Office of the Prime Minister of the Republic of Armenia

Disinformation, Foreign Information Manipulation and Interference (FIMI): Awareness Guide during the Electoral Process

Introduction and background

The evolution of the information environment from the beginning of the century, including the globalisations of exchanges and the rise of social media, has given a fertile ground for the weaponisation of information by state threat and non state-actors to serve their agenda. As a core component of the "hybrid" threats arsenal, Foreign Information Manipulation and Interference (FIMI) is a strategic weapon deployed by hostile actors in a systematic and coordinated manner. It aims notably at undermining the functioning of democratic processes or influencing decision making of individuals and societies.
Autocratic states actors and their proxies frequently use FIMI, including disinformation, to target elections and influence the outcomes according to their interests. Information manipulation can distort democratic debate, fuel mistrust and polarisation in society, exacerbate crises to spread fear and confusion.
These guidelines on countering FIMI aim at raising awareness on the risks; exposing the most common techniques during electoral processes; and providing some key resilience mechanisms.

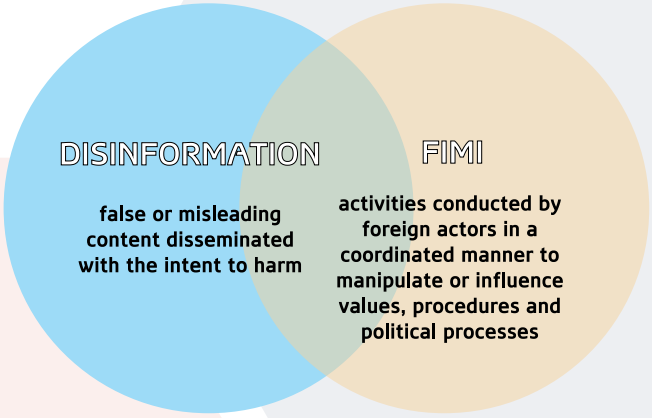
Why it matters for Armenia ?

Armenia's complex geopolitical environment, combined with ongoing domestic political activity, has created conditions conducive to the intensification of Foreign Information Manipulation and Interference (FIMI) campaigns. Particularly over the past year, Armenia has been targeted by large-scale and coordinated disinformation campaigns aimed at influencing public sentiment, sowing panic, and undermining trust in state institutions and national security. These disinformation operations have long evolved into national security threats, and significant efforts are being undertaken to counter and neutralize them.

In the context of the upcoming parliamentary elections, a substantial increase in these information threats is expected. Electoral processes create a favorable environment for both state and non-state foreign actors to employ manipulative tactics aimed at polarizing society and delegitimizing Armenia's democratic path and electoral processes. Therefore, preventing such interference and actively countering it is of critical importance - not only for ensuring free and transparent democratic processes, but also for safeguarding Armenia's sovereignty and maintaining social cohesion.

What is Foreign Information Manipulation and Interference (FIMI)?

FIMI is a mostly **non-illegal** pattern of behaviour that **threatens** or has the potential to negatively impact values, procedures and political processes. Such activity is **manipulative** in character, conducted in an **intentional** and **coordinated** manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.
FIMI is not only disinformation and not all disinformation is FIMI. FIMI focuses on foreign actor behaviour (tactics, techniques and procedures) intentionally manipulating information. In contrast, disinformation may originate from domestic actors and mostly focuses on narratives.



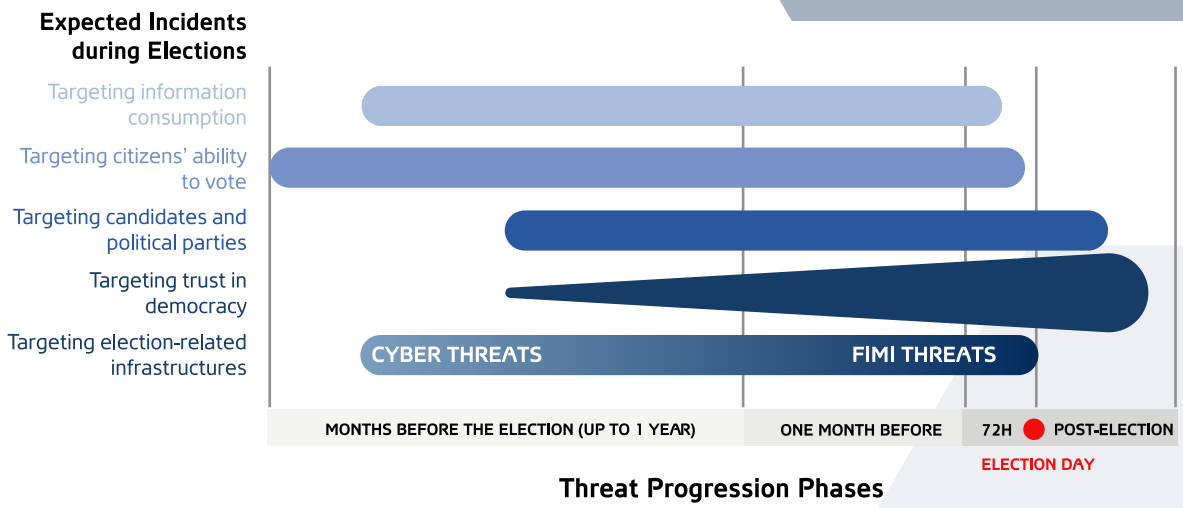
FIMI during elections

Why are elections targeted?

Elections, as the expression of democracy and its values, represent a prime target for foreign actors seeking to destabilize their functioning. These actors seek to undermine trust between citizens and the institutions responsible for representing them. This desire to destabilize electoral processes operates primarily in the lead-up to and during electoral campaign phases. Targeting elections allow threat actors to interfere in national political self-determination.

What is the timeline of a hostile campaign?

FIMI campaigns ahead of election day can follow certain phases of intensification in the long term, shaping the information environment in a constant process. Final days before elections are the most critical , as threat actors may deploy major ressources to mislead voters, notably by targeting specific candidates. However, FIMI and disinformation campaigns do not stop after election day: Threat actors can continue undermining trust in democracy, in particular the electoral process itself or question the results.



Who are the target of attacks?

Every actors of an election is a potential target of FIMI campaigns:

- Institutions and leaders
- Media and press
- International partners
- Political parties and candidates
- Civil society organisations
- Citizens

Some of the most common techniques used during elections include:

Polarization: Dividing into strongly opposing groups or opinions, where extreme views and interests confront, jeopoardizing any nuanced debate or compromis.

Emotional language: Language that contains strong emotional terms—especially those with negative effects such as fear or outrage.

Impersonation: Deceiving an audience by imitating a person or entity in order to damage their reputation, cause emotional harm, or spread manipulation.

Decontextualization: Intentionally presenting text, audio, or visual material in a different context or omitting important background information to alter its meaning.

AI generated FIMI: Using AI tools to increase the quality and quantity of manipulative content, and automatize large scale distribution.

What can you do against FIMI and disinformation?

As citizens are one of the main target audience of FIMI campaigns, each individual can follow some principles to manage the risks of FIMI and mitigate potential impact.

Read and verify content carefully before sharing it on social media or messaging platforms (“Take care before you share”).

Consider the purpose of the content: Is it factual information, a personal opinion, advertising, or spam?

Check the sources: Who created the text or website? Are the sources identifiable and trustworthy?

Verify images and videos if in doubt, for example using reverse image search tools. This helps determine whether content has been manipulated or taken out of context.

Diversify information sources: Follow a range of reputable channels and perspectives, to confront different points of view and make up your mind by yourself.

What is the role of the Prime Minister’s Office of Armenia in institutional response?

The Prime Minister’s Office in Armenia serves as a central actor in the state’s coordinated response to threats of Foreign Information Manipulation and Interference (FIMI). The main areas of coordination include:

Monitoring and Analysis
Continuous monitoring of the information environment to identify manipulative narratives, influence mechanisms, and coordinated campaigns.

Early Warning Systems
Implementation of mechanisms for the early detection of FIMI activities and rapid response.

Interagency Coordination
Cooperation with relevant state bodies (Ministry of Foreign Affairs, National Security Service, and others) to develop a unified position.

Public Communication
Transparent and timely communication aimed at reducing the impact of disinformation and strengthening public trust.

International Cooperation
Partnership with international organizations and partner states to exchange experience and develop joint response mechanisms.

Capacity Building

Training for civil servants and communication officers to strengthen their ability to recognize and counter FIMI threats.

New Tools and Platforms

The Prime Minister's Office supports the development and deployment of advanced technological solutions, such as the Stugel.am platform. Leveraging artificial intelligence, the platform simultaneously analyzes images, videos, and textual content to assess their credibility. By utilizing Natural Language Processing (NLP) and Large Language Models (LLMs), the system cross-references information in real time with highly reliable sources, ensuring the provision of trustworthy information.

Glossary

Disinformation verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm.

Tactics, Techniques, and Procedure (TTPs) in the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. "Tactics" are the operational goals that threat actors are trying to accomplish. "Techniques" are actions through which they try to accomplish them. "Procedures" are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.

Threat Actor is an organisation, a State, an individual or a group that poses a security risk by engaging in malicious activities, such as FIMI campaigns, cyberattacks or other harmful actions. Threat actors can have different motives, including financial gain, political influence, espionage or disruption.

Coordinated Inauthentic Behaviour (CIB) involves organised, deliberate and manipulative efforts to mislead audiences by using multiple fake or inauthentic accounts, working together to spread certain messages.

Troll(s) and bot(s)– In the context of FIMI, a troll refers to an individual(s) (or automated account - bots) that deliberately posts inflammatory or misleading content online to provoke emotional responses and sow discord. Trolls are often part of larger influence operations and may act independently or as coordinated agents within 'troll farms' or influence networks.

Yerevan

2026