Institute of Communication Studies

Guidelines:
Government response to Foreign Information Manipulation and Interference (FIMI) in North Macedonia



This guideline provides the government of North Macedonia with a strategic framework to address Foreign Information Manipulation and Interference (FIMI). The main objective is to build a society that is more resistant to disinformation over time while simultaneously protecting national security and freedom of speech. To ensure this framework remains effective, the government must commit to the ongoing investigation of FIMI operations, using lessons learned from past interference to constantly refine and reinforce its defensive measures.

Section 1: why FIMI is a national threat

To protect society, the government must define FIMI as a national security threat. In order to do so effectively, the concrete characteristics of FIMI must be explained, based on past operations that have targeted both North Macedonia and the broader European region. By analyzing these recurring patterns, we can categorize the danger through four distinct lenses: the source, the manner, the objective, and the impact.

1. The Source

It is vital to distinguish between domestic disinformation and international interference. While domestic disinformation is spread by internal actors such as local politicians or influencers for domestic gain, FIMI is driven by actors linked to a foreign state. FIMI typically flows through a complex network designed to hide its true origin.

- Official State Channels: These are verified foreign government accounts, such as diplomatic profiles on social media, used to push state agendas.

- State-Controlled Media Outlets: Rather than independent organizations, these function as propaganda apparatuses - such as RT and Sputnik - which are funded by foreign states and lack editorial independence.

- Hidden Aligned Channels: This includes a "shadow" network of social media influencers, proxy websites, and automated bot accounts that do not publicly disclose their foreign ties but perfectly mirror state narratives.

2. The Manner

FIMI is defined by deceptive behavior and operating methods rather than just the content of the message. These actions are specifically designed to trick users and manipulate the technical infrastructure of digital platforms.

- Digital Mimicry: Creating "clone" websites that look identical to trusted news sources to fool readers, such as the Doppelgänger operation which mimicked major European outlets including Le Parisien and Le Figaro in France, Der Spiegel and Bild in Germany, La Stampa in Italy, Gazeta Wyborcza in Poland, and El Mundo in Spain.

- Coordinated Inauthentic Activity: Using "bot farms" to post the same message simultaneously to trick algorithms into making a topic trend or spread disinformation. For example: The Team Jorge investigation by investigative collective Forbidden Stories revealed a software suite which allowed operators to control over 30,000 sophisticated, verified bot profiles across multiple social media platforms to manipulate public opinion and elections worldwide.

- Hack-and-Leak: Stealing private information and releasing it strategically to damage a target's reputation, a method often used to disrupt election integrity. For example: during the 2016 US election, stolen campaign emails were leaked to manipulate public opinion.

- Deepfakes: Using AI to create realistic but fake video or audio of leaders to cause confusion or panic. World leaders and political figures are constantly targeted by deepfakes in disinformation attacks

3. The Objective

The goals of FIMI vary depending on the actor's place in the network, ranging from high-level state strategy to low-level profit.

- Political Gain: Foreign governments aim to destabilize rivals or influence major decisions. FIMI operations peak during critical milestones. In North Macedonia: In 2018, disinformation was used to undermine the Prespa Agreement - the treaty that resolved a long-standing name dispute with Greece to allow for Euro-Atlantic integration. In Romania: During the 2024 elections, foreign interference utilized high-volume coordinated social media campaigns to manipulate the electorate.

- Financial Gain: Disinformation is often a business model where "small entrepreneurs" are paid by the click. The Veles Case: Teenagers in North Macedonia produced pro-Trump content ahead of the 2016 US election because sensationalist lies generated high advertising revenue.

4. The Impact

Beyond immediate political influence, the ultimate impact of FIMI is the systematic erosion of a country's "social glue." By flooding the information environment with contradictions, these operations foster a deep distrust that leads citizens to doubt even legitimate democratic institutions. Furthermore, FIMI poses a direct threat to public safety; during crises like a pandemic or security emergency, foreign disinformation can mislead the public on safety protocols, potentially triggering civil unrest or public health disasters.

Section 2: how to identify FIMI?

Identifying FIMI requires a shift in focus. Instead of trying to monitor or control what people say, we analyze the specific Tactics, Techniques, and Procedures (TTP) used to spread the message. By breaking an operation down into these three layers, authorities can recognize foreign interference even when the content itself is not illegal.

1. Tactics (the strategy)

Tactics are the "why" of an operation. They are the strategic goals that a foreign actor wants to achieve, such as 'dividing the public' or 'damaging trust in institutions'.

- Example: During the Prespa Agreement negotiations, the strategic tactic was to undermine North Macedonia's path toward the EU and NATO by creating deep divisions in society.

2. Techniques (the method)

Techniques are the specific "tricks" or methods used to carry out a tactic. This layer describes the way the actor masks their identity or pushes their message forward.

- Example: Digital Mimicry is a common technique where actors create fake versions of trusted websites to make propaganda look like real news.

3. Procedures (the execution)

Procedures are the most detailed part of the analysis. They are the step-by-step technical actions and specific tools used to run the operation. This involves the specific software, the timing of posts, and the technical setups required.

- Example: Using a software suite to manage thousands of fake profiles at once - as seen in the Team Jorge investigation - is a specific procedure for 'coordinated inauthentic behavior'.

By documenting these patterns, the government can build a playbook of interference. This allows security agencies to identify an attack based on red flags, providing a clear reason to act without interfering with the legal right to free speech.

Section 3: how to treat FIMI?

A successful response to FIMI not only lies in debunking disinformation, as engaging with foreign lies often just spreads them further. Since corrections such as fact checking not always reach everyone or change their minds, the government must move from reacting to being proactive. This means building a "psychological defense" through prebunking to help citizens spot manipulation before it takes root. By involving the whole of society, the state can protect the information environment without resorting to censorship. Ultimately, this approach strengthens national security while keeping democratic values safe.

1. Prebunking

While debunking (correcting a lie after it has spread) is a necessary reactive tool, it is often less effective because the original lie has already taken root in the public's mind. Prebunking involves teaching citizens to recognize the tricks of manipulation - such as emotional triggers or the use of fake experts - before they encounter the disinformation. By informing the public about the methods used in FIMI, the government builds long-term resilience for society, making disinformation less impactful when it appears. This can be achieved in multiple ways.

- Gamified Learning: Interactive tools, like the game 'Bad News' allow users to play as a bad actor. By using manipulation tactics to gain fake followers, players learn to spot those same red flags in their own feeds.

- Explainer videos: short, neutral videos that explain common manipulation tricks rather than specific stories. For example: a video might explain 'scapegoating' so that when someone sees an attack using that trick, they recognize the technique immediately.

2. The 'Do No Harm' principle

Any government action must be carefully balanced to protect national security without infringing on freedom of speech.

- Avoid Over-Regulation: strict laws often trigger a 'chilling effect' where platforms over-delete content to avoid heavy fines, which stifles healthy public debate. To prevent this, governments should move away from banning content and instead demand higher transparency, such as public advertising repositories that disclose who paid for manipulative ads. This approach encourages platforms to use labels and warnings - similar to Meta's fact-checking banners - to inform users about potential disinformation without silencing them or removing their posts.

- Target the 'How', not the 'What': the government should focus on stopping the 'machinery' behind the lies. This means targeting 'bot farms' and fake accounts rather than individual opinions, as it is much safer for democracy to delete 10,000 computer-run profiles than to censor one real citizen. By using laws like the Digital Services Act (DSA), the state can pressure social media companies to secure their own platforms so they can no longer be exploited by foreign actors.

- Independence: to ensure that anti-disinformation efforts are never misused for political gain, oversight must be handled by independent agencies. This includes fact-checking

networks, trusted media as well as NGOs (such as Alliance4Europe) that act as watchdogs to protect digital rights. By empowering independent experts instead of politicians, the state ensures that actions only target real foreign threats. This prevents anti-disinformation tools from being misused for political gain.

3. The whole-of-society approach

FIMI is a complex threat that cannot be solved by a single ministry; it requires a coordinated national strategy. The government should establish a unified body involving Foreign Affairs, Defense, Internal Affairs, and Education to share intelligence and plan responses. By communicating transparently to independent media and NGO's , the state strengthens media literacy and builds a more informed public without government interference.

Building a resilient society requires a commitment to education at every level. The Ministry of Education must integrate media literacy into schools, focusing on how democratic systems work and how narratives are used to manipulate history or science. The Ministry of Information Society should focus on digital skills, helping citizens understand how platform algorithms work and how to identify bot-driven "viral" trends.

4. International cooperation

FIMI is a cross-border threat that requires a network to fight a network. By syncing with European frameworks, North Macedonia can access advanced tools and ensure its media environment meets international democratic standards.

- The FIMI Toolbox: The government should adopt the EU's FIMI Toolbox, which includes monitoring, detection, rapid alert systems, and diplomatic responses like sanctions on foreign state-sponsored media.

- Strengthening Self-Regulation: Encouraging media to follow professional ethics codes and even apply for cooperation and membership of the European Fact-Checking Standards Network (EFCSN) or the global International Fact Checking Network (IFCN).

By adopting this proactive and inclusive model, North Macedonia can defend its national security while strengthening - rather than weakening - the democratic rights of its citizens.

Institute of Communication Studies



British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This document is prepared within the programme Strengthening the Operational Readiness for Government Response to FIMI in North Macedonia funded by the UK Government with the support of the British Embassy Skopje. The content of this publication does not necessarily reflect the position or the opinions of the UK Government.