# **Foreign information manipulation and interference (FIMI) with politics and elections:** signs, examples, and implications for Ukraine



Ambasáid na hÉireann | An Úcráin
Embassy of Ireland | Ukraine
Посольство Ірландії | Україна

This report was drafted within the project "Inclusive Dialogues For Democratic Reform in Ukraine" funded by the Ministry of Foreign Affairs and Trade of Ireland but the opinions expressed herein do not necessarily reflect the official position of the Irish Government.

**AUTHORS:**

**Olha Kotsiuruba** PhD in Law, Senior Legal Advisor at Civil Network OPORA

**Bohdan Mokhonchuk** PhD in Law, Legal Advisor at Civil Network OPORA, Associate Professor at the Department of the Constitutional Law of Ukraine, Yaroslav Mudryi National Law University

**Vasyl Lutsyk** PhD in Law, Vice-Rector for Academic Work at the State Tax University

# TABLE OF CONTENTS


**LIST OF ABBREVIATIONS** . . . . . 2

**CHAPTER 1. TYPES AND FORMS OF FOREIGN INTERFERENCE** . . . . . 3

1.1. What is “Foreign Interference”? . . . . . 3

1.2. What forms can foreign interference take? . . . . . 7

**CHAPTER 2. DEBATABLE SIGNS OF FOREIGN INTERFERENCE AND FIMI** . . . . . 12

2.1. Are Coercive or Illegal Actions Always a Sign of Foreign Interference? . . . 12

2.2. How to Differentiate Foreign Interference From Foreign Influence? . . . . . 15

2.3. How to determine the foreign nature of foreign interference, and whether it is necessary to attribute it to a specific state? . . . . . 17

2.4. Is it possible to draw a line between FIMI and freedom of expression? . . 21

**SECTION 3. CHARACTERISTICS AND IDENTIFICATION OF FIMI** . . . . . 24

3.1. What are the characteristics of FIMI, and how does it relate to disinformation? . . . . . 24

3.2. How to identify FIMI? . . . . . 30

**CHAPTER 4. FIMI METHODS AND EXAMPLES** . . . . . 36

4.1. How can actors and assets be manipulated? . . . . . 36

4.2. How can content and promotion be manipulated? . . . . . 43

4.3. What targets of FIMI operations should be expected in Ukraine? . . . . . 49

**CONCLUSIONS AND RECOMMENDATIONS** . . . . . 58

Conclusions . . . . . 58

Recommendations . . . . . 62

**ANNEX** . . . . . 71

# LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| **AI** | — | Artificial Intelligence |
| **CCD** | — | Center for Countering Disinformation |
| **CEC** | — | Central Election Commission |
| **CIB** | — | Coordinated Inauthentic Behavior |
| **CSO** | — | Civil Society Organizations |
| **DHS** | — | Department of Homeland Security |
| **EC** | — | European Commission |
| **ECHR** | — | The European Court of Human Rights |
| **EEAS** | — | The European External Action Service |
| **EP** | — | European Parliament |
| **EU** | — | European Union |
| **FFI** | — | Foreign Financial Interference |
| **FIMI** | — | Foreign Information Manipulation and Interference |
| **IDEA** | — | The International Institute for Democracy and Electoral Assistance |
| **National Council** | — | National Council of Ukraine on Television and Radio Broadcasting |
| **NSDC** | — | National Security and Defence Council of Ukraine |
| **OECD** | — | Organisation for Economic Co-operation and Development |
| **OSCE ODIHR** | — | the Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe |
| **SSU** | — | Security Service of Ukraine |
| **Target state or recipient state** | — | a state that is subject to foreign interference or influence |
| **UNO** | — | United Nations Organization |
| **USC** | — | United States Code |

# CHAPTER 1.

# TYPES AND FORMS OF FOREIGN INTERFERENCE

## 1.1. WHAT IS "FOREIGN INTERFERENCE"?

The problem of combating foreign interference has been actively discussed since the establishment of the UN. In particular, the non-interference principle with a state's affairs is enshrined in the UN Charter and detailed in the 1970 Declaration on Principles of International Law (UN GA Resolution 2625 (XXV)). The principle implies the following:

- each state has an unalienable right to choose its own political, economic, social, and cultural system without interference of any kind from any other state;
- no state may either apply or encourage the application of economic, political, or any other measures with the aim of subjugating another state in the exercise of its sovereign rights and deriving any advantage therefrom;
- no state shall organize, instigate, finance, incite, or permit subversive, terrorist, or armed activities aimed at the violent overthrow of the government of another state, nor shall it facilitate such activities or interfere in civil conflicts within another state.

Elections, as a form of direct democracy and a means of legitimizing authority, are at the heart of these "internal affairs." Among experts, there are differing views on which principle is violated by foreign interference in another country's electoral process — non-interference or self-determination. However, regardless of the approach, we believe that foreign interference violates the principle of sovereignty (it may simply shift the emphasis from the state, in the case of non-interference, to the people, in the case of self-determination).

That is why it is a widespread practice to restrict the political rights of foreigners, especially on matters of national significance, such as active and passive voting rights, the ability to run election campaigns, the ability to fund election campaigns, and membership in political parties. Since citizenship is a political and legal link to the state, and political rights are, by definition, related to the exercise of power within a country, exceptions to citizenship requirements are provided for in international instruments (see par. 26 of the Code of Good Practice for Political Parties; par. 1.1.b. of the Guidelines of the Code of Good Practice in Electoral Matters; the Convention on the Participation of Foreigners in Public Life at Local Level) only for ensuring political participation of foreign nationals on the local level, specifically, as it is stipulated in Art. 40 of the EU Charter of Fundamental Rights, however, only for EU citizens (in other words, the supranational political and legal relationship is taken into account). At the same time, not all countries support the exceptions from citizenship for all foreigners, since, for instance, the Convention on the Participation of Foreigners in Public Life at Local Level was ratified only by 9 member states of the Council of Europe.

At the same time, understanding of foreign interference, its forms and correlation with the lawful influence has not ceased to be a subject for debate, which can be seen illustrated in the OECD 2024 report:

1. European Commission (EC). The definition of foreign interference was provided by the EC in the working document on research and innovation adopted in 2022: "Foreign interference includes activities that are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU)".

2. European Parliament (EP). The definition of the EP is more detailed: "Foreign interference means any illegitimate interference by foreign powers in the democratic and political processes of the EU and Member States. It includes covert or coercive interference by a foreign power in the political or governmental system from within, such as politicians and officials who are working for or under the influence of overseas regimes; influence on the political system from without, such as abuse of the lobbying system, corruption, espionage, cyber-attacks; and manipulative influence on public engagement or views, through online disinformation and manipulation campaigns."

3. Department of Homeland Security (DHS). It defines foreign interference as "malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias

the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."

4. United States Code (USC). The term "foreign malign influence" in 50 USC § 3059(f)(2) is defined as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means — (A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States."

5. Ministry of Internal Affairs of Australia. Foreign interference is understood as "activities carried out by, or on behalf of, a foreign power, that are coercive, corrupting, deceptive or clandestine, and contrary to Australia's sovereignty, values, and national interests. These activities involve foreign powers trying to secretly and improperly interfere in the Australian society to advance their strategic, political, military, social, or economic goals, adversely affecting individuals, information and infrastructure of governments, industry, academia, the media, and communities."

6. Government of Canada. Foreign interference is defined as "activities perpetrated by a foreign state, or proxy, that are harmful to Canada's interests and are clandestine or deceptive, or involve a threat to any person." Malign foreign influence is defined as "a covert or non-transparent undertaking by, at the direction of, on behalf of, or with the substantial support of a foreign principal, with the objective of exerting influence and affecting outcomes." Foreign principal refers to an entity that is owned or directed, in law or in practice, by a foreign government.

OECD suggests a somewhat similar definition: "Foreign interference is defined as intentional actions of state or non-state actors conducted in the interest of a foreign government. These activities are covert, non-transparent or manipulative in nature, and are aimed at negatively impacting the structures of processes of the political system, the economy, the society or the informational space." At the same time, it is emphasized that kinetic operations, such as sabotage attacks, targeted assassinations and terrorist actions, as well as overt and covert military operations, are excluded from the scope of this definition.

All these definitions are rather broad, but share certain commonalities:

- Subject. Each definition explicitly provides that the state may carry out such interventions through intermediaries: "someone on behalf of" (EC), " at the direction of, or on behalf of or with the substantial support of" (USA, Canada), "on behalf of" (Australia), "by a proxy" (Canada), "in the interest of" (OECD) a foreign state.

- Modus operandi. The EC and Australia are using almost identical wording: coercive, clandestine, deceptive, or corrupting. Clandestinity and deception are mentioned in various forms in the documents of the EC, EP, Australia, Canada, and OECD. These attributes are not found in the texts of DHS, and are not formally mandatory in the USC (where it says "through overt or covert means").

However, the definitions also have certain differences:

- Object and goal. Some of the targets of foreign interference include the sovereignty, values and interests (EC, Australia), interests of the state (Canada), and its allies (DHS), politics and public opinion (USC), democratic and political processes (EP), political system, the economy, society or informational space (OECD). In some cases, it is only about the overall influence on the target (USC, Canada), while in others, a more detailed list of goals the actor intends to achieve, such as sowing discord, manipulation of social discourse, discrediting the electoral system, biasing the development of policy (DHS); advancing their strategic, political, military, social, or economic goals (Australia).

- Illegality. Some definitions describe foreign interference as illegitimate (EP) or malign (DHS) actions. In the case of Canada, two concepts are highlighted: foreign interference and malign foreign influence.

In our opinion, the object of interference can be broadly divided into general and specific categories. The general object is state sovereignty. Without delving into a detailed analysis of the characteristics of state sovereignty and related values, we can ascertain that, through its interference, one state attempts to influence another (the target or recipient state) in matters that the latter must resolve autonomously and independently. Therefore, the general object of foreign interference is generally encompassed by the concept of sovereignty.

A specific target of foreign interference may encompass social relations in various spheres — ranging from the activities of politicians or government officials to religious or other nongovernmental organizations. In addition, a specific target may often

be hybrid in nature (for example, two polarized groups that are both religious and electoral in nature). However, to ensure that this report has clearly defined boundaries, it will focus on those forms of foreign interference where the primary target is social relations in the electoral sphere, as well as, to some extent, the activities of politicians (potential candidates who have not yet registered) and political parties (where such activities are systemically linked to elections). The issue of "illegality" as an indicator of foreign interference is more complex and raises a number of interrelated questions; therefore, it will be addressed in a separate section below.

## 1.2. WHAT FORMS CAN FOREIGN INTERFERENCE TAKE?

As mentioned above, a study conducted at the request of the EU suggests that foreign interference can take place covertly or coercively: from within — in the political or state system, in particular through politicians and officials who act in the interests of foreign regimes or are under their influence; from the outside — into the political system, particularly through the abuse of the lobbying system, corruption, espionage, and cyberattacks; as well as through manipulative influence on civic activities or public opinion — for example, through online disinformation and manipulative campaigns.

The OECD notes that foreign interference is constantly evolving, which is why it is developing a classification of the various channels through which foreign states can covertly and adversely influence political processes, the economy, or society. The OECD classifies such channels as the following:

- elite capture — the aim is to establish a relationship of subordination with political, economic, media or civil society elites (among the many tools used — corruption, undue influence, the offer of gifts and other benefits, or the professional mobility of public decision-makers in foreign entities);
- the financing of political life — it is necessary for democratic functioning; political financing is one of the main sources of undue influence and political capture in general;
- electoral interference — may take a variety of forms, which have already been documented, aimed at manipulating the electoral process itself, from the campaign to the results;

- foreign information manipulation — campaigns to manipulate information have become common in an increasingly digital and globalized information environment, and can take various forms:
  - use of state media from a foreign power (e.g., Sputnik, Russia Today, Xinhua or CCTV);
  - investment in the media;
  - creation and financing of websites sharing disinformation;
  - using 'troll farms' and bots on social networks;
  - involvement of influencers and journalists under foreign influence;
  - the use of AI technologies;
- economic coercion — international trade and investment offer a wide range of opportunities for foreign interference in today's globalized and interdependent world;
- misuse of academic and cultural co-operation, civil society organizations and think tanks — they can be used as channels for foreign interference, whether directed at the ideas conveyed, the individuals (researchers, students, influencers, artists) or institutions themselves;
- transnational control, surveillance and repression of diasporas — diaspora communities can offer several opportunities for interference, ranging from influencing local or national politics, to using diaspora businesses as a means of financing interference activities, or manipulating individuals involved in politics, administration or strategic economic sectors.

Thus, OECD identifies foreign interference with elections as a separate channel. At the same time, they specify that to achieve this, foreign states use political financing, the dissemination of misleading narratives through disinformation campaigns, misleading campaigns, or cyberattacks against candidates, as well as the funding of targeted advertising to promote specific candidates or simply undermine trust in the target country's democratic system. However, under this approach, the very same tools that are identified as separate channels are used for foreign interference in elections, which blurs the distinction between them and renders it meaningless.

In our opinion, elections are the domain of social relations that can be targeted by foreign interference. At the same time, informational manipulations (FIMI), foreign financing (FFI), cyberattacks and other similar incidents may be treated as separate

forms of carrying out such interference. To characterize the behavioral pattern of FIMI agents, EEAS refers to the concept of TTP(s), i.e. "Tactics, Techniques, and Procedures". Tactics describe the operational objectives that threat agents seek to achieve. Techniques are the actions they use to achieve these objectives. Procedures represent a specific combination of techniques within several tactics (or stages of an attack), which indicates a specific intent and may be unique to different threat agents. In general, tactics refer to the intermediate goals (objectives and targets) of an interference; techniques refer to the methods used (actions or a combination thereof); while procedures refer to the combination of methods used to achieve intermediate goals, which are employed at various stages of an operation to achieve the overall goal and are characteristic of specific FIMI agents.

For instance, the EEAS report describes an operation related to the explosion near Przewodów in Poland on November 15, 2022. The Russian FIMI ecosystem shared a screenshot of a Facebook post from the deleted fake account pretending to be an ex-mayor of Lublin, and claimed that a missile explosion was a provocation by Ukraine. In TTP(s) terms, the tactic was the twisting — the distorting the perception of an event and imposing a desired narrative, the technique was impersonation of a legitimate entity and the subsequent dissemination/amplification of content through channels within the Russian FIMI ecosystem, and the procedure — a specific combination of these techniques: creating a fake profile, posting a fabricated message through it, and having that message picked up and spread by Russia-linked channels. However, for the sake of convenience, we will use the more common term "methods," which is substantively similar to "tactics" as understood by the EEAS.

As a starting point for our risk analysis, we will use the forms of foreign interference identified in the Central Election Commission's Concept for Countering Foreign Interference in Elections in Ukraine (CEC Concept)approved by the Resolution No.41 of July 14, 2026. It emphasizes that there are numerous forms of interference through which foreign states, their representatives, or private entities can influence the electoral processes of other countries (ranging from disinformation campaigns and cyberattacks to the manipulation of election results and financial interference). At the same time, the CEC's Concept is the first comprehensive document in Ukraine on countering foreign interference in elections, which was approved by a regulatory decision, and which shall become a basis for specific organizational decisions, plans, protocols, and training.

In particular, the CEC identifies the following forms of foreign interference:

- cyberattacks on the electoral information infrastructure, electronic communication systems of election administration bodies, and other government

agencies that interact with election commissions during the organization, preparation, and conduct of elections;

- the dissemination of disinformation and foreign information manipulation and interference (FIMI), including through the use of AI technologies, carried out, in particular, by spreading false or distorted information via the media and information-sharing platforms (Facebook, Instagram, X, Telegram, etc.), the creation and dissemination of fake audiovisual content (deepfakes) and other means of informational influence aimed at manipulating public opinion, promoting foreign interests and anti-democratic narratives, and influencing electoral processes and election results;

- financial interference carried out through the bribery of voters, direct or indirect financing of political parties, candidates, election campaigns, and the activities of official observers from civil society organizations, as well as other individuals or legal entities, with the aim of influencing electoral processes or promoting the interests of a foreign state;

- organizing and funding sham observation with the aim of distorting an independent assessment of the electoral process and producing and publishing false and biased reports;

- Pressure on the media and journalists manifested through attempts to influence editorial policy and media independence — in particular through funding, threats, or the discrediting of journalists — which undermines the principle of freedom of speech and affects the objectivity and impartiality of media coverage of the organization and conduct of elections.

The latter two forms identified in the CEC's Concept may be covered by others. By definition, the financing of pseudo-monitoring is a form of financial interference, and the dissemination of false and biased reports is a form of information manipulation. Under this approach, one can identify the use of proxy organizations (political parties, civic groups, charities, religious organizations, etc.) that are under the influence of a foreign state, or the organization of protests or other destabilizing actions by foreign actors. As for pressure on the media and journalists, this also results in FIMI or the suppression of certain information. Examples include bribery and various forms of criminal offenses, such as threats or violence.

Funding is a cross-cutting indicator (sign) of foreign interference, as it is used both to directly funnel funds into the accounts of political parties or candidates and to bribe voters, journalists, bloggers, and organizations involved in protests and destabilization

campaigns, as well as to support proxy organizations. Therefore, it can be understood broadly — as the financing of any form of foreign interference, or narrowly, as the transfer of foreign funds into the accounts of political parties or candidates (political financing).[1]

Another pressing issue is the financing of political advertising and campaign activities by third parties. IDEA provides a definition of " non-contestant campaigners" — organizations that are neither political parties nor candidates yet spend resources and engage in electoral campaigns and invest into them. The need for regulating their activities was highlighted by the ODIHR OSCE and IFES (in the context of the vote-buying network of Ilan Shor in Moldova). In 2018, after the scandal with donations from Chinese businessmen to senator Sam Dstyari, Australia introduced the Foreign Influence Transparency Scheme, with the corresponding register. After the interference in the 2017 elections, France passed a law obliging social media platforms to disclose payers for promoted content, and the amounts alike (if the amount exceeded 100 euro, and the donation was paid within three months before the national elections). The 2024 Law on combatting foreign interference in France introduced a register of persons acting on behalf of or under the control of a foreign principal.

Ukraine has a requirement to fund electoral campaigns solely through the funds of parties and candidates but voters may also campaign within the framework of a general freedom of expression. Therefore, activities of the non-contestant campaigners is de facto unregulated. The lack of rules governing the funding of such activities and reporting on them creates ample room for potential information operations.

In sum, we can focus on 3 key forms of foreign interference that may be analyzed and detailed:

- Foreign Information Manipulation and Interference (FIMI);
- Foreign Financial Interference (FFI);
- cyber-interference.

In this report, we will focus on information interference (FIMI), while financial interference (FFI) will be considered in a broad sense, solely as an indicator of FIMI.

1 Financing of political parties and candidates aiming to promote foreign interests and narratives was presented as a threat by respondent 3.

# CHAPTER 2.

# DEBATABLE SIGNS OF FOREIGN INTERFERENCE AND FIMI

When examining foreign interference, a number of questions arise whose answers are neither simple nor straightforward, yet they are essential for developing effective countermeasures acceptable in a democratic society. These challenges can be articulated through the following interrelated questions:

- Are coercion or illegal acts signs of foreign interference?
- How do you differentiate interference from lawful foreign influence?
- How can one establish the "foreign" nature of foreign interference, and is it necessary to attribute it to a specific state?
- Is it possible to draw a line between FIMI and freedom of expression?

## 2.1. ARE COERCIVE OR ILLEGAL ACTIONS ALWAYS A SIGN OF FOREIGN INTERFERENCE?

**Coercion and foreign interference**. In a well-known case "Nicaragua v. United States of America" (1986), the International Court of Justice stated that the USA had violated the obligations imposed by customary international law, since they supported the contras (anticommunist rebels) and laying mines in Nicaragua harbors. The court stated (§ 205): "...in view of the generally accepted formulations, the principle *(ed. – non-intervention)* forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly

be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of a foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in a direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State…".

Clearly, the approaches used about 40 years ago may need to be revisited. We may uphold a statement by Hedvig Ördén and James Pamment that the "lack of shared norms on how to interpret the rules surrounding sovereignty in international law, when influence operations are concerned, is a problem that needs to be overcome." The strength of the International Court of Justice's legal position in the case of "Nicaragua v. the United States of America" lies in the fact that it recognized the possibility of foreign intervention in both direct (use of force, as in the case of Russian aggression) and indirect (subversive activities) forms. However, a shortcoming is the requirement that coercive methods be used for the intervention to be unlawful.

The formula that "coercion is the very essence of unlawful interference"clearly does not stand the test of time, given the evolution of technologies and forms of intervention, as it creates the main dogmatic obstacle to the classification of FIMI — any form of information manipulation leaves the recipient formally free to act as they choose. A voter reading some fake news is not exempt from the freedom of choice in legal terms. Similarly, the government, which is the target of an ongoing smear campaign, is not legally obligated to change its policies. At the same time, the influence of such information campaigns on the choice of political (including voting results), economic, social, and cultural system, and foreign policy making may be much larger than the use of coercive methods, such as threats or violence.

That is precisely why we believe that, given the scale of influence and the evolution of intervention methods today, coercion cannot be considered a mandatory characteristic of foreign interference, as this negates the practical possibility of countering it. Conversely, when it comes to FIMI, information manipulation is typically characterized by the absence of coercion, although it may be combined with it (for example, a candidate is intimidated by the threat of launching or continuing a smear campaign if he or she does not withdraw from the election).

**Illegal actions and foreign interference**. The issue of illegality as a hallmark of foreign interference is important both for identifying such interference and for understanding the tools the state can use to counter it (particularly investigations by law enforcement agencies and the imposition of legal liability). It pertains more to FIMI and less to FFI, since foreign donations in support of parties and candidates, according to IDEA, are prohibited in most countries. Thus, such activities are generally illegal and may even constitute a criminal offense. In Ukraine, the ban on foreign contributions is provided for in paragraph 7 of Part 1 of Article 15 of the Law "On Political Parties in Ukraine" and in Part 1 of Article 96, Part 1 of Article 152, and paragraph 1 of Part 3 of Article 215 of the Electoral Code — unlike FIMI.

In their reports on FIMI (from the first report of 2023 to the fourth report in 2026), the European External Action Service (EEAS) defines foreign information manipulation and interference as a "mostly non-illegal" pattern of behavior that threatens or has the potential to adversely impact values, procedures, and political processes. Such activities are manipulative and are carried out intentionally and in a coordinated manner by state or non-state actors, including their proxies, both within and outside their own territory.

One can debate whether it is correct to use specific terms in English ("illegal", "unlawful", "illegitimate" etc.) and Ukrainian ("незаконний", "неправомірний", "нелегітимний" etc.), but a key idea is that, in terms of its outward manifestations, FIMI may be closer to value judgements expressed in a lawful manner (for example, through public platforms). Even when it comes to false information that does not constitute defamation, its dissemination, according to Council of Europe standards, may also be deemed necessary in a democratic society. Moreover, a person who disseminates information that is wholly or partially false is not always aware of this. The speed and scale of information dissemination in today's world can require enormous effort and resources to verify its accuracy. Consequently, based on outward appearances, the same message may be disseminated either with the intent of foreign interference or without it.

The phrase "mostly non-illegal" is a key characteristic that has led to FIMI being described as a specific challenge that falls within the so-called "gray area" from the perspective of legal restrictions. This also means that the EU and other democratic states are developing a system to counter a phenomenon, part of which does not constitute a violation of either international or national law. Understanding this fact is a prerequisite for any proper legal discussion of FIMI, and it stems from the fine line between "information manipulation" and freedom of expression.

## 2.2. HOW TO DIFFERENTIATE FOREIGN INTERFERENCE FROM FOREIGN INFLUENCE?

Christopher Walker and Jessica Ludwig suggested a concept of "sharp power." According to them, the impact of authoritarian regimes is "sharp" in a sense that it "pierces, penetrates, or perforates the information environment in the targeted countries". The key point is that such influence "centers on manipulation and distraction." Authoritarian regimes "are not engaged in public diplomacy as democratic would understand it". Joseph Nye clarified that "without proper disclosure, the principle of voluntarism has been breached" and the "openness remains the best defense". In other words, identifying who is disseminating the information, and in whose interests, is a practical aspect of distinguishing between foreign interference and influence.

A similar approach was applied in a study commissioned by the EP (special committee ING2). It highlights that foreign influence is different from foreign interference, and covers any activity of foreign states with the purpose or consequence to influence the policies and democratic processes in the EU. Foreign influence is a common and legitimate aspect of international relations, and governments regularly seek to influence one another's affairs and decision-making in order to better advance their own interests. In this way, they make a positive contribution to open democratic debate. Foreign influence encompasses diplomacy, lobbying, and public communications. According to the authors of the study, the key difference between foreign influence and foreign interference is that the former is open and honest, while the latter is covert and/or deceptive. At the same time, the recipient of foreign influence must understand the source and nature of that influence.

The US paradigm offers a somewhat different approach to understanding foreign interference and influence. In particular, Lawrence Norden and Kate Lurie, after analyzing a number of US federal laws, say that foreign interference in elections is generally illegal, but at the same time, the legal status of activities related to foreign influence is less clear-cut. Influence campaigns can take various forms of expression, including social media posts, and are often aimed at changing the views of the target audience. For example, during the 2024 election cycle, the U.S. Intelligence Community noted that "foreign actors … disseminate influence narratives aimed at undermining democratic institutions, fueling social divisions, and/or shifting public opinion." It was also noted that foreign actors use "Americans who, knowingly or unknowingly, disseminate and promote narratives that serve the interests of foreign actors and lend credibility to these narratives."

The US Intelligence Community emphasized that, under the First Amendment to the Constitution, the government may not restrict the freedom of speech of U.S. citizens or their access to information, regardless of its source. At the same time, the government may disclose information about the foreign origin of such materials if relevant intelligence is available, and in certain cases may hold foreign entities accountable for violations of U.S. law, including concealing their role in spreading false election narratives or laundering funds to circumvent U.S. sanctions.

In other words, Lawrence Norden and Kate Lurie refer to U.S. federal laws to define foreign interference rather than criminal offenses, such as cyber or physical operations, political assassinations, or military or security interventions. Foreign influence, on the other hand, is viewed as foreign information operations, which are very difficult to distinguish from constitutionally protected political speech. Under this approach, FIMI falls under the concept of foreign influence. This approach also has its merits, but it leads to terminological confusion (FIMI should be defined as "Foreign Information Manipulation and Influence," not "Interference"). In addition, it is necessary to introduce a separate category for different forms of influence (conventionally "integrity" and "non-integrity"). In light of this, as well as Ukraine's need as a candidate country to adapt to EU standards, we propose adopting the European approach.

During the in-depth interviews conducted by OPORA as part of this study, some respondents expressed the view that foreign influence can occur legally through mechanisms of international cooperation, participation in international organizations, and the establishment or promotion of democratic standards and best practices,[2] in the form of open discussions and transparent economic relations,[3] if it is aimed at protecting human rights and the rule of law,[4] takes place within an official institutional framework (diplomatic cooperation, international treaties, intergovernmental negotiations), is transparent, and is attributable.[5] In contrast, foreign interference is focused on advancing the personal interests of the entity or state carrying it out,[6]

2 This view of a possible lawful foreign influence was emphasized by respondents 1 and 3.

3 Mentioned by respondent 4.

4 Mentioned by respondent 5.

5 Mentioned by respondent 8.

6 Mentioned by respondent 3.

is anonymous and covert, employs coordinated actions and illegal funding, and aims to manipulate or divide society.[7]

Therefore, based on the EP study, it can be concluded that foreign interference differs from legitimate foreign influence in that the activities carried out by a foreign state actor or on its behalf are coercive, covert, deceptive, or corrupt and run counter to the sovereignty, values, and interests of the EU. However, these characteristics are alternative — it is not necessary for all of them to be present simultaneously for an act to be classified as interference. To enable foreign actors to conduct lawful activities, countries provide for special mechanisms, such as the Foreign Influence Registration Scheme in the UK, or the Transparency Register in the EU.

## 2.3. HOW TO DETERMINE THE FOREIGN NATURE OF FOREIGN INTERFERENCE, AND WHETHER IT IS NECESSARY TO ATTRIBUTE IT TO A SPECIFIC STATE?

Attribution is the process of establishing the involvement of a state or its representatives in foreign interference. In essence, it is the process of identifying such interference as foreign. Special tools are provided for legitimate foreign influence, such as labeling the origin and sources of funding or creating special registries. At the same time, attributing foreign interference is significantly more complex because, as noted above, such activities are often covert and deceptive.[8]

This is confirmed by data from EEAS, which, in its fourth report, identified and analyzed 540 FIMI incidents between January 1 and December 31, 2025, of which 29% were linked to Russia and 6% to China. In rare cases, Russian and Chinese FIMI infrastructure operated in unison — mostly by opportunistically amplifying each other's content. However, 65% of all recorded incidents remain unattributed, although they show signs of a connection to Russian or Chinese FIMI infrastructure. The identified incidents involved 10,500 unique channels — ranging from fabricated news websites to social

7 Mentioned by respondent 8.

8 The complexity of attribution was underlined by respondent 4, claiming that even if this is possible, it is often only done post-factum.

media accounts and blogs — indicating cross-platform activity and coordination among numerous resources within the FIMI ecosystem. As part of the report, a sample of approximately 3,000 of the most frequently cited resources was mapped and characterized. Only 9.5% of these channels are directly linked to a state actor (official sources or state-controlled sources). The vast majority (90.5%) are covert resources associated with a threat actor or acting in concert with it, with the latter category remaining unattributed. In other words, the largest portion of FIMI's infrastructure is covert or inauthentic, specifically networks of Coordinated Inauthentic Behavior (CIB).

It must be emphasized that this is, to a certain extent, a technical rather than a legal attribution that can be used to apply sanctions or establish legal liability in court. Legal (especially judicial) standards of proof are even stricter, so the percentage of attributed instances of interference may be lower. Therefore, identifying the connections behind FIMI's hidden sources is essential to minimize their potential impact and counteract them.

The EEAS rightly points out that resources used in FIMI are, by their very nature, deceptive, as they conceal the operators and sources of funding. In this regard, identifying and investigating the behavior and infrastructure behind unattributed instances of FIMI is key to uncovering the nature and sources of the threat in question. Even when interference and the manipulative nature of the information have been established, proving a link to a specific foreign state remains a separate challenge. This raises the question: Is it necessary to prove which specific state is carrying out the interference in order to characterize it as foreign in nature?

The fact that the EEAS refers to the non-attributable FIMI facts indicates that they can be identified without establishing a precise or even affiliated source in the form of a specific state.

If we look at the regulations in the United Kingdom, Art. 31 of the National Security Act provides a definition of "foreign power condition" as an element of offence. It is considered to have been carried out with respect to a person's act if:

- the act in question, or the systematic actions of which it forms a part, is carried out "in the interests of or on behalf of a foreign state," and
- a person "knows" or, in light of other circumstances known to them, "should reasonably know" that this is the case.

A specific act or a series of acts of which it is a part shall, in particular, be deemed to have been committed in the interests of or on behalf of a foreign state if it:

- "instigated" (or, to put it in Ukrainian legal terms, it is literally "incited") by a foreign state,
- is carried out "at the direction or under the control" of a foreign state,
- is carried out with "financial or other assistance" provided by a foreign state for this purpose, or
- is carried out "in cooperation with a foreign state or with its consent".

In this context, a "direct or indirect connection" is taken into account, and the condition regarding a foreign state is also considered to be met with respect to a person's act if the person "intends for the act in question to benefit" a foreign state; in such a case, it is not necessary to identify a specific foreign state. In other words, this essentially refers to activities carried out in the interests of foreign entities without identifying a specific beneficiary abroad.

A similar approach is used in Australia, where, under Subsection B of Section 92.2 of the Criminal Code Act, the interference subject may be any person who:

- acts on behalf of a foreign entity or a person acting on its behalf; or in cooperation with a foreign entity or a person acting on its behalf;
- whose conduct is directed, financed, or controlled by a foreign entity or a person acting on its behalf.

At the same time, a person's activity does not necessarily have to relate to a specific foreign entity or may even apply to several.

In their study "What is So Foreign in Foreign Influence Operations?", Hedvig Ördén and James Pamment use three distinct approaches to determine what constitutes a "foreign" entity: foreign states, foreign citizens, and foreign interests. The authors conclude that the lens of "foreignness" can be useful only in a narrow range of cases, specifically when there is compelling evidence of interstate conflict (in the case of Ukraine, Russian aggression has been clearly identified and recognized at the international and national levels), hybrid and irregular warfare, or in the context of defending democratic institutions, such as elections. At the same time, when it comes to safeguarding elections, the authors see the key role of governments as lying in legislative changes regarding election financing and online political advertising. However, when influence

operations are viewed as a broader threat to political discourse, they do not consider foreign origin a useful category for determining legitimacy or illegitimacy of such campaigns. In these cases, rather than focusing on the identity (domestic or foreign) of the malicious actors themselves, it would be more appropriate to identify illegitimacy through specific manipulative communication methods.

In essence, Hedvig Ördén and James Pamment do not deny that a foreign nature is a characteristic of interference, although they view it more as a spectrum or scale rather than a binary distinction. They consider the application of this criterion more appropriate when, first, systematic and coordinated operations are involved, and second, when these are combined with subversive activities and other methods (espionage, coercion, etc.) that can be considered a matter of national security. However, when it comes to individual instances of information manipulation or even individual messages, it will be difficult to assert that they are "foreign" without compelling evidence. Even if this were done, a logical question arises: what changes in terms of the consequences of such a message once it has been identified as manipulative foreign or manipulative domestic? Moreover, a hostile state's objective may be to blur these boundaries by attributing such interests to domestic groups.

Since the disruptive effect of a single message or a group of messages will be the same in and of itself, one can agree with Hedvig Ördén and James Pamment that it is more promising to study the methods used to spread manipulative information, as countermeasures against such information can be regulated by legislation or platform rules. However, in our view, identifying coordinated influence operations can begin with an analysis of individual manipulative messages. Moreover, when certain indicators (foreign funding, identified protection of a foreign state's interests, the use of intermediaries, or widespread support for messages by foreign actors, etc.) point to the foreign nature of the interference, this will obviously require different means of response and counteraction than the dissemination of manipulative information without a foreign element.

Therefore, although the attribution of a specific state carrying out the interference is not a mandatory characteristic of FIMI (as confirmed by regulations in the United Kingdom and Australia), and while methods of information manipulation should be countered regardless of whether or not they involve a foreign element, analyzing indicators that suggest its presence (foreign actor, control, interest, funding, etc.) is essential for identifying coordinated and systematic campaigns.

## 2.4. IS IT POSSIBLE TO DRAW A LINE BETWEEN FIMI AND FREEDOM OF EXPRESSION?

Distinguishing between information manipulation and freedom of expression (including the right to freely form and express one's views) is perhaps the most difficult practical challenge.

Irene Khan, UN Special Rapporteur, in her report "Disinformation and freedom of opinion and expression," noted that there is no agreed-upon legal definition of disinformation, and that states' responses to it can take various forms: restrictions on internet access, censorship, penalties, restrictions on dissemination, and regulation of social media. At the same time, states — justifying these measures as necessary to counter disinformation — may themselves resort to restricting freedom of expression. Part of the problem also lies in the inability to draw a clear line between fact and fiction, as well as between the absence and presence of intent to cause harm. Moreover, it is a universally recognized democratic principle that freedom of expression extends to all information and ideas, including those that may shock, offend, or disturb (see the ECHR ruling in the case "Handyside v. the United Kingdom"), and regardless of whether the content is true or false (see the ECHR ruling in the case "Salov v. Ukraine"). Under international law, people may express unfounded opinions and statements or engage in parody or satire.

Hedvig Ördén and James Pamment also rightly point out, which is absolutely unacceptable to label citizens as agents of foreign interference merely for expressing even marginal or manipulative views, without evidence of a coordinated offence. In any case, such a statement would likely be protected by freedom of speech laws. In this sense, the analogy with information warfare does not allow us to claim that such citizens are turned into foot soldiers, except in cases of truly coercive intervention.

The ECHR has established a broad body of legal principles regarding freedom of expression (Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms). The ECHR applies a three-part test and requires that any restriction on the exercise of this right must:

- be established by law;
- have a legitimate goal;
- be necessary in democratic society.[9]

9 The need to apply a three-part test of the ECHR was emphasized by respondent 8.

Several issues arise in the context of FIMI. First, the legal framework in these countries regarding foreign interference is not yet sufficiently developed and has only recently begun to take shape. In particular, the National Security Act was enacted in the United Kingdom in 2023; the Act Respecting Countering Foreign Interference in Canada in 2024, amendments to the Criminal Code and related changes in Australia in 2018, Moldova amended its regulations only in 2022 and 2025, while the EU continues to study and develop the necessary infrastructure. Second, combating "information manipulation" or "disinformation" is not included in the list of legitimate grounds for restricting freedom of expression under Article 10(2) of the Convention. Therefore, it is necessary to demonstrate the existence of a threat to other values, in particular national security, or the need to protect the reputation or rights of others.

Some important conclusions were reached in the 2025 ruling in the case of "Bradshaw et al. v. the United Kingdom," in which three British Members of Parliament accused their own government of violating the right to free elections due to the lack of an effective system to protect against foreign interference. The essence of their complaint to the ECHR was that the government, despite having reliable intelligence reports about Russia's attempts to interfere in British democratic processes (including the 2014 referendums on Scottish independence and EU (Brexit) in 2016 and the 2019 parliamentary elections), failed to conduct a proper investigation into these facts, thereby jeopardizing the fair and free nature of the expression of the will of the people.

Although the ECHR did not find a violation of the right to free elections, the application was declared admissible, and a number of legal positions were articulated:

1. The Existence and Scope of Positive Obligations. Although countering foreign interference does not constitute a separate and autonomous obligation for states, a flagrant failure to act may violate the very essence of the right to enjoy the results of elections held "under conditions that ensure the free expression of the will of the people" (para. 138).

2. Distinction from Criminal Prosecution. Positive obligations to counter foreign interference were distinguished from investigations under Articles 2–4 of the Convention due to their different nature (para. 137).

3. Broad discretion in choosing countermeasures. Although states must not remain passive in the face of evidence of interference, they must be granted a wide margin of appreciation in choosing the measures to be taken to counter it (paras. 159, 162).

4. Recognizing the Complexity of the Problem. The court upheld its previous ruling in the case "Partija "Jaunie Demokrāti" and Partija "Mūsu Zeme" v. Latvia" (regarding political parties' exceeding campaign spending limits) that the outcome of a vote is influenced not only by campaigning but also by other factors — political, economic, social, and psychological. As a result, it is very difficult, if not impossible, to establish an exact and real causal link between campaigning and the number of votes received *(as is the case with foreign interference and its impact on the outcome – author's note).* Therefore, the court concluded that, in fact, the only conclusion on which there is a clear consensus is that this is a complex global problem that cannot be solved without the cooperation of international partners and social media companies (paras. 158, 160).

5. Reservations Regarding State Abuse. There is a very fine line between mitigating the dangers of disinformation and outright censorship; therefore, international organizations warn against the risk of knee-jerk reactions. As an example, they cite cases involving the impermissibility of designating organizations, media outlets, and individuals as "foreign agents" in Russia. Therefore, any countermeasures must be balanced against the right to freedom of expression under Article 10 of the Convention (paras. 160, 161).

Despite the importance of the case "Bradshaw and Others v. the United Kingdom," it merely opens a judicial debate on measures to counter foreign interference and their relationship to freedom of expression. It is a sort of "trial run," as evidenced by frequent references to the positions of international organizations and the emphasis placed on the complexity of this issue. Ultimately, the ECHR noted that states have positive obligations to counter foreign interference, but these are not as stringent as those under Articles 2–4 of the Convention, given the broad discretion in choosing measures, the difficulty of proving causal links, and the need to respect the requirements of freedom of expression. From this, it can be concluded that, in order to exclude FIMI from the protection afforded by freedom of expression regulations, clear criteria and a solid justification must be established. Drawing an analogy with the presumption of innocence — until doubts regarding whether the disseminated information constitutes manipulation or foreign interference are refuted, such conduct will be considered lawful (freedom of expression) rather than prohibited (foreign interference).

# SECTION 3.

# CHARACTERISTICS AND IDENTIFICATION OF FIMI

## 3.1. WHAT ARE THE CHARACTERISTICS OF FIMI, AND HOW DOES IT RELATE TO DISINFORMATION?

There are initiatives aimed at countering disinformation (e.g., the European Digital Media Observatory) or a Ukrainian Center for Countering Disinformation) disseminated primarily on behalf of or in the interests of foreign states. Therefore, FIMI is often associated with disinformation, but the two concepts are not the same.

The EC interprets disinformation as information that has been verified as false or misleading, created, presented, and disseminated with the aim of obtaining economic gain or intentionally deceiving the public, which may cause harm to society (to democratic processes, public health, security, or the environment). It is specifically emphasized that reporting errors, satire, and parody, as well as clearly identified partisan news and commentary, do not constitute disinformation.

In a report of the Council of Europe, researchers distinguish between three forms of information based on the criteria of truthfulness and harm:

- mis-information — false information disseminated without intent to cause harm *(error or inattentiveness — author's note.)*;
- dis-information — false information deliberately disseminated with the intent to cause harm;
- mal-information — true/authentic information deliberately disclosed with the intent to cause harm *(leaks of private data, leaks of compromising material, etc, — author's note)*.

Without getting into a broad discussion, we can say that disinformation has at least two defining characteristics: manipulative (misleading or false) content and intent (to cause harm). However, as early as its first report, EEAS introduced the concept of FIMI and rightly pointed out that it overlaps with the concept of disinformation, but is at the same time both narrower and broader than it:

- narrower — since it concerns only the manipulation of information by foreign actors and does not cover domestic sources;
- broader — since it does not require that the information disseminated by threat actors be proven to be false or misleading.

The defining factor for a phenomenon to be considered FIMI is not the false or misleading content of the information, but rather deceptive or manipulative behavior. An illustrative and intuitively understandable example of FIMI is coordinated inauthentic behavior (CIB) on social media platforms, in which actors seek to create the impression that a particular narrative has broader support than it actually does, by spreading and amplifying it through fake and deceptive social media accounts. The information disseminated by such networks does not necessarily have to be proven false or misleading for the activity in question to constitute a FIMI incident. This is precisely what makes the concept of FIMI broader than the classic definition of disinformation.

International Institute for Democracy and Election Assistance (IDEA) defines FIMI as coordinated actions by foreign actors aimed at influencing or destabilizing electoral processes by manipulating the information environment. IDEA identifies the following characteristics of FIMI:

- coordinated actions by foreign entities or their proxies;
- the use of various types of content: false, misleading, or emotionally charged;
- the goal is to weaken institutions, influence elections, or shape public discourse;
- these activities often span multiple platforms and communication channels;
- an effort to undermine trust and exacerbate social or political divisions.

The emphasis placed by the EEAS and IDEA on behavior and coordination is important and necessary for identifying FIMI. However, before proceeding to analyze the identification process, it is important to summarize the characteristics of FIMI. At the same time, the fact that certain characteristics are not mandatory does not mean that they cannot be used to identify FIMI. For example, we argued above that information manipulation can occur through lawful behavior. At the same time, the illegality of the behavior can serve as an additional, albeit optional, identifier. In particular,

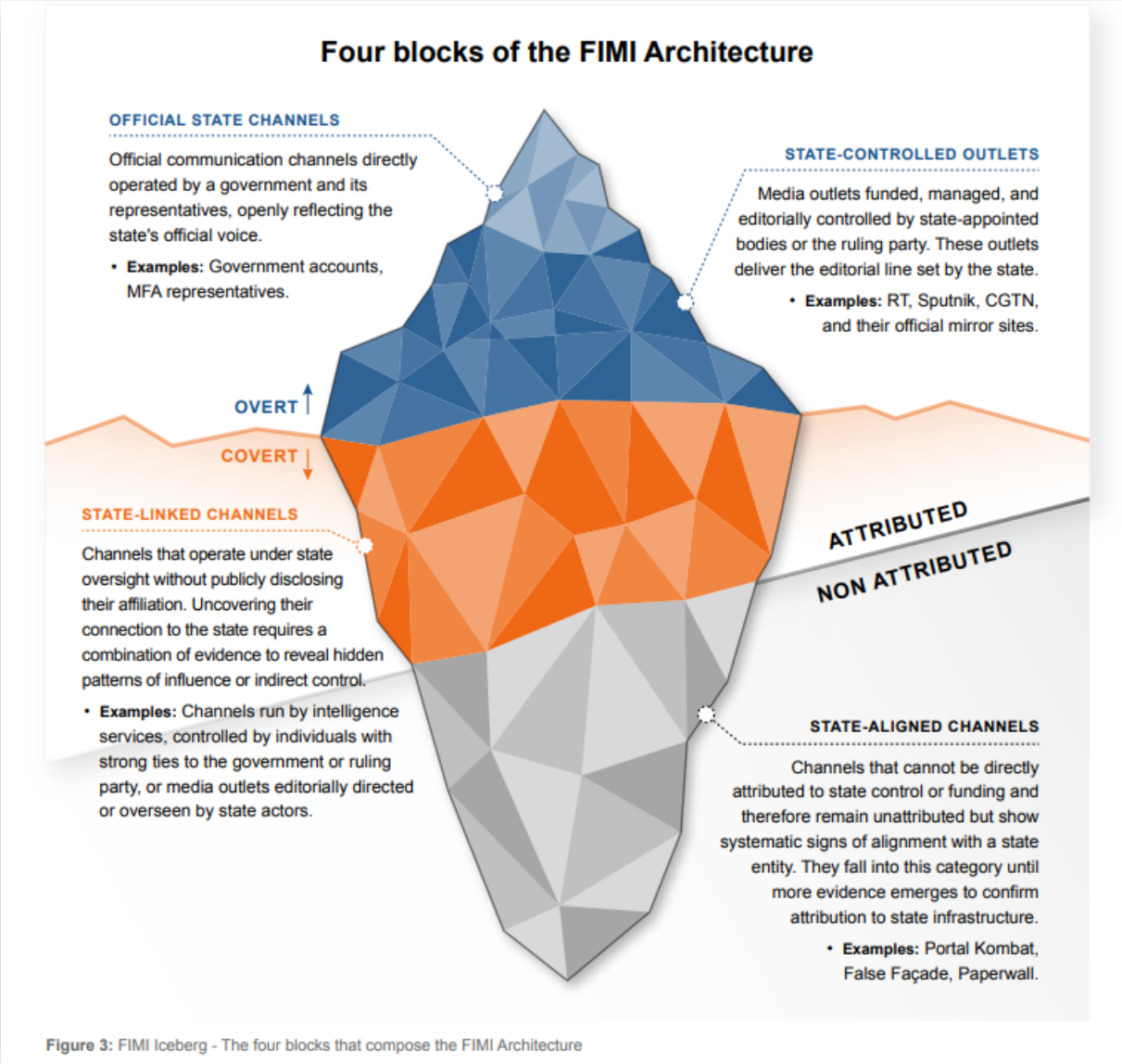
the dissemination of information containing elements of defamation or incitement to hostility, or the illegal financing of such information, may merely confirm the coordinated nature, intent, or purpose (e.g., election interference) of such behavior.

As for the mandatory characteristics of FIMI, the following seem to us to be reasonable compromises:

1. Manipulative (deceptive or covert) behavior. Deception or covertness may relate to the authenticity of the behavior, its purpose or intentions, or the source or funding of the information. As noted above, this includes, but is not limited to, information that is deceptive in content. The dissemination of false information without deceptive behavior or hidden motives may be protected by freedom of expression. At the same time, inauthentic behavior such as "padding" view counts or artificially promoting even truthful information on social media — particularly when it includes specific narratives or evaluative judgments — constitutes manipulation based on behavior rather than content.

2. Coordinated actions (actions aimed at intervention, united by a specific intent and purpose). Coordinated actions were mentioned in the definitions by EEAS and IDEA, and they allow distinguishing between individual expressions of opinion (even if the information disseminated is manipulative in nature) and interference campaigns. In addition to indicating premeditated behavior and the existence of a specific structure, it is difficult to imagine coordinated activity without the intent to harm the national interests of the target state and without a specific goal (for example, to undermine confidence in the election results or to reduce support for a particular candidate).

3. Foreign involvement (a connection to a foreign state or its proxy). By definition, interference can be considered foreign only if someone acts on behalf of, under the control of, or in the interests of a foreign state. The EEAS uses a classification of channels depicting them in the form of an iceberg *(see image below)*, where the visible part consists of official and state-controlled channels, and the lower (hidden) part consists of channels associated with or loyal to a particular state. Although Hedvig Ördén and James Pamment call into question the value of attributing information manipulation; nevertheless, without such attribution, the interference can hardly be classified as foreign. However, as noted above with reference to British National Security Act and the Australian Criminal Code Act, and also to cases of incidents provided by the EEAS, attributing an intervention to a foreign source does not necessarily require identifying a specific state or foreign entity as the beneficiary.




FIMI Iceberg. Source: EEAS

Among the characteristics of FIMI that are not mandatory but may help identify it, we highlight the following:

1. Coercion or other forms of violence. According to the ruling of the International Court of Justice in the case "Nicaragua v. The United States of America," the presence of coercion remains a key indicator of foreign interference. As noted above, FIMI does not typically involve the use of violence, but manipulative campaigns may be combined with violence or threats of violence (for example, to discredit and remove a specific candidate or party from the electoral race).

2. Illegal activities or the commission of offenses. If the collection, processing, or dissemination of information violates legal regulations (which do not necessarily constitute an offense), this alone is sufficient grounds for action. Similarly, offenses such as collaboration with the enemy, incitement to hostility, and calls to violate sovereignty may be combined with information manipulation.

3. Violations of platform policies or media standards. Legislative regulation is not the only basis for the dissemination of information — platform policies, codes of ethics, media standards, and the like may carry even greater weight due to the transnational nature of large companies, as well as their role in primary content moderation. Accordingly, failure to comply with these rules or abuse of them may indirectly reveal interference campaigns.

4. Misleading or false content. As noted above, freedom of expression applies to any information and ideas, including those that may shock, offend, or disturb, and regardless of whether their content is true or false. However, FIMI campaigns are often, though not always, accompanied by disinformation or manipulative information. In any case, misleading content can be an important indicator for verifying whether other signs of disinformation are present.

5. Funding or the provision of other benefits. Since FIMI is inevitably linked to the interests of foreign actors and requires resources to carry out, the funding of such information campaigns or the provision of other benefits to entities that create or disseminate them is an important indicator. In fact, proving this indicator can be of great practical value, since, for example, a FIMI campaign will be much easier to identify if it can be proven that the dissemination of information was paid for with funds of foreign origin than based on the nature of the behavior (moreover, this can confirm the "foreign" element).

6. Advocacy for the interests of a specific state. This criterion cannot be applied on its own, as it would encompass legitimate foreign influence, such as diplomacy, public lobbying, or international relations. Furthermore, FIMI is usually accompanied by an attempt to conceal the true beneficiary of the interference. However, identifying a specific state with an interest (especially a hostile one) in conducting information campaigns can help uncover the FIMI chain. The official recognition of Russia as an aggressor state (at the international and national levels) as a result of its aggression against Ukraine makes it possible to track FIMI networks based on Russian narratives and information campaign strategies and to counter them specifically. The fact

that a particular message is favorable to Russia does not in itself make it an instance of FIMI, but it does provide grounds for initial identification and a search for other indicators.

It should be added that the set of FIMI indicators required for identification depends on the purpose of the identification. For technical incident analysis (such as that conducted by the EEAS) or research, the mandatory indicators listed above may be sufficient. However, the application of legal response mechanisms may require additional indicators. This logic can be presented as "levels" of response to information manipulation campaigns:

1. For legal liability mechanisms to apply, the elements of an offense must be present (when information interference is combined with coercion, violence, or corruption, or when it constitutes a crime in and of itself, such as collaboration or espionage).

2. In order to apply sanctions or similar legal mechanisms (such as fines imposed on media outlets by regulatory agencies, vetting measures, or exclusion from elections), it is necessary to establish a threat to national security or a failure to comply with legal requirements.

3. In case of retaliation, in order to take retaliatory action (in response to unfriendly acts), it is necessary to identify the specific state on whose behalf the interference is being carried out.

4. In order for platforms or media outlets to ban content, it must be determined that the content violates their policies, codes of ethics, or standards.

5. For soft-power countermeasures (fact-checking, debunking misinformation, revealing facts such as funding sources, etc.), individual indicators (such as deceptive behavior or foreign funding) are sufficient, since such measures can be used in response not only to information campaigns but also to individual messages.

6. For proactive (preventive) soft power measures (raising awareness, promoting media literacy, providing information and education, etc.), it is generally not necessary to identify an instance of interference, since these measures are designed to prevent threats.

## FORMS OF RESPONSE TO FIMI




Grounds for applying different forms of responding to FIMI incidents.

## 3.2. HOW TO IDENTIFY FIMI?

In their first FIMI report, EEAS mentions the ABCDE methodology (described by James Pamment) that includes such key components as the assessment of actors (A — Actor), behaviors (B — Behavior), content (C — Content), degree (D — Degree), and effect (E — Effect). For illustration, Pamment provides the following questionnaire (yet underlines that it may be adapted to specific needs):

→ Which actors are involved?

- Is the individual acting in a private capacity?
- Is the actor affiliated with a private or nongovernmental organization?
- To what extent is the distribution platform independent?
- Is the individual acting on behalf of a political entity?
- Is the actor an agent or representative of a foreign state?

→ What is the actor's behavior like?

- Does the actor conceal their identity or activities?
- Is the actor acting on behalf of another person?
- Are illegitimate communication methods being used?
- Is there evidence of coordination?
- Does the behavior indicate malicious intent?

→ What kind of content is being created and disseminated?

- Can it be verified that the content is false or misleading?
- Does the content align with known disinformation narratives?
- What languages are used to spread disinformation or other online content?
- Is the content manipulative or fabricated?
- Is the content a reasonable form of self-expression protected by fundamental freedoms?
- Is the content harmful?

→ What is the overall impact of a particular case, and whom does it affect? (degree of impact)

- Who is the primary target audience?
- Have you determined which channels or platforms are used to distribute content and how they interact?
- Does the content go viral on social media in a way that could indicate inauthentic growth in online engagement?
- Is the content tailored or micro-targeted, and if so, for which audiences?
- Does the scale indicate a single operation or a prolonged campaign?

- What is the overall impact of a particular case, and whom does it affect? (effect)
    - Is the online content based on a specific issue? Does it contain, among other things, false information, polarization, or trolling?
    - Is the content targeted at a specific audience? Does it contain, among other things, false rumors, cybersecurity breaches, fabrications, and/or media leaks?
    - Does the content undermine fundamental freedoms? For example, does it aim to suppress freedom of expression or political debate?
    - Does the content pose a threat to people's health, physical well-being, or the medical safety of the general public?
    - Does the content pose a threat to the physical health or public safety of individuals?
    - Is the content intended to reduce voter participation in elections? Does it attempt to undermine election results?
    - Does this content pose a threat to the territorial integrity or national security of a sovereign state?

In fact, the ABCDE mnemonics has been evolving into different branches. Camille François described it as the ABC frame (Actors, Behaviors, Content), while Alexandre Alaphilippe added a "D". However, he did not imply the Degree but rather the Distribution — with the focus on technical distribution infrastructure.

This report does not aim to delve into discussions regarding the appropriateness (since "Degree" and "Effect" both describe impact, albeit with different emphases) or additions (such as "Distribution") to this methodology. Finally, as the EEAS emphasizes, analytical groups representing a broad range of stakeholders should be able to contribute to its improvement, and any attempt to draw up an exhaustive list of steps necessary to identify FIMI seems utopian. However, the approach must be versatile enough to allow for the adaptation of processes and the development of tools based on it.

In our opinion, FIMI can also be identified using a framework more typical of legal analysis — subject, object, method, content, and impact.

An analysis of a **subject** (or rather, subjects, since we are referring to different individuals) during FIMI identification may pertain to those who:

- disseminate information;
- organized (also funded) informational operation;
- designed or facilitated an information operation;
- has an interest in or exercises control over (in case of FIMI, it is, obviously, foreign).

An analysis of an **object** may include the following:

- the sphere of social relations targeted by the operation (e.g., elections);
- specific social relations targeted by the operation (e.g., campaign activities);
- the objective (the goal sought during the information operation, such as discrediting a specific candidate or undermining confidence in the election results);
- the target audience (for example, voters with specific views, ideologies, from a specific region, or of a specific social status, etc.)

**The method** essentially encompasses the tools used:

- where the information was disseminated (for example, a specific platform or media outlet);
- the status of a media outlet, platform, community, or page;
- whether digital content creation tools (including artificial intelligence) were used;
- whether tools involving inauthentic behavior or microtargeting were used.

**Content** analysis focuses on the information operation itself:

- the factual data of the information message (in particular, its reliability or unreliability)
- the evaluative judgments in the information message (in particular, narratives);
- the inferences to which the information message or operation leads;
- the cause-and-effect relationships that the message attempts to demonstrate between facts, evaluative judgments, and inferences.

**Effect** refers to the consequences that the information operation was aimed at and led to:

- the overall goal the actor sought to achieve (discrediting, polarizing, intimidating, etc.);
- specific tasks (steps) necessary to achieve the goal;
- quantitative indicators of impact (views, reposts, reactions, etc.);
- qualitative indicators of influence (sphere of social relations, audience reach, sensitivity of the issue, etc.).[10]

This is an indicative list of what may be subject to analysis for identifying a FIMI operation, and it is not exhaustive. Regardless of the approach, it is crucial to establish all possible indicators (mandatory and optional), as this will determine the legal and informational measures that can be taken to counteract the operation.

A unified taxonomy is necessary for effective cooperation between states and all actors countering FIMI. The EEAS proposes using the DISARM framework developed by the DISARM Foundation to analyze cyberattacks, but which is fully applicable to characterizing FIMI operations and describing the relevant tactics, techniques, and procedures

DISARM Red Framework is used to describe the behavior and tools of malicious actors at various stages of an information campaign, including the following:

- planning and preparation (studying the target audience, identifying polarizing topics, creating front media outlets and channels, etc.);
- infrastructure development (registering bot farms, generating deepfakes, purchasing verified accounts, etc.);
- narrative generation (fabricating documents, manipulating facts, spreading emotionally charged messages, etc.);
- dissemination and amplification of influence (coordinated reposts, inflating view counts, covertly engaging influencers, etc.).

10 Although assessing the consequences of information operations is complex and somewhat arbitrary, it will contribute to a better understanding of the mechanisms for countering them.

DISARM Blue Framework outlines measures to counter and neutralize threats — also depending on the stage of the information campaign:

- preventive measures (for example, warning the public about a planned disinformation campaign before it gains traction);
- technical measures (e.g., flagging or blocking coordinated bot networks on platforms);
- rebuttals (e.g., fact-checking and providing verified context);
- strategic communications (e.g., building audience resilience to specific manipulative patterns).

In addition, to describe FIMI incidents, the EEAS proposes (although it questioned the advisability of this in its first report) using the STIX (Structured Threat Information Expression) data format — which is used to encode and exchange intelligence on cyber threats — with a special extension.

The use of a unified taxonomy and data format is important for networked cooperation among government agencies, governmental, and nongovernmental organizations in different countries, as FIMI is transnational. These should be integrated into operational guidelines and training programs.

# CHAPTER 4.

# FIMI METHODS AND EXAMPLES

The DISARM Framework provides a broad description of influence operation methods that are also applicable to FIMI. Here, we will present examples of FIMI with descriptions of methods based on the DISARM Framework, though they do not necessarily replicate it. To this end, we will first examine FIMI methods (a non-exhaustive list), including the manipulation of actors and assets, content, or advocacy, and then discuss the targets and examples of potential information campaigns in the electoral sphere.

## 4.1. HOW CAN ACTORS AND ASSETS BE MANIPULATED?

**1. Creating fake accounts (sockpuppets).** Creating accounts with fictitious or borrowed identities that pose as citizens of the target country, including journalists, activists, experts, party members, or candidates.

An example of such an operation is "Doppelganger," specifically its activities during the 2025 presidential election in Poland. For instance, fake Polish accounts on X were created en masse in February 2025 or purchased from real users. From March 4 to April 4, the campaign generated 1.5 million views and 256,549 inauthentic shares. Key narratives included criticism of the EU (going as far as calling for Poland's exit from the European Union) and the government of Donald Tusk, as well as calls to reduce support for Ukraine and block its EU membership.




Example of a post as part of the Doppelganger operation Source: Alliance4Europe

**2. Purchasing real accounts**. Acquiring or hacking real accounts belonging to citizens of the target country to bypass the platforms' authenticity checks and capitalize on the audience's existing trust

For example, according to a report by The New York Times, during the presidential election in Ukraine, instead of creating fake Facebook pages, the Russians tried to find real Ukrainians who would sell them their own accounts, and use them to promote political advertisements or spread fake stories. The goal was to discredit candidates opposed by Moscow and to criticize Ukraine's democratic development in the post-revolutionary period.

**3. Generating or imitating individuals or channels.** Artificial intelligence allows for the creation of both entirely fictional accounts and pages that pose as accounts of real people. This is done to discredit politicians, journalists, opinion leaders, experts, or other figures.

For example, attackers hacked into the broadcast of the "Ukraine 24" TV channel and inserted a message about "surrender," while simultaneously spreading a deepfake video in which "Zelenskyy calls for laying down arms." The video was also posted on hacked websites and on social media.

Another, larger-scale and more coordinated example is the Russian influence campaign "Operation 'Overload,'" also known as "Matryoshka" or Storm-1679, which aimed to shift public opinion regarding the war in Ukraine and foment division in democratic countries. As part of the campaign, accounts were created that posed as media outlets, academics, and law enforcement agencies and published videos resembling news reports. The use of AI to clone voices, fabricate headlines, and manipulate images was also documented.

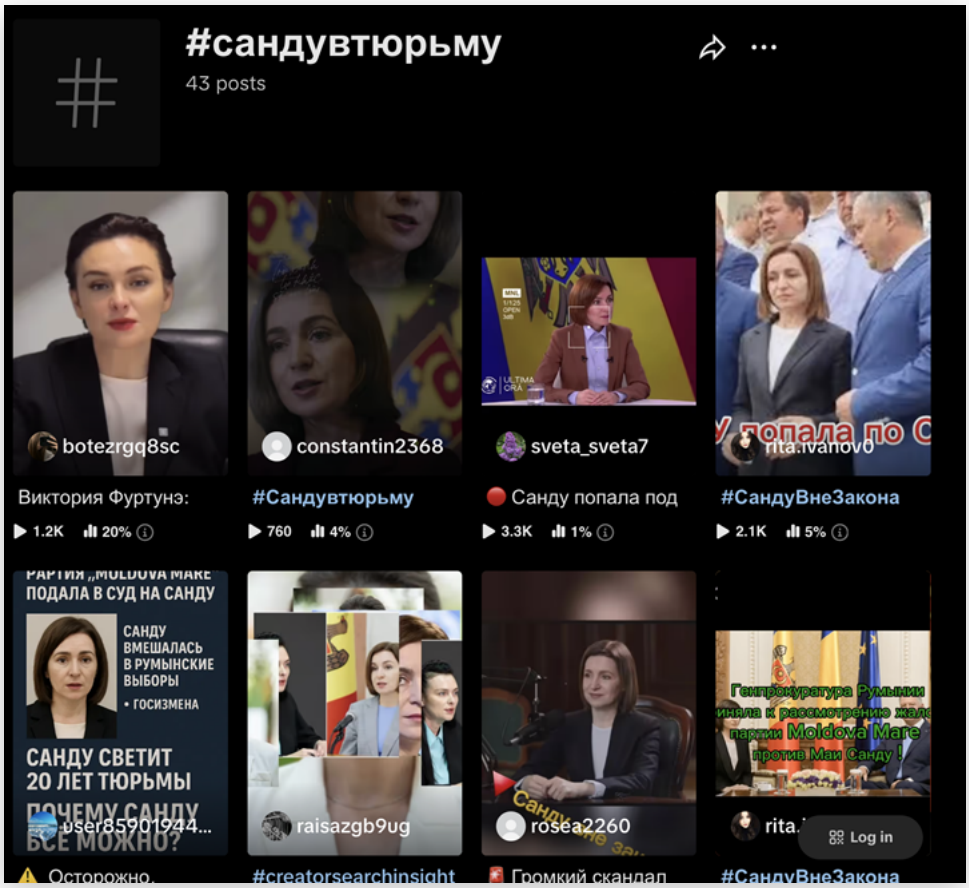



Source: Institute for Strategic Dialogue

**4. Paid influence networks ("digital army").** To carry out large-scale information interference campaigns, entire networks are sometimes formed with hired staff, technical tasks, performance metrics, and reporting requirements for the organizer or client. Although this requires a high degree of coordination, the development of anonymous platforms and closed groups has made it much easier to create such networks. The tasks themselves can vary widely — from participating in political flash mobs to spreading information and launching "attacks" in the comments sections of competitors' posts.

An example of the use of a "digital army" that received money "directly from Moscow" is the 2025 election in Moldova. The goal of the campaign was to discredit the "Action and Solidarity" (PAS) political party and Maia Sandu, in particular by spreading narratives that she had interfered in the Romanian elections and betrayed national interests. The main platform was the social media app TikTok (though information

was also disseminated on Facebook and Instagram), and Telegram was used for coordination. A high level of coordination and a gradual increase in the scale of operations made it possible to recruit about 200 so-called "infoleaders," generate 28,708 posts that collectively reached 55,367,950 views, 2,207,894 likes, 295,608 shares, and 239,016 comments across the three platforms.

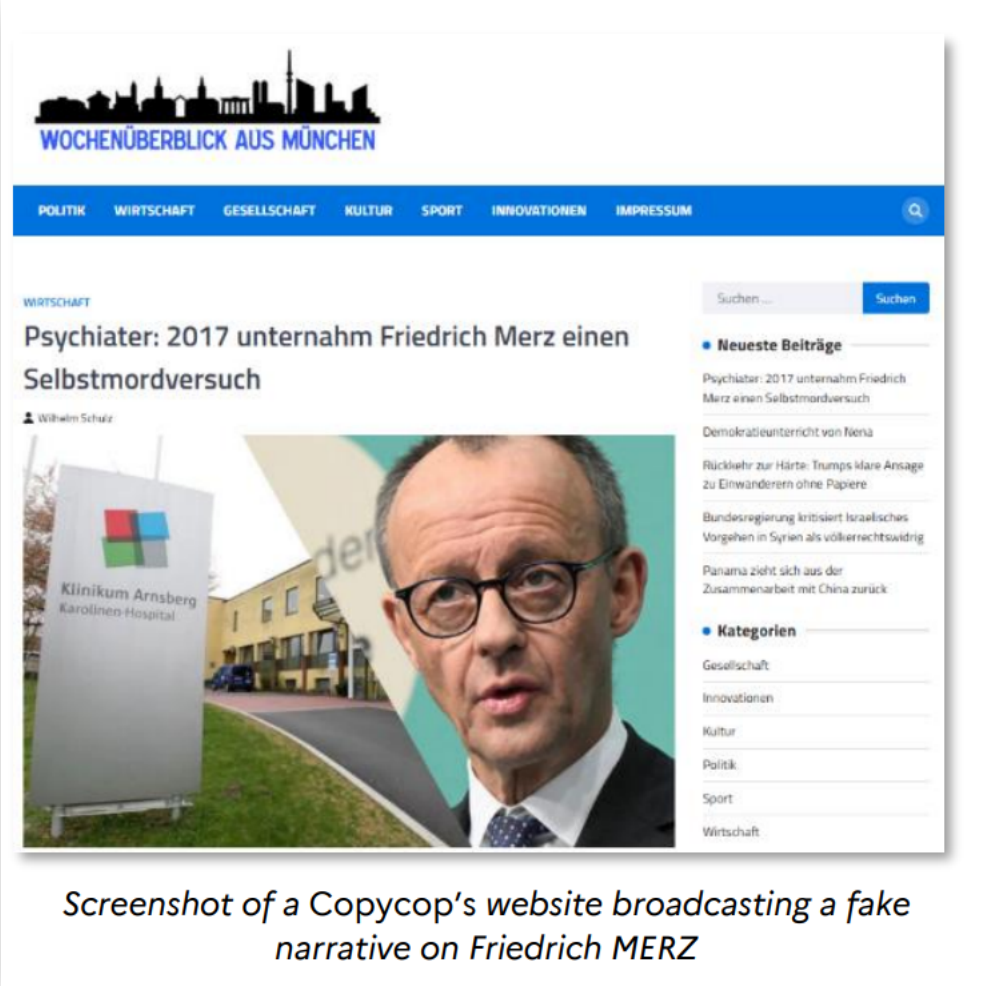



Source: DFRLab

**5. Impersonation of institutions.** This method involves registering similar ("typosquatting") domains and cloning layouts, logos, posts, programs, and documents to impersonate media outlets, political parties, government agencies, or any other institutions.

VIGINUM (the French agency for monitoring foreign influence) has documented many examples. France became the target of Operation Storm-1516 following the dissolution of the National Assembly and the holding of special parliamentary elections in 2024. In particular, the domain name "ensemble-24.fr" was registered, which resembles the official website of the "Ensemble" coalition ("ensemble-2024.fr") and replicated its visual identity. The coalition offered voters a "Macron bonus" of 100 euros in exchange for their vote.

That same year, immediately after the collapse of former Chancellor Olaf Scholz's coalition, the operators of Storm-1516 began attacking Germany, registering over a hundred domain names. The first three operations were aimed at discrediting Robert Habeck (Vice Chancellor): he was accused of sexually assaulting a minor, organizing the arrival of millions of Kenyan workers, and involvement in the theft of works of art. Starting in February 2025, the narratives shifted to discrediting the conservative candidate Friedrich Merz — spreading claims about the alleged absence of the far-right party "Alternative for Germany" (AfD) from the ballots and the destruction of ballots cast in its favor.




*Screenshot of a Copycop's website broadcasting a fake narrative on Friedrich MERZ*

Screenshot from a typosquatted website broadcasting a fake narrative on Friedrich Merz.

Source: General Secretariate of Defense and National Security of France

6. **Bribing influencers or politicians.** Paying bloggers, activists, experts, politicians, or other individuals with influence or their own audience to promote desired narratives without disclosing the source of funding.

For example, in 2024, the U.S. Department of Justice announced that it was shutting down a Russian foreign interference operation led by Sergei Kirienko (first deputy chief of staff of the Russian Federation), which relied on opinion leaders (according to CNN, two employees of the Russian television network RT were accused of transferring approximately $10 million to Tenet Media to bribe influencers) and fake profiles to promote false narratives generated by AI on social media. Overall, this operation combined several methods ("cybersquatting," "doppelganger," the use of AI, etc.) and was aimed at reducing international support for Ukraine, as well as influencing voters in the U.S., particularly in the 2024 presidential election.



Source: Reddit

Another striking example is Calin Georgescu, the pro-Russian candidate in the 2024 Romanian presidential election, who, according to opinion polls, had only 4–7% support but unexpectedly won over 22% of the vote.[11] In addition to aggressive promotion on TikTok and copying Vladimir Putin's campaign tactics, their methods included reaching out to influential figures via email from a South African company called "FA Agency," which offered 1,000 euros per video share to "collaborate." These actions formed the basis of the Romanian Constitutional Court's decision, which annulled the results of the first round of voting.

11 Respondent 2 said that the Georgescu example is no longer a pro-Russian construct but a Russian one. Russia literally modeled the election results to suit its own agenda.

**7. Bribery or the creation of "puppet" media outlets or civil society** organizations. The creation of media outlets or organizations that mimic independent journalism, civil society, or think tanks, without disclosing their sources of funding, in order to promote desired narratives or displace genuinely independent organizations.

Examples of such media in Ukraine include pro-Russian television channels, notably "112 Ukraine," NewsOne, and ZIK, which were banned by a decision of the National Security and Defense Council.

In addition, researchers at the Wilfrid Martins Center for European Studies have described a broad network of "puppet" organizations created or funded by the Russian government. These include the EU offices of the "Russian World" and "Rossotrudnichestvo" foundations, the Valdai Club, funding directed to the French Institute of International and Strategic Relations, the activities of the Eurasian Observatory for Democracy and Elections — which legitimizes elections in temporarily occupied territories — as well as the Berlin-based "Dialogue of Civilizations" Research Institute, whose mission is to coordinate a global network of Russian think tanks. These organizations were "physically" used to displace other NGOs during the OSCE conference.



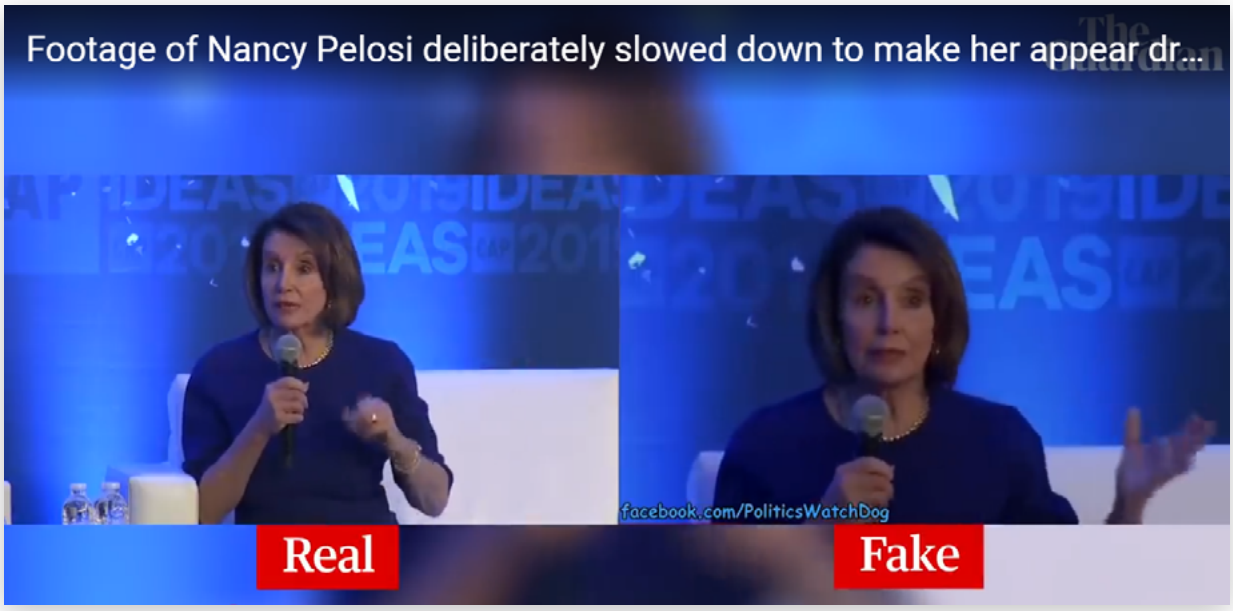

A cover of the study on Russian government-funded organizations in the EU.
Source: Wilfried Martens Centre for European Studies

## 4.2. HOW CAN CONTENT AND PROMOTION BE MANIPULATED?

**1. Different degrees of content manipulation.** Manipulation can include both completely fabricated materials (news, articles, exposés, etc.) and partially altered (date, location, headline, characters, etc.) or distorted (removal of content, slowing down the video, replacement of subtitles or logos, etc.) materials. In the latter case, disinformation — even material that is easy to fact-check — can have an advantage during large-scale information operations, since it can be produced quickly and cheaply (for example, one can take "negative" material about one politician and pass it off as information about another, simply by replacing the first and last names).

As an example of entirely fabricated content, we can once again cite the "Doppelganger" operation during the 2025 presidential election in Poland, where, from March 4 to April 4, 279 tweets and 43 fake articles were published, "attributed" to 13 real Polish media outlets.

Among the "cheap" (which does not mean ineffective) manipulations, we can mention the "cheap fake" involving a video of Nancy Pelosi (the 52nd Speaker of the U.S. House of Representatives). The original video was deliberately slowed down to create the impression that she was intoxicated. This and similar clips appeared on TikTok and were later posted on YouTube, Facebook, and Twitter.




Screenshot comparing a real and a fake video with Nancy Pelosi. Source: The Guardian

**2. Manipulation of various forms of content.** In today's digital age, manipulation is not limited to distorting textual information but can also involve high-quality fake videos or audio. Advances in AI have made the tools for creating such content widely available, and without specialized skills, it is surprisingly difficult to distinguish it from the real thing, so consumers can easily be led to believe it is authentic.[12]

An example of the use of deepfakes is a video featuring Maia Sandu, shared on the Telegram channel "Sandu Oficial," in which she allegedly speaks ironically about the standard of living of Moldovan citizens. Another deepfake video is mentioned in the OSCE report on the results of the 2025 parliamentary elections in Moldova. It claimed that the cost of gas for citizens would be reduced by 50 percent.

Voice forgery is technically simpler and cheaper than video forgery, and it was also used in the run-up to the elections. For example, two days before voting (the "quiet period") in the 2023 parliamentary elections in Slovakia, a deepfake audio recording was circulated in which the well-known journalist Monika Todova "discussed" the falsification of election results with Michal Šimečka, the leader of the "Progressive Slovakia" party.

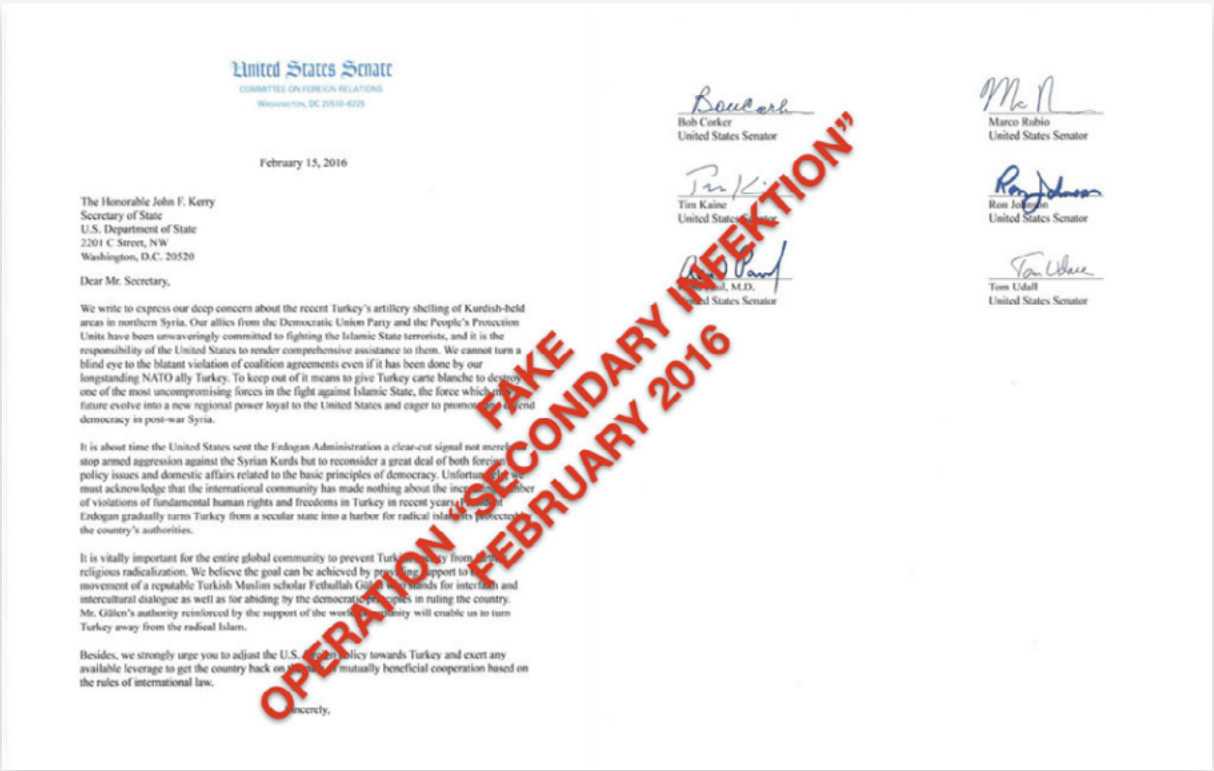
Another example of the use of such technology is robocalls. Specifically, in the U.S., a man was charged with sending automated calls to thousands of New Hampshire residents featuring a generated voice of President Joe Biden urging them to abstain from voting in the primaries.

However, fake videos and audio can be created not only using AI or other digital technologies but also through "live staging." VIGINUM documented audio content (as part of the aforementioned Operation Storm-1516) in which a person speaking Arabic accuses Ukraine of recruiting Islamic State militants. The video also features a simulated conversation between Volodymyr Zelenskyy and his wife in a mixture of Ukrainian and Russian.

12 The accessibility of AI generated content and the improvement in its quality was highlighted by respondent 1.

**3. Forgery of official documents.** The dissemination of manipulative posts on social media without sufficient evidence may not inspire trust; so to amplify the impact of FIMI operations, they often involve fabricating official documents or those affiliated with official institutions (orders, letters, draft decisions, reports, etc.), as well as opinion polls or scientific studies.

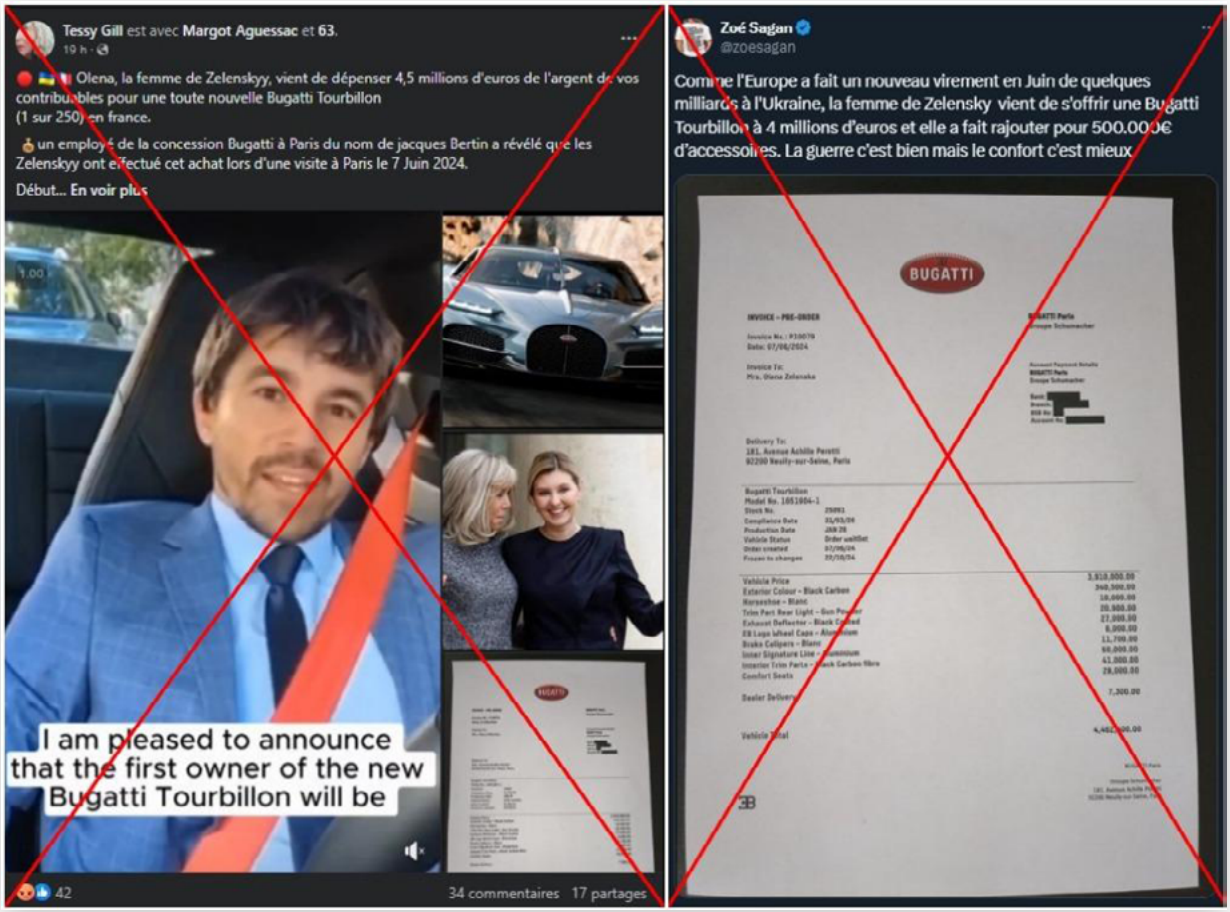
For example, the "Secondary Infektion" operation stands out for its regular use of forged documents, sometimes of surprisingly poor quality. The Graphika team identified more than 250 suspected forgeries (ranging from letters to petitions) that were circulated online during this operation. Among the forgeries were letters, tweets, and blog posts purporting to be from high-ranking officials, including U.S. Secretary of State Mike Pompeo, former White House Chief of Staff General John Kelly, various members of the U.S. Senate Committees on Foreign Relations and Intelligence, representatives of the governments of Germany, the United Kingdom, and Ukraine, as well as former heads of state, including Carl Bildt (Sweden) and Mikheil Saakashvili (Georgia). In addition, part of the operation involved the dissemination of forged documents, images, and videos attributed to a wide range of nongovernmental organizations: from the World Anti-Doping Agency (WADA) and the Organization for Security and Co-operation in Europe (OSCE) to the Committee to Protect Journalists and the environmental organization Greenpeace.




An example of a fake document (operation "Secondary Infection"). Source: Graphika

A report on FIMI's "Overload" operation describes a case in which seven videos, mostly bearing the BBC logo, were falsely labeled as investigations by the Bellingcat group. The videos claimed that Bellingcat was conducting investigations into Ukraine or exposing Ukrainian leaders for alleged crimes or corruption.

An example of forged financial documents is the 2024 case, in which publications distributed in several languages claimed that Olena Zelenska, the wife of the President of Ukraine, had allegedly purchased a Bugatti Tourbillon hypercar for no less than 3.8 million euros. To support this claim, they presented a video featuring a fake Bugatti representative and a forged invoice.




Examples of untruthful posts on purchasing a Bugatti car by Olena Zelenska. Source: Factuel

**4. Manipulation of content promotion.** As noted above, FIMI can involve not only misleading content but also manipulation during its promotion (though these methods are usually combined). To achieve this, they may use methods such as flooding the information space, hijacking or replacing the content of others' hashtags, artificially inflating engagement (likes, reposts, views, etc.), and technical circumvention of promotion algorithms (such as SEO optimization of fake websites under candidates' names or filling low-frequency search queries in contextual advertising, etc.).

For example, less than two days before the final round of the French election, a new campaign using the hashtag #MacronLeaks spread rapidly across many social media platforms. Just three and a half hours after the first post, the number of tweets using this hashtag reached 47,000. It directed users to a purported leak of emails from Emmanuel Macron's campaign, which allegedly contained evidence of offshore accounts, tax evasion, and a number of other illegal activities. The biggest surge occurred when WikiLeaks published a link to this "leak."

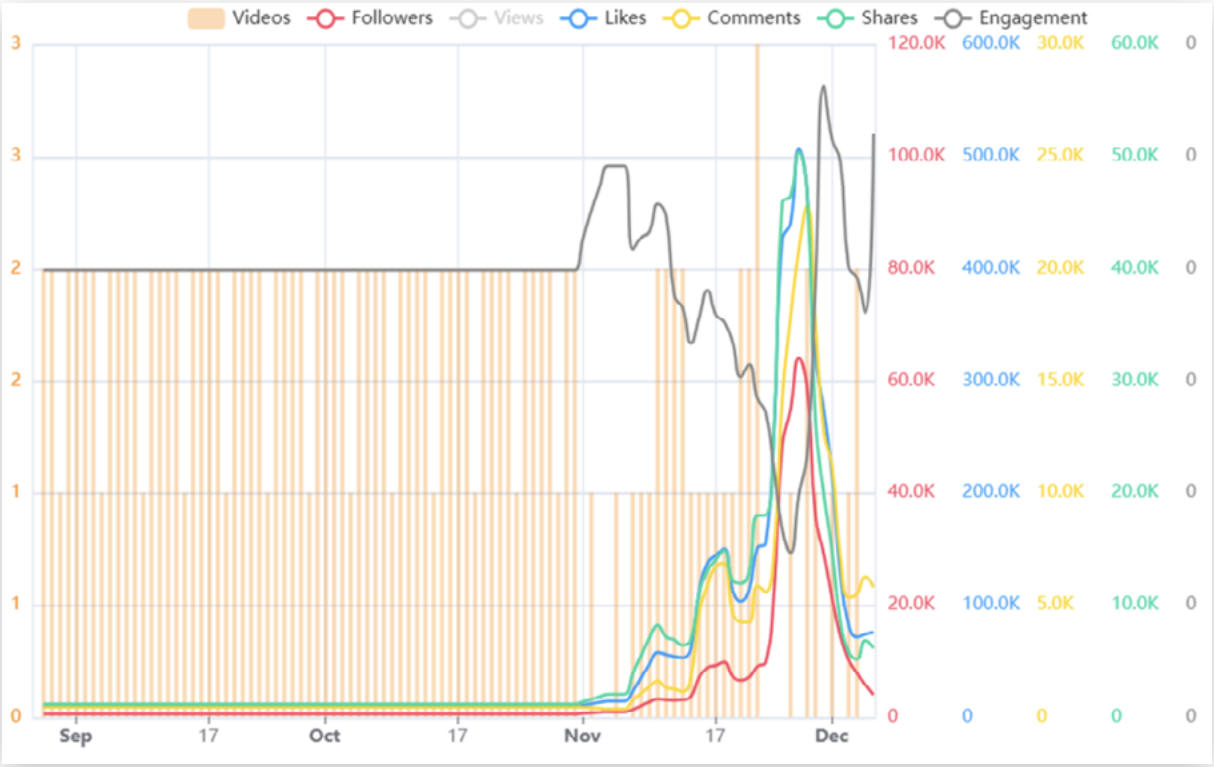



A post from WikiLeaks on the X about a possible data leak about the election campaign of Emmanuel Macron. Source: DFRLab

Another example is the promotion of the aforementioned Calin Georgescu, a pro-Russian candidate in the 2024 Romanian presidential election. More than 1,800 pieces of campaign material were distributed through a central channel known as "Propagator." This channel also coordinated the further dissemination of information across separate Telegram channels[13] — for each of Romania's 41 counties, as well as on the social media platforms TikTok and Facebook. TikTok became the primary hub

13 Respondent 2 highlighted that many people in Ukraine receive information through the Russia controlled Telegram-channels.

for this campaign. Georgescu's account successfully amassed over 540,000 followers by the first round of voting in late November. That month, his page's popularity skyrocketed: followers increased by 2,541%, likes by 1,496%, comments by 1,581%, and shares by 1,146%. Ultimately, this led to the 12 most popular hashtags from Georgescu's campaign garnering 1.4 billion views in Romania, across the EU, and beyond.




Increase in popularity of a TikTok account of Calin Georgescu. Source: DFRLab

**5. Manipulative countermeasures against opponents' campaigns.** FIMI operations are, in one way or another, aimed either at promoting certain narratives or at countering specific views, individuals, or organizations. In the latter case, they may use methods that abuse platform moderation, such as filing complaints against opponents' accounts or content (mass-reporting) or a coordinated flood of commenters (brigading).

In its 2021 report, Meta reported four operations of coordinated inauthentic behavior (CIB) originating from China, Palestine, Poland, and Belarus; one brigading network in Italy and France for coordinated swarms of commenters; and one network in Vietnam for mass reporting. A 2020 report by Oxford University researchers noted that the technique of mass reporting had been observed in seven countries.

## 4.3. WHAT TARGETS OF FIMI OPERATIONS SHOULD BE EXPECTED IN UKRAINE?

FIMI operations are constantly evolving, expanding their arsenal of methods and targets. However, in recent years, a whole catalog of examples of information interference has emerged in Ukraine and around the world, which should be studied to preserve the legitimacy of the electoral process in future campaigns. At the same time, Ukraine is a unique case in which, over a prolonged period without elections, the country has remained at the "top" of FIMI incidents (112 out of 540 documented by the EEAS in its 2026 report).

It is difficult to predict the potential targets and methods of future FIMI operations in Ukraine's elections for two main reasons: first, the uncertainty surrounding the end of the war and, consequently, the timing of the elections and the pool of potential participants (primarily candidates and parties); second, the rapid evolution of information technologies and manipulation methods. Therefore, first and foremost, we must be prepared for at least those FIMI operations that have already been empirically confirmed. On this basis, we can predict a number of potential targets for manipulative information interference.

1. **Delegitimization of election results.** FIMI operations can seriously undermine trust in elections, which will obviously delegitimize the elected government in the eyes of both its own citizens and the international community. The target of an attack may be not only the voting results but also any stage of the electoral process; thus, narratives may cover topics such as fraud, corruption, and foreign control, and may incite protests or encourage non-participation in elections (reduced voter turnout). The impact of such attacks will be particularly dangerous against the backdrop of the challenges of the post-war period.[14] In its guide to monitoring election campaigns on social media, the OSCE also draws attention to the problem of foreign interference in elections and political discourse, as well as the use of bots and trolls to set the public agenda, shape voter opinion, and increase or decrease voter turnout.

According to estimates by the Atlantic Council, most Russian disinformation messages during the 2019 presidential election in Ukraine stemmed from the overarching narrative that the election would be rigged and illegitimate, and therefore should not be trusted regardless of the outcome. Kremlin propaganda sought to use the election to discredit not only democratic processes but also Ukraine as a state. Russian pseudo-media outlets made numerous false accusations regarding the alleged spread

14 This was emphasized by Respondent 1.

of Nazism in Ukraine, as well as claims that the state was planning terrorist attacks and contract killings on its territory to influence the election. Another grand narrative spread during the election campaign portrayed Ukraine as being under "external control by the West."

Other countries have also faced widespread FIMI operations aimed at delegitimizing elections. In particular, in the Czech Republic, narratives were spread about election fraud following the "Romanian scenario" (posts claiming that the Constitutional Court and the government were preparing to "steal" the election garnered up to 8,000 views on Telegram); state-imposed censorship under the pretext of combating disinformation (the goal was twofold — to discredit measures to counter FIMI and to equate them with authoritarian practices); the normalization of propaganda on election day (the neČT24 outlet published an interview with Russian pseudo-political analyst Vadim Trukhachev on the very day of the vote, which was reprinted by four other dubious publications).

The results of the first round of the 2024 presidential election in Romania — with a stunning victory for the pro-Russian candidate Georgescu — were themselves the result of a large-scale FIMI operation promoting him on social media; after the Constitutional Court annulled the results, criticism intensified (with claims that the election results had been "stolen"), and protests even broke out.

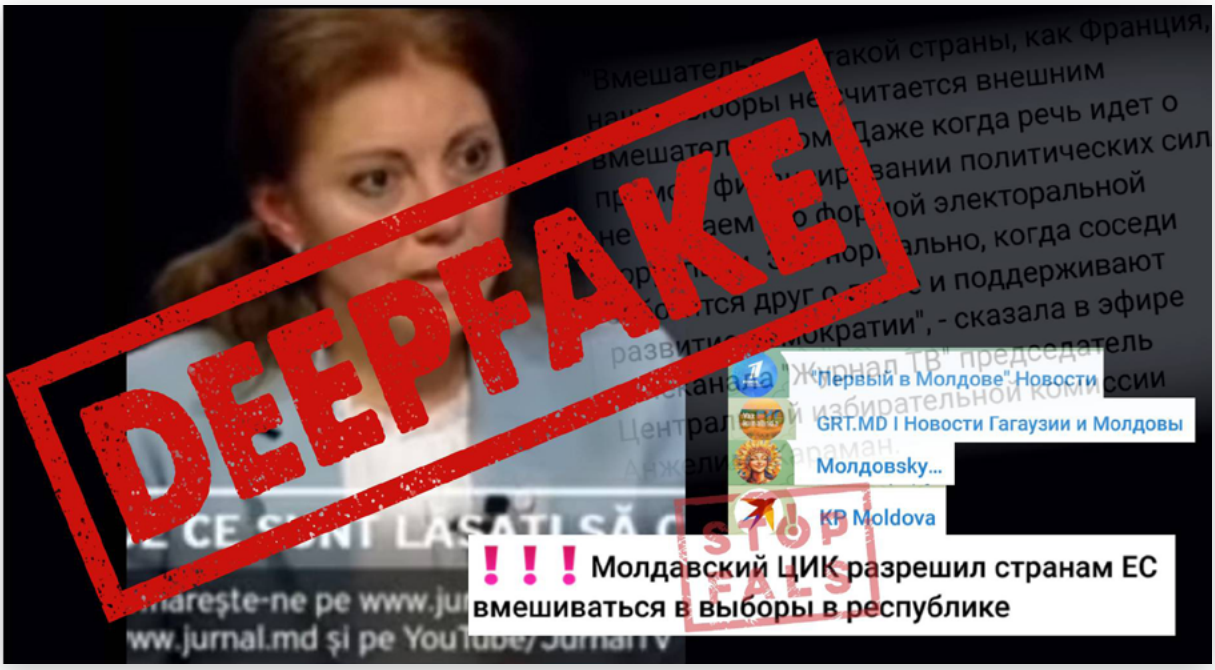
Ahead of the Bundestag elections in Germany, several fake videos appeared online claiming that mail-in voting was allegedly being manipulated to the detriment of the AfD party. One of the videos shows two ballots from Leipzig's 151st electoral district on which the AfD is not listed. In a similar video, where the AfD is not listed on the ballot, an unidentified person in the background says indignantly: "I just received my ballots, and what can I say? This is fraud — the AfD isn't listed, but everyone else is." The fake videos became particularly popular on Platform X: some of them had over 500,000 views.



Protests in Romania. Source: Euractiv

**2. Discrediting government authorities (particularly election administration bodies).** Undermining trust in state institutions — especially election commissions, law enforcement agencies, and courts — will result in the delegitimization of the election results as a whole. In contrast, more narrowly targeted attacks can lead to political crises, changes in the personnel of government bodies, intensified parliamentary debate, or discord within a coalition. Furthermore, the erosion of trust undermines legal mechanisms for protecting electoral rights, resolving disputes, and preventing and investigating violations, which affects the perception of the state not only as a democracy but also as a state governed by the rule of law.

For example, in its report on the results of the 2025 parliamentary elections in Moldova, the OSCE emphasizes that on the eve of the vote (especially one week before the vote), Moldova's Central Election Commission (CEC) was the target of cyberattacks (attempts to overload the CEC's servers) and disinformation campaigns from abroad aimed at undermining public trust in this body by spreading misinformation. Several Telegram channels and Russian websites (including Russian Foreign Ministry spokesperson Maria Zakharova) shared an AI-generated deepfake in which Anzhelika Karaman (chair of the CEC) states that "interference by a country such as France in our elections is not considered foreign interference".[15]




Screenshot from a fake video showing a Chair of the Moldova CEC Alina Karaman.
Source: Stop Fals

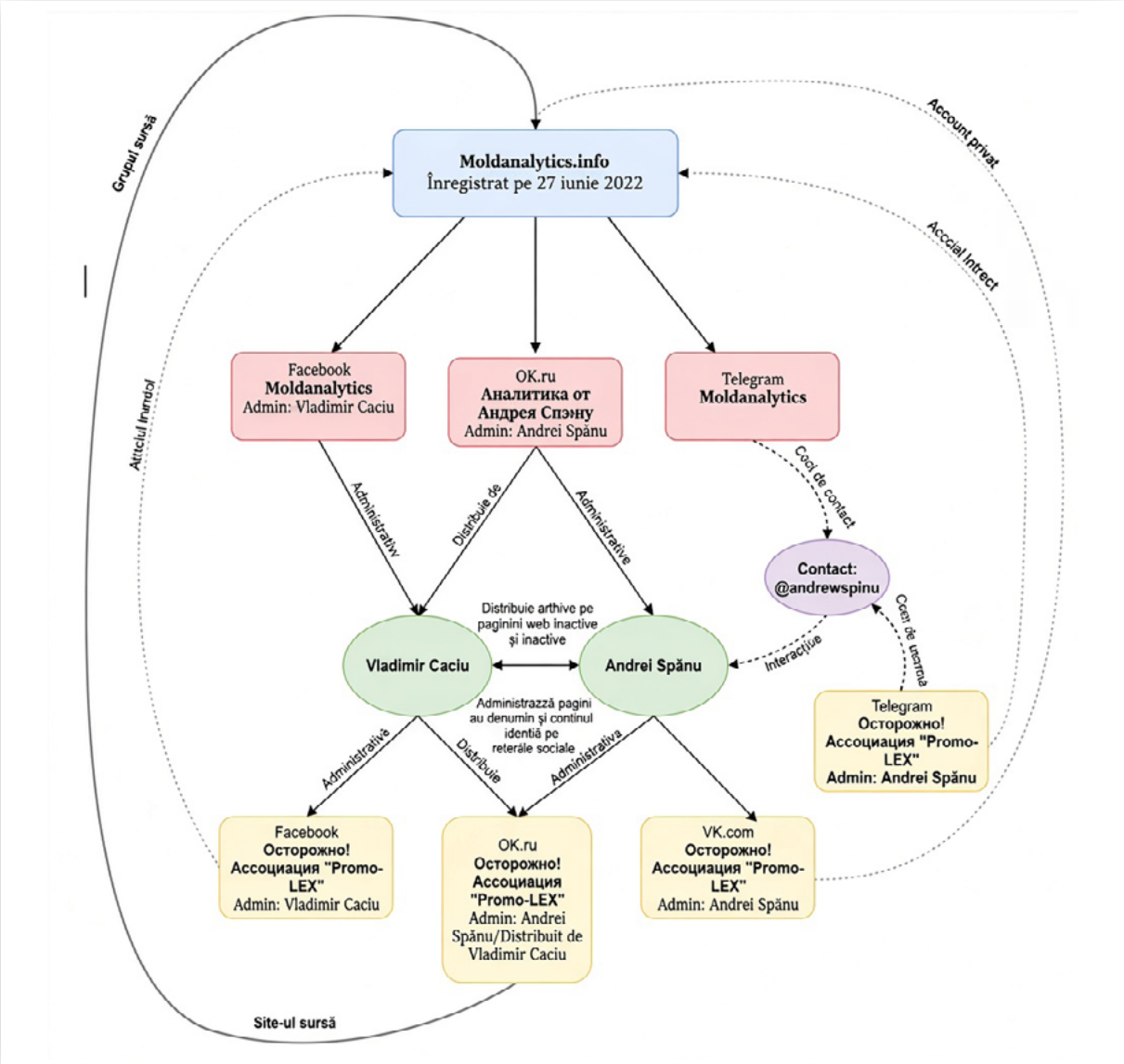
15 Respondent 3 said that mitigating the consequences of this FIMI operation required significant effort and resources.

In the Czech Republic, on the eve of the 2025 parliamentary elections, the eDoklady app — which allows users to verify their identity and obtain a ballot — experienced a malfunction. According to experts at the FIMI Information Sharing and Analysis Center (FIMI-ISAC), this situation illustrates how technical malfunctions can quickly become a source of disinformation if official communication is delayed or unclear. Although government authorities responded effectively, this incident underscores the need for proactive and transparent public communication protocols regarding all critical digital systems.

**3. Discrediting independent observers and the use of pseudo-monitoring mechanisms.** Independent international and national observation missions play a crucial role not only as a means of building trust in the electoral process but also as a mechanism for preventing violations and abuses, particularly the falsification of voting results. Therefore, FIMI operations, carried out primarily by authoritarian regimes, may focus on discrediting observers or preventing them from attending elections, manipulating reports and conclusions, and deploying "fake" missions to conduct subversive activities within the target state or on international platforms.[16]

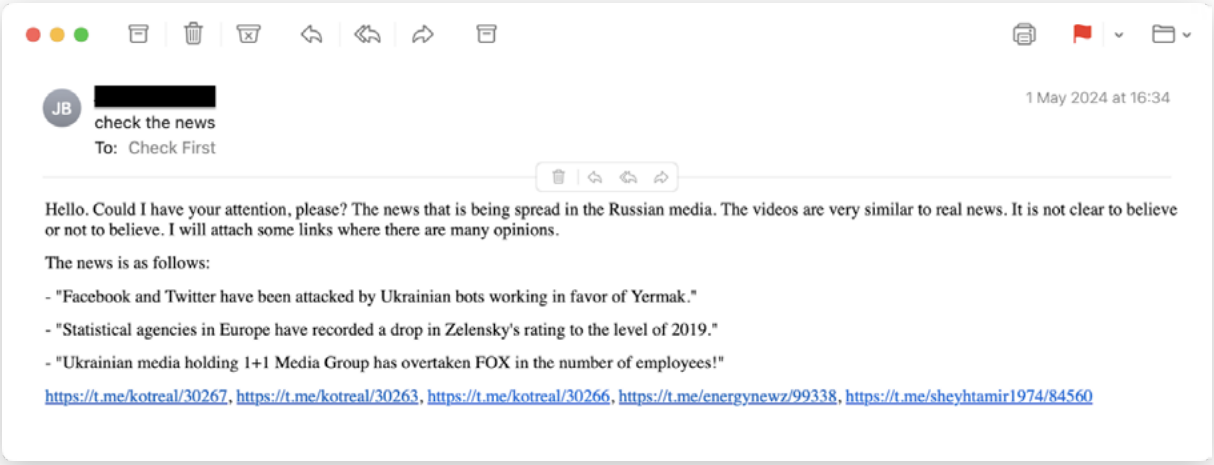
Although there are not many direct, documented FIMI operations by third countries against national observation missions (i.e., not carried out by the authorities of the host country itself, which are usually authoritarian), one such case has been recorded in Moldova. A report by StratCom (a government agency established to protect the information space and combat manipulation and foreign interference) cites the example of the Moldanalytics[.]info, which uses Facebook, Telegram, OK.ru, and VK.com to publish content hostile to Moldovan state institutions and civil society organizations, specifically Promo-LEX and Zona de Securitate. For example, fake pages were created that purportedly are run by "former members" of the targeted CSOs. In reality, however, they almost entirely repost material from propaganda sources in order to undermine trust in these organizations.

16 Respondents 1, 3, and 10 emphasized Russia's use of this mechanism or the threats it poses.




The scheme for disseminating disinformation on Moldovan CSOs.
Source: Stratcom *(the image resolution was improved with the help of Grok — author's note)*

The previously mentioned Operation Overload serves as an example of how monitoring missions and fact-checkers can be overwhelmed. Its name literally describes the tactic — "overloading" the fact-checking ecosystem with a significant amount of fabricated material, requests for verification, and coordinated posts. Amory L., CTO of CheckFirst, said: "Overload is a 'Matryoshka' on steroids." More than 800 organizations were targeted by nearly 2,400 tweets, and over 200 targeted emails were sent to newsrooms across Europe and beyond. The project achieved its goals within the first few months, as more than 250 articles were published fact-checking or debunking information from fake sources created for Operation Overload. Verifying information disseminated in such large-scale operations can require significant resources, which is why these operations are capable of hindering or even blocking the work of specialized organizations by exhausting their capacity.




Request for verification of information under the Operation Overload. Source: Check First

In addition, the Atlantic Council described instances of manipulation of observation reports: Kremlin-controlled quasi-media outlets distorted the report of the Parliamentary Assembly of the Council of Europe (PACE) on Ukraine, and a few weeks later, the report of the OSCE's ODIHR. In both cases, Moscow-controlled media ignored the generally neutral or even positive tone of the reports (PACE highly commended the country's preparations for the elections; the OSCE ODIHR acknowledged that the elections met constitutional requirements) and exaggerated even the slightest negative aspects.

Georgia served as an example of efforts to undermine independent observation and the use of fake observers, particularly after the adoption of the "foreign agents" law in 2024. In the 2025 local elections (as of September 29), the Central Election Commission registered 23 organizations with 7,865 observers, of whom 7,138 (about 91%) belonged to five organizations considered to be affiliated with the ruling "Georgian Dream" party. The two largest organizations were founded by attorney Grigol Gagnidze, who regularly shares the party's posts on social media.

**4. Discrediting parties and candidates.** Discrediting specific parties or candidates is the most obvious target of foreign interference. Such FIMI operations are carried out not only on the eve of or during the electoral process (although, of course, they intensify during this period), but also at any stage of the electoral cycle.

One example is the 2024 U.S. election, where a fake video targeting Democratic Party candidate Kamala Harris was circulated as part of the Russian operation Storm-1516. In this video, a woman claims that as a child in 2011, she was allegedly injured in a car accident involving Harris, who fled the scene, leaving the woman confined to a wheelchair. Later, fabricated allegations of sexual assault were spread against Tim

Walz — Kamala Harris's running mate in the 2024 presidential campaign and the Democratic Party's candidate for U.S. vice president. According to media reports and analysts, John Mark Dugan, a former Florida police officer who now lives in Moscow, is responsible for dozens of fake news websites in the U.S. He creates these websites and fills them with articles rewritten using AI tools.

Similar tactics were also used during the German Bundestag elections. In addition, the EEAS published a separate report in 2024 on the mass creation of fake political party websites (Operation Doppelganger), where absurd or harmful statements by politicians were published to lower their approval ratings among voters.




**Figure 4:** Examples of the Doppelganger impersonation of La Stampa with content related to elections

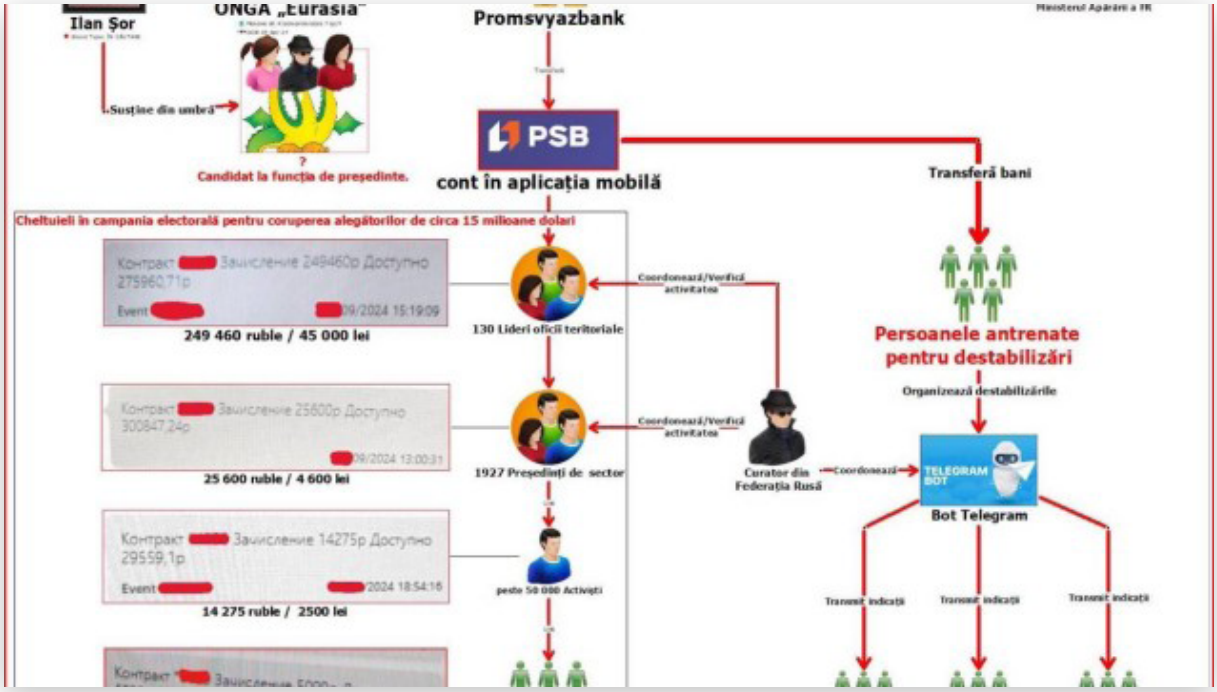
**Figure 6:** Examples of the Polityka impersonation of Die Welt with content related to elections

Examples of Doppelganger websites. Source: EEAS

**5. Attacks on Voters.** Since voters are the primary consumers of this content — and it is ultimately they who determine the outcome of elections in democratic countries — it can be argued that, in one way or another, they are the target of most FIMI operations, which distort the free formation and expression of their will. However, looking more closely, voters in general, a specific group of voters (for example, those living abroad, representing national minorities, in certain professions, etc.), or their personal data may become the target of information interference aimed at polarization (the OPORA Civic Network has studied polarization among different groups in Ukrainian society),

bribery, or intimidation. For Ukraine, the post-war elections will raise pressing issues regarding security (both physical and informational) and the protection of voting rights for specific categories of individuals (military personnel, citizens abroad, internally displaced persons, etc.[17]).

Moldova's experience may be relevant for Ukraine.[18] During the 2025 parliamentary elections in that country, the OSCE documented reports of a series of threats of bombings at the premises of some precinct election commissions both within the country and abroad, as well as on bridges across the Dniester River, which led to a temporary suspension of the voting process and caused long lines at river crossings. Prior to this, the "SHOR" political party had actively used social media to bribe citizens, which was one of the reasons for its ban. The very organization of voting abroad, where pro-European sentiments prevailed among the diaspora, became the subject of intense criticism from the Party of Socialists of the Republic of Moldova (PSRM) — a pro-Russian political force that supported the candidacy of independent candidate Alexandru Stoianoglo in the 2024 presidential election.




The scheme of illegal funding of political parties and voter bribery in Moldova.
Source: Anti-Corruption Prosecutor's Office of Moldova

17 Respondent 2 emphasized that Russia would potentially target their FIMI operations at draft dodgers.

18 The relevance of Moldova's experience was also emphasized by respondent 1.

Examples of intimidation (both physical and online) have been documented in the United States. According to the FBI, one such case involved reports of bomb threats at polling places in several states, many of which likely originated from Russian email domains. CBC News reported that the false bomb threats were directed at polling places in five "swing" states: Georgia, Michigan, Arizona, Wisconsin, and Pennsylvania. As a result, Georgia had to temporarily evacuate some polling places.

Another example of cybersecurity threats (though the fact of foreign interference itself has not been confirmed) involved robocall technology, similar to the aforementioned example featuring Joe Biden's voice. Well-known American right-wing political lobbyists and conspiracy theorists, acting on behalf of the fake "human rights" organization "Project 1599," made approximately 85,000 automated phone calls through the Message Communications platform. These calls, directed primarily at people of color, conveyed a message that their personal data, when voting by mail, would allegedly end up in a database that would be used for persecution by the police and debt collectors, and even for mandatory COVID-19 vaccination.

Another example highlighted in the EEAS report demonstrates targeting of a specific audience. For example, in Germany, farmers' protests became one of the targets of interference. Specifically, 73 cases were identified in which existing discontent was artificially stoked to undermine trust in institutions and sow division within society.

In general, FIMI operations, by spreading certain narratives, are often targeted at a specific audience and therefore focus on topics that are important to that audience. In the aforementioned "Doppelganger" operation, such topics included migration, energy, climate, the war in Ukraine, and the promotion or discrediting of specific political parties or candidates.

# CONCLUSIONS AND RECOMMENDATIONS

## CONCLUSIONS

Foreign interference is based on the principle of non-interference in the internal affairs of states, and elections — as a means of legitimizing authority — are at the core of these "internal affairs." There is no single definition, but the approaches of the European Commission, the European Parliament, the DHS, and the legislation of the United States, Australia, Canada, and the OECD share common features: interference may be carried out by a state directly or through intermediaries, and the method of operation is characterized by secrecy and deception. Differences concern the object of interference and whether illegality is a mandatory characteristic. It is advisable to divide the object of interference into a general one — state sovereignty — and a specific one — a particular sphere of social relations (for example, elections).

Forms of interference should be distinguished from the spheres in which they occur: elections are a specific object, while FIMI, foreign financial interference (FFI), and cyber interference are forms, each of which employs its own methods and specific actions. This approach eliminates the confusion characteristic of the OECD's classification of channels, where interference in elections is singled out separately, even though it is carried out using the same instruments. Funding is a cross-cutting indicator of interference: in a broad sense, it refers to the provision of any form of interference; in a narrow sense, it refers to the transfer of foreign funds into the accounts of parties or candidates.

Coercion cannot be considered a mandatory element of interference. The formula established by the International Court of Justice in the case "Nicaragua v. United States of America," according to which coercion constitutes the "very essence" of unlawful interference, does not stand the test of time. Information manipulation leaves the recipient formally free, while its impact on sovereignty may be even greater than that of threats or violence. For FIMI, the absence of coercion is rather typical, although

the two may coexist. Illegality is equally optional: the EEAS defines FIMI as a "mostly non-illegal" model of behavior, placing this phenomenon in a "gray area" of legal restrictions. Unlike FIMI, financial interference is usually explicitly prohibited.

The key distinction between interference and legitimate foreign influence is transparency. Foreign influence encompasses diplomacy, lobbying, public communications, and the like, and is a legitimate aspect of international relations provided that the recipient understands the source and nature of the influence (who is exerting it, with whose funds, and in whose interests). Interference, on the other hand, is covert or deceptive and may — though not necessarily — be accompanied by coercion or illegal activities. Transparency in legitimate influence is ensured by specialized tools such as the UK's Foreign Influence Registration Scheme or the EU Transparency Register.

Attribution to a specific state is not required to classify an act as foreign interference. This is confirmed by both practice (65% of the 540 incidents documented by the EEAS remained unattributed, and 90.5% of the mapped channels are covert resources), and by legislation: the UK National Security Act employs a "foreign state condition" that can be met without identifying a specific state, while the Australian Criminal Code Act allows for an individual's activities not necessarily to relate to a specific entity. At the same time, technical attribution sufficient for use in analysis should be distinguished from legal attribution, for which the standards of proof are significantly higher. Since the disruptive effect of an individual message does not depend on its origin, manipulation methods should be countered regardless of the presence of a foreign element. At the same time, an analysis of the indicators pointing to such interference (foreign actor, control, interest, funding, intermediaries) is necessary to identify coordinated campaigns and select appropriate response measures.

The line between FIMI and freedom of expression remains the most challenging practical issue. Freedom of expression extends to ideas that may shock, offend, or disturb, regardless of the truthfulness of the content, and combating "disinformation" does not fall within the legitimate aims of restriction under Art. 10 of the Convention; therefore, it is necessary to demonstrate the threat that FIMI poses to other values — primarily national security or the rights of others. The ECHR's decision in the case of "Bradshaw and Others v. The United Kingdom" merely opens the judicial debate, as the Court recognized the state's positive obligations to counter interference, though less stringent than those under Articles 2–4 of the Convention, granted broad discretion in the choice of measures, confirmed the difficulty of proving a causal link between an information campaign and the outcome of a vote, and cautioned against impulsive reactions bordering on censorship. Therefore, clear criteria and serious grounds are

required to exclude conduct from the protection of freedom of expression; in their absence, the dissemination of information must be presumed lawful.

The concept of FIMI is not synonymous with disinformation: it is narrower, as it concerns only the manipulation of information by foreign actors, and broader, as it does not require proof that the disseminated information is false. What is decisive is not the content, but deceptive or manipulative behavior, the most obvious example of which is coordinated inauthentic behavior (CIB). The following should be considered mandatory characteristics of FIMI: 1) manipulative (deceptive or covert) behavior, which may relate to the authenticity of actions, goals, intentions, or funding; 2) coordination, indicating premeditated behavior, intent, and purpose; 3) a foreign link — a connection to a foreign state or its proxy. While not mandatory, the following are useful for identification: coercion, illegal activity, violations of platform policies and media standards, deceptive content, funding, and advocacy for the interests of a specific state.

The set of characteristics that must be proven depends on the chosen response: for the application of legal liability mechanisms — the existence of the elements of an offense; for the application of sanctions or similar mechanisms — a threat to national security or non-compliance with legal requirements; for retaliation — identification; for content bans by platforms or media outlets — violations of policies, codes of ethics, or standards; for reactive soft-power measures (fact-checking, debunking information, disclosing facts such as funding sources, etc.) — individual indicators are sufficient (e.g., deceptive behavior or foreign funding); for proactive (preventive) soft power measures (raising awareness, media literacy, information dissemination, and education, etc.) — none are required, as they are designed to prevent threats.

Alongside the ABCDE methodology (actors, behavior, content, degree, and impact), the "subject-object-method-content" approach is universal and commonly used in legal analysis. The transnational nature of FIMI requires a unified taxonomy (the most applicable today is DISARM, which, however, can be further modified for FIMI operations) and a common data format (e.g., STIX), integrated into guidelines and training programs.

Manipulation of actors and assets is evolving from the creation of fake accounts (sockpuppets) to the acquisition or hacking of real ones, which allows for bypassing platform verifications and exploiting the audience's trust, as well as the impersonation of individuals, media outlets, and institutions — ranging from domain cloning to the generation of voices and images using AI. A separate level of organization involves paid influence networks with hired staff and performance metrics, the bribery of influencers and politicians, and the creation of "controlled" media and fake civil

society organizations. The development of AI has made these methods cheaper, while proving the existence of funding remains the most effective indicator, as it confirms both coordination and a "foreign" element.

Content manipulation encompasses a wide range of phenomena — from completely fabricated materials and forged official documents to "cheap fakes," deepfake videos, synthesized audio, and robocalls. Equally significant are manipulations involving promotion: flooding, hashtag hijacking, artificially inflating engagement, circumventing algorithms, as well as countering opponents through mass complaints and a flood of commenters. Hence the key conclusion: verifying the truthfulness of content is not enough; effective identification of FIMI requires analysis of behavior and the infrastructure used for dissemination.

For Ukraine, the following risks associated with such FIMI operations may be relevant: delegitimizing election results and specific stages of the process; discrediting government bodies, particularly election administrators; discrediting observers, along with pseudo-monitoring and the depletion of monitoring missions' resources; discrediting parties and candidates; attacks on voters (polarization, bribery, intimidation). A distinctive feature of the Ukrainian situation is that the country ranks among the top in terms of documented FIMI incidents (112 out of 540 in the 2026 EEAS report) even in the absence of electoral processes. Therefore, with the start of the post-war electoral cycle, we should expect not only new methods but, above all, an escalation of tried-and-tested ones — with increased focus on security narratives and the electoral rights of specific groups (military personnel, IDPs, and citizens abroad).

# RECOMMENDATIONS

The conclusions drawn and the results of the interviews conducted allow us to formulate preliminary recommendations, which can be grouped thematically into several categories.

**Strengthening institutional capacity:**

- conducting an audit of the powers of existing agencies (the Center for Countering Disinformation, the Center for Strategic Communications and Information Security, the State Service for Special Communications and Information Protection, the Security Service of Ukraine, etc.) to identify overlapping functions;
- discuss options for strengthening institutional capacity and make decisions regarding the body responsible for countering FIMI (a comparison of various models is provided in the Appendix) — for example, creating a separate specialized agency (modeled after France's VIGINUM), an interagency coordination body[19] (analogous to Stratcom[20] or the interagency working group proposed in Article 35 of the CEC's draft law)[21] or expanding the powers of existing bodies (primarily the Center for Countering Disinformation, established under the National Security and Defense Council of Ukraine);

19 Respondent 12 supports the coordinating interagency format of the body.

20 Its council consists of a director, as well as representatives from the Office of the President, Parliament, the State Chancellery, the Ministry of Defense, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Council on Television and Radio, the Information and Security Service, and two representatives from civil society.

21 Respondent 10 expressed an idea to establish an analogue to the National Cybersecurity Coordination Center.

- regulating the activities of the FIMI countermeasures body, including the publication of annual and technical reports on the results of specific operations, the issuance of sector-specific preventive guidelines, and the launch of pre-banking and de-banking platforms *(see the introduction of countermeasures below)*;

- establishing interagency cooperation and the exchange of expertise, in particular among the following bodies: the Center for Countering Disinformation (established under the National Security and Defense Council of Ukraine);[22] the National Security and Defense Council of Ukraine (in general);[23] the Center for Strategic Communications and Information Security (under the Ministry of Culture of Ukraine); the National Council of Ukraine on Television and Radio Broadcasting;[24] the Central Election Commission; the National Commission for State Regulation in the Spheres of Electronic Communications, Radio Frequency Spectrum, and Postal Services;[25] State Service for Special Communications and Information Protection (in particular, the National Center for Operational and Technical Management of Electronic Communications Networks and the State Center for Cyber Protection of the State Service for Special Communications); State Financial Monitoring Service of Ukraine; National Agency for the Prevention of Corruption; Security Service of Ukraine[26] (in particular, the Counterintelligence Department,[27] the Department for the Protection of National Sovereignty, the Cybersecurity Department, as

22 Respondent 4 emphasized that the CCD has the capacity to counter foreign interference through, in particular, contacts with Big Tech.

23 Respondent 11 believes that countering FIMI best aligns with the NSDC's mandate (particularly due to its constitutional status), since the National Council of Television and Radio Broadcasting deals with registered media, the Central Election Commission is limited to electoral processes, while the CCD and the Center for Strategic Communications and Information Security focus on "debunking myths" and proactive cognitive operations.

24 Respondent 5 considers it the most capable, as it has a legislative framework, works with content, restricts access to Russian media, and maintains "blacklists of actors."

25 Respondent 8 noted that this commission could be entrusted with the responsibilities of an agency responsible for regulating the digital space and interacting with digital platforms.

26 Respondent 10 believes that the SSU should be the primary agency, as countering information security threats is its constitutional mandate. Respondents 11 and 12 noted that the SSU has the greatest capacity to counter FIMI.

27 Thanks to its counterintelligence activities, Respondent 5 considers the SBU to be the most capable law enforcement agency.

well as in the context of criminal investigations); National Police of Ukraine (in particular, the Cyberpolice Department, as well as in the context of criminal investigations); The Foreign Intelligence Service of Ukraine; the Main Intelligence Directorate of the Ministry of Defense of Ukraine; the Special Operations Forces;

- Involving relevant civil society organizations, research institutions, fact-checkers (including representatives of the International Fact-Checking Network), media outlets,[28] and business representatives who develop, implement, or use technologies (including AI) applied in conducting or countering FIMI operations in working groups and interagency cooperation.

**Improving legal regulation:**

- discussing the feasibility of enacting a special law to counter foreign interference (either in general or with a separate section on information interference) or introducing a set of amendments to other laws (the "Media Act," the "Information Act," the "Advertising Act," the "National Security of Ukraine Act," the "Sanctions Act," the "All-Ukrainian Referendum Act," the Electoral Code of Ukraine, etc.), which would include definitions of key terms (foreign interference, information manipulation, inauthentic behavior, disinformation,[29] political advertising, etc.), indicators of FIMI, the powers of authorities, and a set of countermeasures;[30]

28 Mentioned by respondent 4.

29 At the same time, Respondent 5 considers this impractical, since it is difficult to provide comprehensive definitions of these concepts, and there is a risk that they could be used against political opponents during a change in government. Respondent 6 also notes that a legislative definition of the term "disinformation" carries the risk of restricting freedom of speech.

30 Respondent 8 emphasized the need for clear definitions, as well as the lack of sufficient tools and legislative authority among government agencies, while Respondent 9 highlighted the need to clarify legislation and authority.

- discuss the advisability of regulating the activities of bloggers, as well as political consultants[31] or influencers, as media entities or individuals who have a significant influence on public opinion;[32]
- consider the feasibility and risks of introducing additional categories of offenses related to the conduct of FIMI operations[33] which pose a significant public danger (massive use of bots,[34] distribution of illegal campaigning materials and political advertising,[35] systematic and coordinated operations, etc.);
- adoption of a new comprehensive information security strategy[36] (the implementation of the current strategy was planned for the period up to 2025) involving all stakeholders, identifying current threats, clear objectives, and responsible entities (since the current strategy relies entirely on the Secretary of the National Security and Defense Council), as well as a corresponding program (defining indicators, timelines, and implementing entities);
- integration into the European Union's digital market, in particular the adoption of necessary legislation (such as the Digital Services Act,[37] the Regulation on Transparency and Targeting of Political Advertising, etc.), regulation of digital platforms, and the establishment of transparent rules for interacting with them.[38]

31 Mentioned by respondent 2.

32 Respondents 2, 7, and 8 supported the idea of granting bloggers a status analogous to that of the media.

33 Mentioned by respondent 10 and 13.

34 Mentioned by respondent 5.

35 Mentioned by respondent 7.

36 Respondent 12 noted the need for a strategic approach to counter FIMI.

37 Mentioned by respondent 5, 6, 10, and 11.

38 Supported by respondent 10.

**Introduction of countermeasures:**

- developing a methodology for identifying and assessing FIMI operations (for example, the aforementioned ABCDE methodology or the "subject, object, method, content, and impact" framework described in this report), in particular, trends and common characteristics (possibly even creating a separate database for this purpose), primarily regarding Russian information manipulation (discrediting European and Euro-Atlantic integration and those who support it, denying Russian aggression, federalizing Ukraine, using Russian propaganda terminology,[39] etc.);

- identifying the characteristics of annual reports (the agency's operational intensity over the course of the year; quantitative indicators of detected inauthentic phenomena; the breakdown of interventions by methods, platforms, and target audiences; the number of complaints submitted to platforms and the outcome for each type of complaint; the number of materials forwarded to law enforcement agencies and the results of their review; the number of cases in which the agency decided not to intervene and the grounds for such decisions, etc.) and technical reports on the results of specific operations (description of the operation, its time frame, channels, volumes, narratives; detection methodology; indicators of compromise, such as domains, accounts, hashes, and patterns in machine-readable format; the level of attribution, distinguishing between technical and legal attribution; what remains unidentified) by the responsible authority;

- the use of AI to review party platforms and statements by opinion leaders, and to identify FIMI operations (including disinformation and fake news),[40] analyzing the information environment, filtering information, and searching for comments on social media,[41] as well as pre-banking and de-banking in general (however, such use requires control mechanisms and adherence to ethical standards[42]);

39 Mentioned by respondent 2.

40 Mentioned by respondent 2.

41 Mentioned by respondent 3.

42 Mentioned by respondent 11.

- the application of a unified taxonomy (based on the DISARM framework, with possible improvements) and data format (e.g., STIX) for online collaboration among state agencies, governmental, and nongovernmental organizations;
- discussion of the feasibility and practicality of implementing blocking mechanisms (particularly through the imposition of sanctions), which can serve as a tool to counter[43] (as evidenced, in particular, by the experience of blocking "VKontakte," "Odnoklassniki," and other Russian platforms), however, these must be used in accordance with due process (the three-part test, the right to be heard, an independent body, clear criteria and grounds, etc.), and must also take into account collateral damage[44]), the balance with freedom of expression, and the technical complexity of implementation (for example, regarding Telegram);[45]
- Developing collaboration and broad engagement of civil society in monitoring and raising awareness about threats[46] .

**Regulation and oversight of financing:**

- Regulating the status of virtual assets[47] and platform-based quasi-payment systems (gifts on TikTok, Telegram bots with payments in Toncoin, donation platforms, etc.) as channels for indirect political financing and establishing guidelines for handling them (building blockchain analytics capabilities within law enforcement agencies before the start of the electoral process: purchasing licenses for analytical platforms; training staff; implementing clear blockchain analysis procedures in each agency; developing methodologies for conducting investigations, report templates, procedures for appointing expert examinations, resolving issues regarding the admissibility of data obtained from a commercial provider in a foreign jurisdiction, etc.);

43 Mentioned by respondent 7.

44 When the negative consequences of blocking outweigh the positive ones, such as outrage among some users due to restricted access to information (in particular, Telegram channels are currently being actively used to monitor the threat of Russian shelling).

45 Mentioned by respondent 5.

46 Mentioned by respondents 6, 9, 11, and 12.

47 Mentioned by respondent 7.

- improving political financing regulations (in particular, the adoption of draft laws No. 11462, No. 14289, and No. 8310, and the implementation of the Politdata system during the election process[48]);
- strengthening legal liability for foreign funding of political parties[49] and election campaigns;
- discussing the feasibility of strengthening financial monitoring of parties and candidates for foreign interference (in particular, monitoring offshore transaction chains, screening for "anomalous" activity, and the use of "dummy" parties);[50]
- comprehensive regulation of campaigning by third parties that are not candidates or parties but finance election campaigns: setting a spending threshold that takes financial support into account, labeling requirements, the creation of a public registry and reporting system, and the introduction of proportionate sanctions;
- discussion of the advisability of strengthening financial monitoring of influencers, particularly regarding sources of funding and tax compliance,[51] [52] with special attention to the use of cash[53] and virtual assets.[54]

**Establishing international cooperation:**

- researching legislative frameworks for countering foreign interference (in particular, FIMI) in countries such as the United Kingdom, Canada, and Australia (which have comprehensive regulations), as well as France, Romania,

48 Mentioned by respondent 7.

49 Mentioned by respondents 2, 7, and 9.

50 Mentioned by respondent 2.

51 Mentioned by respondent 3.

52 Respondent 6 emphasized that granting a media-like status to bloggers, and the regulation of their activities is a complex issue and may contradict the European standards of the freedom of speech, as well as the tracking of the related payments.

53 Mentioned by respondent 5.

54 Mentioned by respondent 7.

and Moldova (countries belonging to the Romano-Germanic legal family, to which Ukraine also belongs),[55] Taiwan (which faces similar threats from China),[56] and the Scandinavian and Baltic countries[57] (which have systematic experience with effective media literacy campaigns), while taking into account the uniqueness of the situation in Ukraine.[58]

- Establishing direct cooperation with transnational companies and platforms[59] to enable rapid countermeasures (situation centers, risk-based assessments) against FIMI operations,[60] and concluding direct memoranda or agreements with the National Council;[61]

- conducting consultations with the EEAS and competent authorities of foreign states regarding countering FIMI,[62] and initiating or participating in the creation of international countermeasures (e.g., the Convention on Disinformation[63]).

55 In particular, respondents 1 and 3 pointed out the advisability of taking into account the experience of Moldova, Romania, Canada, France, and Germany.

56 Mentioned by respondent 4.

57 Mentioned by respondents 6, 9, and 12.

58 Respondent 5 emphasized that none of the foreign experiences are suitable for Ukraine, since European regulatory frameworks are not always effective, and the "information resilience" models of the Nordic countries are often successful due to a language barrier that does not exist between Ukraine and Russia. Respondent 10 also emphasized that Ukraine actively provides data on Russia's information campaigns to its partners, rather than the other way around, and that it is precisely these partners (NATO, the EU, and the U.S.) who often lack the political will to take tougher action against FIMI, while Ukraine serves as a sort of "testing ground" for studying Russian tactics.

59 Mentioned by respondent 12.

60 Mentioned by Respondent 5.

61 Mentioned by respondent 7.

62 Mentioned by respondent 12.

63 Mentioned by respondent 5.

**Strengthening resilience:**

- regular educational activities[64] (films, TV series, short videos, and game formats[65]);
- education (incorporating into educational programs[66] from early childhood[67]) on digital hygiene, the basics of fact-checking, and critical thinking in the information space;
- launching the pre-banking platform,[68] which will enable proactive measures against foreign information manipulation — a particularly pressing issue ahead of elections (for example, Google's pre-banking campaign against pre-election disinformation in Indonesia reached 57.6 million unique users).

64 Mentioned by respondent 1.

65 Mentioned by respondent 4.

66 Mentioned by respondent 12.

67 Mentioned by respondent 10.

68 Respondent 10 supported efforts to improve media literacy and pre-banking (informing the public about the preparation of information operations).

This report was drafted within the project "Inclusive Dialogues For Democratic Reform in Ukraine" funded by the Ministry of Foreign Affairs and Trade of Ireland but the opinions expressed herein do not necessarily reflect the official position of the Irish Government.

# ANNEX

## MODEL (BODY)

### 1. Specialized body for combatting foreign digital interference

MODELS: VIGINUM *(France)*

Myndigheten för psykologiskt försvar *(Sweden)*

ADVANTAGES:

- **Specialization.** The only center with expertise in the methodology of detecting, technically attributing, and accumulating data on the tactics, techniques and procedures (according to EEAS) of threat agents.
- **Narrow mandate.** A mandate limited to foreign interference, with clear eligibility criteria, reduces the risk of using the body against domestic political opponents.
- **Analysis is separated from coercion.** The body shall document operations and transfer the data to platforms, regulators, and law-enforcement bodies, while the content will not be blocked, however the body may respond to it in the information field. Under these terms, it is easier to comply with Art. 10 of the Convention.
- **External ethical oversight.** An independent committee may produce annual reports on compliance with the law and standards of ethics.
- **Single source of information.** It is convenient for the interaction with international organizations (such as the EEAS) and digital platforms.

DISADVANTAGES:

- **Time and other resources.** Qualified staff needs to be recruited; the body shall be equipped with analytical tools and access to data platforms.
- **The risk of overlapping.** There may be an overlap of responsibilities with the CCD, CSC, Security Service of Ukraine, and the State Special Communications Service, and the competition over the mandate and donor funding.
- **Uncertainty in the case of regulation by a by-law.** If a status and the scope of powers are established by a by-law, they can be easily modified. Therefore, the status of a specialized body shall be defined by the law.
- **Dependance and discommunication.** Without its own authority, the body's response will depend on the willingness of other agencies to act, and communication between different institutions may be hampered by bureaucracy, lack of time, or unwillingness.

- **The blurred line between the "foreign" and other.** The boundary is blurred when foreign narratives are reinforced by domestic actors. However, this disadvantage may be mitigated by regulating the foreign markers for information campaigns.

## 2. Interagency coordination body, peer body of heads of dedicated authorities

SIMILAR CASES:

National Coordination Center for Cybersecurity at the NSDC

Interagency working group at the CMU suggested by the CEC

Counter Foreign Interference Coordinator *(Австралія)*

ADVANTAGES:

- **Requires less resources.** Does not require any new bureaucracy or significant costs. Shall be established by the law, through the decision of the NSDC or the CMU regulation.
- **Combination of tools and expertise.** Analytics, counterintelligence, regulators, cybersecurity, and financial monitoring all operate within a single framework. FIMI are often combined with financial interference and cyberattacks, thus requiring a set of various instruments.
- **Shared rules for interaction.** Protocols for information exchange may be introduced, as well as the unified taxonomy, contact points, and the shared incident log.
- **Collegiality.** Collegiality reduces the risk of unilateral decisions and the dominance of a single agency in the evaluation of information campaigns.
- **Scalability.** For the election period, the body can be easily reinforced with the situation awareness center and additional representatives.

DISADVANTAGES:

- **Irregularity.** Meetings of such a body are held periodically, while FIMI operations unfold within a matter of hours. Without a permanent secretariate, the response will be significantly delayed.
- **There is no own analytical staff.** The body relies on data provided by its participants, therefore, the quality of its work will depend on the performance of each participant and their coordination.
- **Solutions as recommendations.** Decisions of NCCC "shall be mandatory to consider" by authorities, rather than to enforce — no one shall be personally liable for the missed operation and lack of response.
- **Less openness.** If law-enforcement and security bodies prevail among members the focus will shift to higher secrecy, whereas public accountability may be restricted.
- **No clear regulation.** Interagency bodies are usually less formalized, which may offer certain flexibility but leaves much uncertainty during the work.

- **Risk of political influence.** Although no model can avoid it, the Moldova case shows how in 2025 the StratCom Center council transformed into an advisory body, while the Center passed to the control of the President and the Parliament.

### 3. Assigning the function to the Disinformation Combatting Center at the NSDC

Expanding the mandate of the existing body instead of creating a new institution

ADVANTAGES:

- **Readiness.** The body has functioned since 2021: it has a fixed number of staff (52 staff positions), premises, central budget funding, round the clock monitoring, and the established analytical processes. The creation of a new service before elections would require time to recruit the staff and build the capacity.
- **Minimal change.** This model does not require new solutions but only some changes and scaling. This is the fastest possible option since it only needs to amend the Regulations by the Presidential decree.
- **Data Collection and Methodology.** Every year, the CCD processes a large number of incidents and produces analytical reports, while monitoring Russian narratives and the channels through which they are disseminated. FIMI's analysis would be based on this existing database rather than starting from scratch.
- **Well-established international cooperation.** CCD has an established partnership with the EEAS (joint report 2026), NATO, government agencies of partner countries and platforms.
- **Preparing the conditions for imposing sanctions.** CCD analytics could serve as the basis for Ukraine's only rapid-response tool — sanctions imposed by the Defense Council. In addition, the CEC has already signed a memorandum of cooperation with the National Council and the CCD.

DISADVANTAGES:

- **Status under a by-law.** The CCD status is defined by the Regulation approved by the Presidential Decree which may be amended or repealed at any time (unlike in Moldova, where the corresponding center was established by a separate law).
- **Mandate.** The scope of its activities covers disinformation in general, without a mandatory criterion of foreign origin, and current legislation contains no definitions of either disinformation or FIMI. Furthermore, the CCD does not issue decisions that can be appealed; instead, its tools consist of public labeling and appeals to platforms.

- **Lack of independent and parliamentary oversight.** The CCD reports to the National Security and Defense Council, and its head is appointed by the President. This means there is neither an independent ethics committee (as is the case with the Secretary General for Defense and National Security in France), nor mandatory public accountability, nor parliamentary oversight.
- **Political and Personnel Dependence.** Over the past five years, the CCD has had four directors, two of whom — including the current one — served in an acting capacity. Furthermore, the controversial use of the NSDC's sanctions mechanism against Ukrainian citizens, coupled with the expansion of its mandate to cover not only foreign but also domestic information manipulation, could undermine public trust. This could be critical for effectively countering FIMI, since in the French model, the involvement of a foreign actor is a mandatory criterion that keeps the agency out of domestic political discourse.

---

An analysis of the strengths and weaknesses of the models described above shows that none of them, on its own, strikes the right balance between specialization, responsiveness, accountability, and institutional coordination. The most acceptable approach appears to be a combination of two elements: a **permanent body** that will operate both during and between election cycles, as well as **a mechanism for interagency coordination** that will begin its work well in advance of the election process and conclude several months after it ends. To ensure the stability and legitimacy of the chosen model, the status and mandate of the permanent body, the criteria for identifying information operations of a foreign nature, the procedure for establishing and the duration of the interagency group's work, as well as mechanisms for independent oversight and public accountability, should be defined by law.

## ADVANTAGES OF COMBINING THE MODELS:

→ Continuity of monitoring. Since information operations are prepared well in advance of elections (networks of accounts are created, audiences are built, and channels for disseminating narratives are established), a permanent body will be able to detect them at an early stage, collect data on tactics, techniques, and procedures, and ensure attribution, thereby establishing an analytical foundation for further interagency cooperation.

- Strengthening coordination during periods of highest risk. An interagency framework during the election period will combine the permanent body's analytics with the tools of the Central Election Commission, regulators, cybersecurity agencies, counterintelligence, and financial monitoring agencies, allowing resources to be concentrated when the threat is greatest, without creating additional permanent bureaucracy.

- Compensating for the shortcomings of the models. The permanent body's own analytical apparatus will eliminate the main shortcomings of the interagency format — irregularity and dependence on participants — while the interagency format, with clear protocols for information exchange, will ensure a response that a body without enforcement powers would lack, thereby reducing the risk of miscommunication between institutions.

- Coverage of the post-election period. Continuing interagency cooperation after Election Day will make it possible to counter campaigns aimed at undermining confidence in the certification of results, the resolution of election disputes, and the formation of government bodies — at a stage when foreign interference often does not subside but merely changes form. Furthermore, the operation of an interagency framework during the post-election period will ensure the transfer of documented materials to law enforcement agencies, the preservation of the evidence base, and support for investigations, thereby promoting the inevitability of punishment.

- Human rights guarantees. Separating analysis (a permanent body) from decisions on how to respond (a collegial interagency framework) will reduce the risk of a single agency monopolizing the assessment of information campaigns, which will facilitate compliance with requirements regarding freedom of information dissemination, while the temporary nature of the enhanced format will simultaneously limit the risk of exceptional practices spilling over into ongoing inter-election political activities, particularly those of opposition parties.

- Institutional memory. Concluding interagency cooperation with a joint report on the election results will make it possible to assess the effectiveness of the response, update the taxonomy, protocols, and the incident registry, thereby ensuring institutional continuity and a cumulative approach to countering FIMI, in which preparation for future election cycles will be based on the systematized experience of previous cycles.