types of attackers in disinformation campaigns, their motivations and the TTPs they use. The ATHENA consortium analyzed FIMI cases from Russia, China, North Korea, Turkey, Saudi Arabia, Iran, and India, finding Russia to be engaging in FIMI more than any other country.

Unwitting allies of FIMI: role of ‘useful idiots’ in FIMI

Success of these campaigns often hinges on "useful idiots", individuals who unwittingly support a cause or agenda—often political or ideological—without fully understanding its implications, particularly when that cause is manipulative or harmful. The phrase was used to describe Western sympathisers of Soviet communism during the Cold War. The term is used more broadly now to describe people who, in their enthusiasm or naivety, support movements, organisations or regimes that ultimately manipulate or exploit them.

Amplifying distrust and weakening alliances

Attackers effectively employ information warfare techniques (such as content distortion and exploiting breaking news events) to amplify distrust within the EU, weaken transatlantic alliances and promote politicians sympathetic to their causes.

- Various threat actors, including state-sponsored groups, criminal organisations, hacktivists and individuals with malicious intent sometimes work together without any agreements because it suits their shared, but uncoordinated objectives. Exploiting an infrastructure that allows them to conceal their identity through anonymity, FIMI attackers find in social networks a fertile ground to cultivate and proliferate their propaganda.

Although FIMI is frequently associated with elections, it has a much broader reach and continues to thrive even after the European Parliament (EP) elections of 9 June 2024. There remains a growing threat to democratic society. The actual impact of a FIMI campaign is uncertain. The effectiveness of these campaigns and the impact of Western countermeasures remain subjects of ongoing analysis and debate.

The ATHENA case studies showed that social networks played a key role in distributing disinformation, frequently paired with distorting facts (53.3%) and leveraging existing narratives (50%). This reinforces the role of **social media as a primary conduit for disinformation, designed to distort facts, overwhelm users and reinforce misleading content.**

Among the best defences against disinformation is transparency, effective communication and the use of counter-narratives that challenge disinformation targeting the European Union. Evaluating different disinformation incidents implies being self-critical and taking seriously the relationship of trust between European institutions and the societies of the different Member States.

The EU has developed various measures to combat disinformation, including the EU Cybersecurity Strategy[1] and initiatives through the European Centre of Excellence for Countering Hybrid Threats[2].

[1] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[2] https://www.hybridcoe.fi/

Recommendations

- A multifaceted countermeasure to disinformation Effective countermeasures against disinformation campaigns require a multi-faceted approach, involving cooperation between governments, social media, civil society and the public. However, this whole-of-society approach can be realistically achieved only if the stakeholders engaged in countering FIMI share a common "language" such as the DISARM[3] and STIX[4] frameworks to harmonise the monitoring, analysis, assessment and response to FIMI operations.

Building a critical citizenry:

Governments and civil society organisations (CSOs) should focus on media literacy initiatives to help citizens critically assess news sources and evaluate the credibility and motives behind information them. Individuals should be encouraged to question information in public campaigns. For specific actions taken in response to FIMI attacks, citizens and practitioners alike should be able to consult official sources or reports from credible research institutions, project consortia and think tanks that focus on disinformation and cybersecurity.

Promoting factchecking EU Member States should promote image and video fact-checking skills to help individuals identify manipulated content and other forms of digital deception. **Educating citizens, including school-age children, about FIMI tactics can help them act as a first line of defense, significantly reducing the spread and impact of false information.**

- Rapid response disinformation team Governments should establish rapid-response teams trained to debunk FIMI as soon as it emerges. Such teams should comprise government officials, academics, CSOs and fact-checking journalists. Governments should strengthen monitoring mechanisms, improve transparency and work more closely with fact-checking organisations to mitigate the impact of FIMI.

Urgent investments in multilingual tools

The European External Action Service (EEAS), the EU's foreign service, should prioritise investment in **multilingual tracking tools capable of detecting FIMI across different languages.** This would allow for faster identification of manipulative content in different linguistic and regional contexts.

Knowledge sharing

The EC should encourage EU-funded projects addressing FIMI to network and share knowledge with other similar projects in the Member States, the US, Canada, Australia, Japan, Latin America and other countries resisting foreign information manipulation and interference.

For the more detailed conclusions and recommendations from the case studies, see the **briefing paper** which can also be accessed at the ATHENA website, where you can learn more about the project.

---

[3] https://disarmframework.herokuapp.com/
[4] https://oasis-open.github.io/cti-documentation/stix/intro.html

Consortium

CONTACT

Email: athena.comms@trilateralresearch.com

Funded by the European Union (grant number 101132686). UK participants in Horizon Europe Project ATHENA are supported by UKRI grant number 10107667 (Trilateral Research). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA) or UKRI. Neither the European Union nor the granting authority nor UKRI can be held responsible for them. HORIZON-CL2-2023-DEMOCRACY-01.