PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NO. 3 (216), JUNE 2024 © PISM

Editors: Sławomir Dębski, Wojciech Lorenz

EU Adopts Approach to Countering Foreign Information Manipulation and Interference

Filip Bryjka

Responding effectively to foreign information manipulation and interference (FIMI) is one of the EU's priorities for countering hybrid threats. Since the adoption of the Strategic Compass in March 2022, the Member States and EU institutions have succeeded in establishing a common framework for defining, detecting, and analysing FIMI incidents to facilitate information-sharing. The challenge remains to establish a system for a coordinated response at the EU level. More proactive action within the FIMI Toolbox, more effective sanctions enforcement, and operationalisation of the response system will be key to countering the systemic threat from Russia, as well as from other states and non-state actors.

Since Russia's annexation of Crimea in 2014, EU states have been subjected to intensified Russian information operations aimed at influencing political processes and decisions, deepening social divisions, and disrupting debate shielded by the right to freedom of expression. To counter FIMI, EU states are creating appropriate structures in public administration, engaging civil society and cooperating with online platforms and the media. In doing so, they must constantly adapt to the changing tactics, techniques, and procedures (TTPs) used by threat actors. FIMI operations are characterised by increasing levels of automation due to technological advances. Using bot farms—computer programs that mimic human online activities—attackers spread manipulated content on a massive scale and increase the reach of malicious activity. A common method is to impersonate politicians or institutions by cloning their websites and official social media accounts. FIMI operations are carried out with the help of sophisticated infrastructure and cloaking software, making it difficult to detect the attacker and attribute responsibility. The use of artificial intelligence (AI) is playing a growing role in these operations, which in the future will not only be used to create manipulated content but also to plan entire campaigns (including determining narratives and target groups). New technologies give an advantage to the attacker, as they enable the distribution of manipulated content on a massive scale using inauthentic methods (bots). Currently, the attacker suffers almost no consequences for unethical actions.

FIMI operations are characterised by increasing levels of automation due to technological advances.

FIMI as a New Conceptual Framework in the EU

The category of "foreign information manipulation and interference" was introduced into the official language of the EU in March 2022. It is a broader concept than disinformation, which is understood as false or misleading content that is disseminated with the intent to deceive or provide economic or political gain and that can cause public harm. FIMI, in turn, describes a pattern of behaviour that is mostly not illegal, but threatens or has the potential to negatively affect democratic values and political processes. Such activities are manipulative, carried out in a deliberate and coordinated manner by state or non-state actors, including their proxies inside and outside their own territory. The conceptual framework of FIMI is therefore not limited to fake news, propaganda, or disinformation, but focuses on interference in the political processes of states subjected to hostile information influence. They cover this problem more broadly by taking into account the evolving TTPs used by Russia, China, and Belarus, among others, including in the cyber domain (e.g., attacks on voter registries, deep fakes, or hack-and-leak operations involving the stealing of confidential information or correspondence and publishing it).

FIMI describes a pattern of behaviour that is mostly not illegal, but threatens or has the potential to negatively affect democratic values and political processes.

EU Member States use different criteria to qualify information incidents as FIMI. Considered one of the leaders in resilience, the Swedes consider it to: 1) have a foreign origin; 2) contain content that misleads the recipient; 3) have the intent to inflict harm; and 4) carry potential security risks. The French agency VIGINUM considers similar criteria for digital interference: 1) involvement of foreign actors; 2) inauthenticity of behaviour; 3) misleading content; and 4) specific target.

Challenges in Developing the EU's FIMI Response System

Like in cases of other hybrid threats, responsibility for countering FIMI is the responsibility of the Member States. However, the effectiveness of these activities depends on the cooperation of various countries and organisations. Institutions responsible for countering FIMI in EU countries are located in different government structures (e.g., foreign affairs, interior, defence ministries) by which they have

different mandates, organisation, and scope of tasks. They also use different methodologies for analysing FIMI incidents, which makes it difficult to share information.

The EU aims to standardise the detection and response to FIMI based on the DISARM-STIX method.

Since the adoption of the Strategic Compass in March 2022. The EU aims to standardise the detection and response to FIMI based on the DISARM-STIX method, used, among others, by the Data Analysis Team in the Strategic Communications, Task Forces and Information Analysis Division (SG.STRAT.2) of the European External Action Service (EEAS). This method allows, among other things, the analysis of tactics, techniques and procedures used, as well as information on the infrastructure used to carry out influence operations (e.g., domains, servers, inauthentic accounts, etc.) to be entered into a common database.

Among other things, the EU's conceptual work to date has made it possible to define a common definitional framework and methodological standards, which, although not mandatory for EU countries, are considered best practice. It is up to individual Member States to decide their implementation. Further standardisation of the working methods of analysts in the institutions of EU countries, as well as NGOs involved in combating FIMI, would greatly expand the situational awareness of the Member States and improve the exchange of information within the framework of the EU Rapid Alert System (RAS) and the Information Sharing and Analysis Centre (ISAC).

Standardisation of FIMI analysis methods would also facilitate attribution of attribution to the attacker. This, in turn, should improve decision-making at the political level regarding joint (coordinated) responses. The ability to attribute responsibility for an attack is also an essential element in deterring such actions, as it comes with various costs to the aggressor, such as image, political, and even financial if sanctions are imposed.

Standardisation of FIMI analysis methods would also facilitate attribution of attribution to the attacker. This, in turn, should improve decision-making at the political level regarding joint responses.

The European External Action Service (EEAS) has proposed four ways to respond to FIMI incidents depending on their harmfulness: 1) *ignore* – sometimes it's better to ignore an incident than to react to it, which can lead to publicised manipulation and be counter-productive; 2) *contain* – inform online platforms when an inauthentic network or harmful content is detected; 3) *minimise* – remove inauthentic accounts and the content they distribute; 4) *redirect* – redirect the recipient's attention to reliable information with a message at the appropriate level.

So far, the EU's responses to FIMI have focused on conducting active strategic communications, debunking, "naming and shaming", and strengthening societal resilience through education and cooperation with the non-governmental sector. While these activities are important and should be developed, they are not sufficient to effectively combat FIMI attacks, which are being used on a massive scale due to the development of new technologies. The EU imposes almost no costs on those using FIMI against Member States for their harmful effects. An example of this is the ability to view Russian websites (e.g., RT, or Sputnik) on EU territory, despite EU sanctions on these media imposed in March 2022. After Russia's full-scale invasion of Ukraine, some countries (e.g., Czechia and Poland) briefly (for about 3-6 months) maintained blocks on websites spreading pro-Russian propaganda and disinformation, but national courts found insufficient legal grounds for such measures. In contrast, such measures were effectively taken by the Estonian authorities, where 53 TV channels and some 300 websites were blocked on the basis of a law prohibiting the promotion of an offensive war.

The EU imposes almost no costs on those using FIMI against Member States for their harmful effects.

The ineffectiveness of the EU's response system to FIMI is the result of varying degrees of progress by individual EU countries in countering FIMI, different regulations at the national level, a lack of political will to be more proactive, restrictions related to the protection of freedom of expression, or the provisions of the GDPR.

The ineffectiveness of the EU's response system to FIMI is the result of varying degrees of progress by individual EU countries in countering FIMI, different regulations at the national level, a lack of political will to be more proactive, restrictions related to the protection of freedom of expression, or the provisions of the GDPR. The implementation this year of the Digital Service Act (DSA), which is expected to increase the ability of states to influence online platforms to combat and remove illegal content, is expected to help change this.

Conclusions and Recommendations

To increase the effectiveness of countering FIMI, EU countries should develop national capabilities to defend against and deter informational aggressors by increasing the cost of their operations. Implementation of EU standards by the Member States will improve information-sharing and facilitate joint responses to FIMI in the form of removing inauthentic account networks by online platforms, blocking domains and servers used for FIMI operations, or imposing and enforcing sanctions on individuals and entities involved. It is also important to disclose information about the infrastructure used, which makes it difficult to reuse it and requires significant resources to create new channels of influence.

Poland should have a specialised institution for detecting, analysing, and responding to FIMI in accordance with EEAS standards.

Poland should have a specialised institution for detecting, analysing, and responding to FIMI in accordance with EEAS standards. Given the foreign origins of FIMI incidents, such a structure could be created in the Ministry of Foreign Affairs and report to the Foreign Minister's Plenipotentiary for Countering International Disinformation, appointed in May this year). In order to properly carry out its task, such an institution must have a budget and trained human resources to continuously monitor the information space. The mandate of such an institution should allow it to coordinate the activities of other entities involved in countering FIMI (e.g. the NASK Institute, intelligence and counterintelligence services), as well as relevant units in other ministries (especially the Government Security Centre, the Ministry of Defence, the Ministry of Internal Affairs and Administration, and the Ministry of Digitisation). The same standards for detection and analysis of FIMI incidents should be in place in these institutions, which will enable the efficient exchange of information and ability to operationalise it at the state and EU levels.

Ultimately, Poland should develop a comprehensive system for countering FIMI based on a whole-society approach, which will increase the role of non-governmental organisations (NGOs), especially fact-checking organisations and those debunking disinformation, civic society initiatives, and the private sector (especially digital service providers) by creating a body for systematic consultation and information exchange with state structures. This would greatly relieve the burden on state structures and more broadly counter the FIMI problem, which is widespread due to the development of new technologies. To maintain continuity, the state could consider co-funding the activities of NGOs through grants. In doing so, it will be crucial to define objective criteria for the selection of partners and how to determine the scope of their tasks (sectors of responsibility), which they would carry out as part of this cooperation. This is because cooperation with the state administration should not limit their autonomy of action in other spheres

Ultimately, Poland should develop a comprehensive system for countering FIMI based on a whole-society approach.

of their functioning. However, it will be crucial for the effectiveness of the system that partner organisations are trained in accordance with EEAS standards.

One of the priorities of the Polish presidency of the EU may also be to initiate a debate on more proactive measures against states and non-state actors using FIMI.

One of the priorities of the Polish presidency of the EU may also be to initiate a debate on more proactive measures against states and non-state actors using FIMI. An appropriate response system in the form of effective sanctions and domain-blocking could be developed within the Cyber Toolbox or FIMI Toolbox. Some of the work in protecting against FIMI should be redirected to platforms that profit financially from sponsored disinformation. During its EU presidency, Poland may also propose that as part of the implementation of the Digital Services Act, platforms should be required to have specialised structures to detect and respond to FIMI incidents.