

FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity

October 2023

EXECUTIVE SUMMARY

There is now a robust body of evidence displaying how foreign information manipulation and interference (FIMI), including disinformation, feeds on vulnerabilities and hot-button issues. It twists them to sow divisions and distrust, and to polarise our societies. One of the groups considerably targeted with FIMI is the LGBTIQ+ community.

In recent years, significant progress has been made in understanding and responding to FIMI. Nevertheless, analysis concerning specifically the LGBTIQ+ community has been scarce. This report – the first one of its kind – aims to start filling this void.

The report **is the first such document focused on the topic of FIMI targeting solely LGBTIQ+ persons, and it includes specific FIMI cases.** The aim is to help the defender community understand the nature of FIMI as well as the Tactics, Techniques and Procedures (TTP) used to target the LGBTIQ+ community. With this knowledge comes increased ability to act against FIMI – both for the LGBTIQ+ community itself and for other groups, who can learn from the repetitiveness of FIMI tactics.

FIMI targeting the LGBTIQ+ community – what have we learned?

This report first builds on the methodology to identify, characterise and, where possible, attribute cases of FIMI targeting the LGBTIQ+ communities in the EU's Eastern Partnership countries, the Western Balkans and the Southern neighbourhood. It then uses the analysis of the case studies, interviews with key stakeholders and the findings of a workshop organised by the EEAS in August 2023, attended by representatives from NGOs, academia, government and industry to propose actions to address FIMI targeting LGBTIQ+ communities.

Of 31 LGBTIQ+ FIMI cases identified between June 2022 and July 2023, almost 80% used narratives implicating Western governments, the Ukrainian government, civil society organisations, the European Union, international organisations, or sports organisations to demean or

insult LGBTIQ+ communities. Over half of the identified cases were attributed to Russia. The remaining 45% of cases used channels not previously attributed.

The reach of FIMI cases targeting LGBTIQ+ goes beyond this community. According to the evidence collected during the investigation, FIMI actors aimed to provoke public outrage not only against named LGBTIQ+ individuals, communities, or organisations - but also against government policies, the concept of democracy as such, and local or geopolitical events. While undermining LGBTIQ+ people was a common theme in many of the FIMI cases identified, the overarching narrative in many of them was that the West is in decline. By leveraging the narrative of decline, **FIMI threat actors attempt to drive a wedge between traditional values and democracies.** They claim that children need to be protected from LGBTIQ+ people, that LGBTIQ+ people get preferential treatment in sports and other fields - to the detriment of others - and that Western liberal organisations or political groups are demonstrably weak because they surrender to "LGBTIQ+ propaganda".

The report is an important step in highlighting how FIMI threat actors use a wide combination of Tactics, Techniques and Procedures (TTPs) to plan and execute attacks. The cases showed the frequent use of such TTPs as impersonation, fabrication and alteration of documents, and the appropriation and re-use of existing multimedia content. However, a wide variety of additional TTPs was identified, which shows the ability of FIMI actors to adapt their tactics over time.

Research findings suggest that the **main gaps in tracking, preventing and combating FIMI targeting LGBTIQ+ are related to the lack of coordination, cooperation and communication between different stakeholders** such as government, academia, non-government organisations, social media platforms and the media. Insufficient use of existing networks and few opportunities to bring experts together mean that initiatives often operate in isolation from other efforts, and suffer from a lack of funding.

Recommendations

The report includes **a comprehensive section with recommendations, highlighting what specific stakeholders can and should do to address the threat of FIMI**. Recommendations were developed in close cooperation between the EEAS, civil society organisations and representatives of academia.

The general recommendation is for all stakeholders to work more closely together. Recommendations call for governments, academia, industry, civil society and local communities **to share information about new and emerging threats, facilitate a more collaborative response, and identify ways in which stakeholders can support and inform the work of others**.

Ultimately, the success of the defender community will depend on its ability to support local initiatives, while coordinating at national and international levels.

Stakeholders will need to overcome traditional barriers to find ways to cooperate with new partners and build trust. The EEAS has already begun this process, and the recommendations in this report are informed by the EEAS outreach to the defender community in the European Union, its neighbouring regions and beyond.

The recommendations also point to the role of platforms in disrupting the spread of FIMI. For this to be effective, stakeholders will need to reflect on new ways of working together, for example by **agreeing to cooperate rather than compete**, or by investing in potentially expensive product features that improve information gathering and moderation efforts, but do not necessarily generate revenue. Any regulation of social media platforms must also find ways to balance the need to ensure that platforms do not host or promote illegal or harmful content with the expectation of political neutrality in content moderation decisions.

This study has been produced under the EEAS Stratcom project on FIMI activities targeting LGBTIQ+ communities. The content of the report has been produced by the EEAS Stratcom Division in collaboration with Rodrigo Cruz (researcher at the Université Libre de Bruxelles) and Alliance4Europe.

The empirical data analysed is based on the strategic monitoring efforts of the EEAS STRAT.2. It represents a limited time-period and reflects patterns seen in known outlets related to overt Foreign Information Manipulation and Interference (FIMI) or attributed operations to foreign actors. The evidence presented in this report serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity.

TABLE OF CONTENTS

Executive summary	2
Introduction	5
Scope and methodology	7
FIMI and LGBTIQ+ terminology	8
Terms and definitions	8
What do we mean by FIMI targeting the LGBTIQ+ community?	9
FIMI targeting LGBTIQ+ and the international political context	11
Implications for values and democratic processes	11
Vulnerabilities and potential impacts	12
Assessing FIMI cases targeting LGBTIQ+ communities	13
Understanding patterns of manipulation and FIMI Tactics, Techniques and Procedures (TTPs) targeting LGBTIQ+ communities	14
Responding to real-world events and crises	20
Segmentation of target audiences with localisation of FIMI content and narratives	21
Strategic use of meta-narratives in relation to LGBTIQ+ community	23
Selection of channels and platforms to deliver content	24
Gaps and obstacles to better understanding the threat and activating responses	25
Recommendations for responding to and countering FIMI targeting LGBTIQ+	27
Responding to FIMI targeting LGBTIQ+	28
1. Situational awareness	29
2. Resilience building	30
3. Disruption and regulation	32
4. The role of EU external action	34
Conclusions	35
Appendices	36
References	37

INTRODUCTION

Foreign actors have been using information manipulation and interference (FIMI), including disinformation, to polarise the public sphere, and to sow discord in democracies. Disinformation using identity-based stereotypes is a threat to democracy that targets and undermines vulnerable communities. **LGBTIQ+ communities, who are subject to identity-based attacks, have been repeatedly targeted by disinformation campaigns.**

The body of research and records of FIMI cases targeting LGBTIQ+ communities show that they are increasing in frequency. A report by the EU-funded European Digital Media Observatory (EDMO) in May 2023 found that unsubstantiated claims against LGBTIQ+ communities “often incite hatred against minorities, laws and institutions” and warned that LGBTIQ+ disinformation “is becoming more and more insidious”.¹

Potential and real consequences of FIMI targeting LGBTIQ+ communities include **hardening public opinion** in support of existing discriminatory legislation, **fuelling the potential further erosion of hard-won rights of LGBTQ+ people** as well as posing perceived and **real risks to personal safety** and personal relationships at home, work or elsewhere. FIMI targeting LGBTIQ+ is often politically motivated, and it seeks to undermine LGBTIQ+ rights, well-being, dignity, physical and emotional integrity, political mobilisation and freedom of expression.

In analytical terms, the impact of FIMI activities is complex to measure, both for societal costs and for the effects on individual members of the LGBTQ+ communities. **Specific research on information manipulation targeting LGBTIQ+ communities is still limited compared to evidence on attacks against other vulnerable groups.** This report aims to widen the evidence-based knowledge collected in this field and to contribute to the activation of specific responses to mitigate and counter the threat of FIMI. This report is divided into five building blocks.

The first block proposes a specific terminology to define FIMI targeting LGBTIQ+ communities. This term, aligned with the elements of the FIMI definition, combines the narrative level with the identification of behavioural patterns that indicate manipulation, coordination and intent to mislead.

The second section discusses some of the implications of FIMI targeting LGBTIQ+ for values and democratic processes.

The results of the analysis of 31 documented FIMI cases attacking LGBTIQ+ communities are set out in the third part of the report. Specific cases show how threat actors use a wide combination of Tactics, Techniques and Procedures (TTPs) to plan and execute attacks on the LGBTIQ+ community, such as impersonation, fabrication and alteration of documents, appropriation and re-use of existing multimedia content and distortion of facts around certain events and real-world crises. This diversity is problematic because **FIMI threat actors exhibit adaptive and evolutionary characteristics**, continually refining and innovating their TTPs to identify weaknesses and defeat FIMI defences, with the added benefit of keeping FIMI threat actors’ strategies elusive and effective over time. **The use of different TTPs may allow FIMI threat actors to escape from detection mechanisms and countermeasures** while continuing to reinforce FIMI narratives targeting communities such as LGBTIQ+.

The fourth and fifth segments of the report identify current challenges, in order to counter the threat, and connect the analytical level to actionable responses, based on the framework of the FIMI toolbox. The European External Action Service has worked with a cross section of academia, civil society, the private sector, EU Member States and international partners to develop a framework for responses to FIMI, the FIMI Toolbox². The framework divides the areas of responses into four categories: situational awareness, resilience building, disruption and regulation, and external action.

Research findings suggest that one of the challenges in addressing this threat is the **major gaps in tracking, preventing and combating FIMI that targets LGBTIQ+.** **These relate to the lack of coordination, cooperation and communication among different stakeholders**, such as the international organisations, government, academia, non-government organisations, social media platforms and the media. Poor use of existing networks and few opportunities to bring experts together mean that initiatives often operate in isolation from other efforts, lead to duplication of initiatives or suffer from a lack of funding.

The overarching theme in the detailed recommendations is the **need for greater cooperation between and among stakeholders.** The recommendations call for the international organisations, governments, academia,

industry, civil society and local communities to develop communication networks **to share information about new and emerging threats, facilitate a more collaborative response, or identify ways in which stakeholders can support and inform the work of others.**

Ultimately, the success of the defender community will depend on its ability to support local initiatives while coordinating at national and international levels. **Stakeholders will need to overcome traditional barriers to find ways to cooperate with new partners and build trust.** The EEAS has already begun this process, and the

recommendations in this report are informed by EEAS outreach to the defender community in the European Union, its neighbouring regions and beyond. The EEAS workshop held in Brussels in August 2023 was an important step in bringing together representatives from platforms, government, civil society and academia to discuss the challenges they face and their suggestions on how to develop a way forward together. The event was the first opportunity for many participants to hear directly from civil society actors about their different experiences and perspectives and began the ongoing process of breaking down traditional barriers between stakeholders.

SCOPE AND METHODOLOGY

The report uses a triangulation of four data sources. For the definition of the terminology presented in this report, researchers at the Université libre de Bruxelles (ULB) carried out desk research in order to describe the state of the art and to connect the proposed term to existing academic work and the FIMI terminology.

Using the FIMI definition, the collection of cases refers to incidents of proven information manipulation, according to the analysis of TTPs, in which actors outside the EU were involved. The analysis of FIMI cases with elements of LGBTIQ+ disinformation was recorded between June 2022 and July 2023. During the reported period, the European External Action Service's (EEAS) Stratcom division collected, analysed and documented 31 incidents. Details of the analytical methodology that was used can be found in the EEAS' 1st Report on Foreign Information Manipulation and Interference Threats³. The type of standardised methodology applied in this report relies on the systematic use of standardised analytical frameworks, taxonomies and standards to describe FIMI threats, such as the ABCDE framework, DISARM Red Framework and the Structured Threat Information Expression Language (STIX)^{4,5,6}. The use of this standardised methodology provides evidence-based analysis. As such, this methodology is a key element in supporting the application of better-informed responses.

The preliminary results of the desk research and case analysis were presented in an expert group discussion held in Brussels (Belgium) in August 2023. The event brought together 50 stakeholders from different environments to

understand the gaps and discuss measures to respond to and counter FIMI targeting LGBTIQ+ people. The results of the discussions were submitted to an analysis grid containing the following variables: gaps, issues to be addressed and a list of priorities. A second type of information, covering recommendations, was subjected to a second analysis grid based on the four scopes of the FIMI Toolbox: situational awareness, building resilience, disruption and regulation, and the role of EU External Action.

Moreover, in September 2023, researchers from the ULB conducted nine interviews with experts in the areas of disinformation, gender and LGBTIQ+ rights (representing international organisations, academia and civil society organisations). The interviews were conducted with informed consent and in accordance with the standards established by the EU General Data Protection Regulation (GDPR). The interview guide was divided into three sections, each covering the following topics: *General aspects and reasons behind FIMI targeting LGBTIQ+ community; Actors, narratives and tactics; Impacts, good practices and policy recommendations*. The guide was constantly adapted according to the profile and expertise of each interviewee to ensure more efficient data production.

Information extracted from the expert discussion and the interviews was then condensed and broken down by stakeholder group to reinforce the holistic, "whole-of-a-society" approach suggested by the FIMI Toolbox and the research findings. The case analysis enabled the identification of gaps, key issues to be addressed and types of priority recommendation.

FIMI AND LGBTIQ+ TERMINOLOGY

This section seeks to delve into a largely untheorised topic: the proliferation of foreign information manipulation and interference targeting the LGBTIQ+ community. It begins with a discussion of terminology, including the concept of FIMI targeting LGBTIQ+ proposed by the EEAS.

TERMS AND DEFINITIONS

This first subsection provides clarification on some of the key terms used in this field of study. The aim is to establish a clear distinction between FIMI and other harmful behaviours such as hate speech, harassment, hate crimes, disinformation, and gendered disinformation in order to provide a clear concept of LGBTIQ+ foreign information manipulation and interference (FIMI). By establishing clear concepts, it is possible not only to understand the threat posed by FIMI targeting the LGBTIQ+ community, but also to assess its impact and develop effective actionable responses.

In public debate, information manipulation tends to be easily conflated with other harmful behaviours such as hate crime, hate speech and harassment (Wardle & Derakhshan, 2017; Bayer et al., 2019). Thus, although the analysis of empirical cases is complex enough to challenge some rigid definitions that may require the combination of different concepts, the main difference between these behaviours lies in their illegal and non-illegal status. While hate speech, hate crime and harassment are often considered illegal (at least in EU Member States), the same cannot be said for disinformation, misinformation, malinformation, gendered disinformation and FIMI. The latter, while harmful, are not considered criminal behaviour.

Illegal and harmful behaviours

Hateful, threatening and violent behaviour: Such behaviours as hate speech, hate crimes and harassment are also often confused with misleading information because of their potential to cause individuals to engage in violent, intimidating or illegal behaviour. Due to their illegal nature, official legal definitions can be useful to explain the differences between them and make clear how they differ from other types of threat related to information manipulation. Here are those conceptual definitions:

- **Hate speech:** Hate speech can be defined as “all types of expression that incite, promote, spread, or justify violence, hatred or discrimination against a person or group of persons, or that denigrates them, by reason of their real or attributed personal characteristics or status such as ‘race’, colour, language, religion, nationality, national or ethnic origin, age, disability, sex, gender identity and sexual orientation”.⁷
- **Hate crime:** Hate crime can be defined as “criminal offences committed with a bias motive” (OSCE/ODIHR, 2009). It includes a wider range of criminal offences, such as property vandalism, arson, physical assault, and murder and always comprises two essential elements. The first component concerns an act that can be qualified as a criminal offence under general criminal law. The second aspect of a hate crime is the perpetration of a criminal act driven by a specific motive or “bias”. This means that the perpetrator deliberately selects the victim on the basis of certain protected characteristics such as “race”, language, religion,

Illegal and harmful

Hate speech
Hate crime
Harassment

Not illegal, but harmful

Misinformation
Malinformation
Disinformation
Gendered disinformation
FIMI

Figure 1: Illegal and non-illegal behaviours

ethnicity, nationality, sexual orientation, gender, gender identity, disability or any other similar common factor (OSCE/ODIHR, 2009).

- **Harassment:** Harassment is usually characterised by an unwanted one-off incident or persistent behaviour that can take various forms (physical, psychological, verbal and/or sexual, online). It is intended to annoy, threaten, intimidate, or cause distress to an individual or a group, often motivated by emotional reasons, personal dislike, or prejudice based on gender, race/ethnic origin, religion or belief, disability, age, sexual orientation or body image, which may result in a hostile or intimidating environment.

Non-illegal but harmful behaviours

In order to address FIMI, the EEAS has proposed to focus on non-illegal but harmful behaviour. However, as FIMI is not the only type of manipulated information, it is important to establish clear differences between existing concepts. Here are some of the main concepts used.

Disinformation: Disinformation consists of “*intentional falsehoods spread as news stories or simulated documentary formats to advance political goals*” (Bennett and Livingston, 2018, p.124). This concept has been used as an alternative to the term “fake news”, which is widely used in the media. While “fake news” tends to portray the issue as sporadic instances of falsehood and confusion, the term “disinformation” would have the advantage of highlighting the more systematic dissemination of misleading information.

Misinformation: Misinformation refers to misleading information created or shared without manipulative or malicious intent (Fallis, 2014), although it can still have harmful effects. It is the strategic nature of disinformation that distinguishes it from misinformation. For example, in the early months of the COVID-19 pandemic, many people shared misinformation due to fear or lack of accurate official information (Lovari, 2020), but often without malicious intent.

Malinformation refers to the deliberate sharing of genuine information with the intention of causing harm (Walker, 2019). Intentional leaks of politicians’ emails, such as those observed during the 2017 French elections, are a good example of malinformation practices (Wardle & Derakhshan, 2017). What makes misinformation and malinformation different from disinformation is the intentional and malicious nature of the latter.

Gendered disinformation: Gendered disinformation is an emerging concept used both to encompass a subset of disinformation that directly attacks women’s identities or seeks to undermine feminism (Herrero-Diz, 2020) and to describe a form of violence against women in politics (Bardall, 2022). Research institutes and public authorities have also recently resorted to this concept. According to a recent study conducted by Canada, the European External Action Service, Germany, Slovakia, the United Kingdom and the United States, it is a “subset of misogynistic abuse and violence against women that uses false or misleading gender and sex-based narratives, often with some degree of coordination, to deter women from participating in the public sphere”, adopting a definition cited in previous literature (Jankowicz et al., 2021). Both foreign state and non-state actors are reported to use targeted gender disinformation tactics with the strategic intent of silencing women, undermining political discourse online, and influencing societal perceptions of gender and the role of women in democracies.

Foreign Information Manipulation and Interference (FIMI): In order to “prevent, deter and respond” to threats related to foreign interference through misleading information, the European External Action Service proposed the concept of FIMI (EEAS, 2021). It describes “a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.” What distinguishes FIMI from disinformation is its orchestrated character, by foreign actors, which can be demonstrated through behavioural analysis of disinformation focusing on tactics, techniques and procedures (TTPs).

WHAT DO WE MEAN BY FIMI TARGETING THE LGBTIQ+ COMMUNITY?

Although foreign information manipulation and interference targeting the LGBTIQ+ community are often cited as a relevant trend in some studies (e.g., Rosińska, 2021; Serrano, 2020; Shu et al., 2020; Strange, 2020; Cushman, 2020; Myers, 2021; Prior, 2021; Moskalenko & Romanova, 2022; Eady et al., 2023), there is still no specific conceptualisation to address it. The analysis of the incidents presented in this report demonstrates that the FIMI concept can help to fill this conceptual gap by shedding light on the international and politically

orchestrated nature of some information manipulation against the LGBTIQ+ community. For example, while many studies recognise that Russian media outlets play an important role in spreading misleading narratives about the LGBTIQ+ community in strategic regions, they are not always able to demonstrate how, or which

local channels act as proxies for these foreign sources of false information. The FIMI concept highlights the key relationship between state and non-state actors acting inside and outside their own territories, allowing for the analysis of a broader disinformation ecosystem and enabling more effective, targeted responses.

In this report, when we refer to FIMI targeting the LGBTIQ+ community, we are referring to a non-illegal pattern of behaviour that threatens and causes direct or indirect harm to members of the LGBTIQ+ community, affects values and disrupts the political process. It is often based on misleading narratives with a strong moral appeal involving gender, sexuality, family, reproduction or child protection. These narratives are fabricated, adapted, presented and disseminated in different contexts and territories with different political objectives. Such activities may or may not have the LGBTIQ+ community as their ultimate target (e.g., when authorities and institutions are associated with the LGBTIQ+ community with the aim of damaging their reputation), but they still rely on biases about the community to achieve other political goals while undermining the rights, well-being, dignity and safety of LGBTIQ+ people. Like other forms of FIMI, this type is manipulative in nature and is conducted in a deliberate and coordinated manner by state and non-state actors, including their proxies inside and outside their own territory. Intentionality can be demonstrated through the behavioural analysis of Tactics, Techniques and Procedures (TTPs).

FIMI TARGETING LGBTIQ+ AND THE INTERNATIONAL POLITICAL CONTEXT

Although they are not often the main research subject, women, LGBTIQ+ people and refugees are consistently mentioned in the literature on FIMI and disinformation as some of the main targets of misleading narratives. This chapter of the report discusses why LGBTIQ+ issues have become so central in contemporary politics, particularly in geopolitical debates based on existing literature on identity-based disinformation.

IMPLICATIONS FOR VALUES AND DEMOCRATIC PROCESSES

Regardless of their form and objective, they are contentious topics that touch on moral issues and deep-rooted prejudices. As observed in previous research (Strand & Svensson, 2022; Jones, 2020), these narratives are usually employed due to their high potential to reinforce social divisions, propagate moral panics⁸, incite hatred, evoke strong emotional responses, mobilise people and ultimately provoke hate crimes. Academic research on the reception of disinformation underscores the crucial role of emotions, especially negative ones, and emphasises the ability of these narratives to generate or tap into strong feelings to better engage audiences (Cheskin, 2017; Crilley and Chatterje-Doody, 2020; Edenborg, 2022). This means that effective FIMI, disinformation and other types of manipulative content do not necessarily lead to bias against certain social groups but rather resonate with audiences in which certain biases are already deeply ingrained (Schmitt, 2018).

In this sense, social media platforms have played a crucial role in the dissemination of recent FIMI campaigns. Gerbaudo (2018) points out that the algorithmic logic of these platforms tends to favour instantly popular content, which generates a high number of reactions within minutes of its publication. This mode of operation leads to a “mobocratic” tendency that favours more sensational and emotionally engaging content, giving disproportionate visibility to some issues and formats. The aggregative capacities of social media, such as the production of “filter bubbles”, tend to limit the public’s access to content that reinforces their pre-existing ideological positions and insulates them from contradictory positions (Gerbaudo, 2018). In addition, these platforms can also be used strategically to target specific audiences with

disinformation. This was the case with Russian interference in the 2016 US election, when targeted Facebook ads were used extensively to manipulate specific audiences (e.g. pro- and anti-LGBTIQ+) with misleading narratives (Jones, 2020). Social media platforms also become channels for specific groups engaged in the dissemination of FIMI and other forms of disinformation, such as internet trolls, *gamergaters*, hate groups, the “manosphere”, conspiracy theorist influencers and “alternative” media (Marwick & Lewis, 2017).

Previous research has presented numerous examples of FIMI and disinformation campaigns revolving around gender and sexuality. Russia-led disinformation campaigns often feature narratives around sexuality, gender and “race”, presenting Europe as a sort of dystopian realm characterised by sexual perversion (the so-called “Gayropa”) (Shevtsova, 2020), broken families, confused gender identities among children, and migrant men engaged in acts of rape and pillage (Edenborg, 2022). This situation is allegedly encouraged by governments and European institutions in the name of tolerance, feminism and multiculturalism (Cushman, 2020). By disseminating these narratives, political actors involved in FIMI intend to destabilise liberal democracies (Bennett and Livingston, 2018; Giles, 2016) and gain support for the conservative project advocated by the Kremlin (Keating and Kaczmarek, 2019; Edenborg, 2020).

Some of these campaigns have been relatively impactful in fuelling distrust of media, institutions and politicians, disrupting public policy and contributing to an environment of division, instability and discord. Given the broader goals, some scholars have pointed to the unsurprising overlap of interests between Russian state-sponsored disinformation and disinformation propagated by Western far-right groups, as they tend to have similar intentions (Innes et al., 2021). However, as Edenborg (2022) has observed, right-wing movements tend to criticise feminists and LGBTIQ+ activists at the domestic level for allegedly pushing radical agendas, but they also often portray the values of immigrants, particularly Muslims, as conflicting with an egalitarian gender order associated with the ideals of secular European modernity (Lentin and Titley, 2011). In both cases, the aim is to highlight the alleged negative effects of multiculturalism.

VULNERABILITIES AND POTENTIAL IMPACTS

In recent years, the growing visibility and mobilisation of LGBTIQ+ movements and significant legislative changes have become a relevant tool for threat actors interested in the erosion of human rights and democratic freedoms in different countries. Disinformation has been used as a weapon (Jones, 2020 Strand & Svensson, 2021 Luciani, 2021) placing LGBTIQ+ rights at the centre of various political and geopolitical debates. For example, in the case of Georgia, Luciani (2021) mentions the omnipresence of disinformation narratives disseminated by Russian actors contributing to the growing antagonism between the EU and Russia regarding their “shared neighbourhood” — in which Georgia occupies a strategic position. Moskalenko & Romanova (2022) refer to some Russia-affiliated sources that have been spreading a misleading video on Georgian social media, combining fragments of Ukrainian army footage with a UK-produced video advocating gay marriage. These narratives, also driven by local elites, help to crystallise “the idea of a value-based divide between the West/Europe and the East/Russia on LGBT+ issues” (Luciani, 2021, 197), even leading to violent conflicts between LGBTIQ+ and conservative activists.

The more general literature on disinformation is replete with references to harmful and misleading narratives about the LGBTIQ+ community (Rosińska, 2021; Serrano, 2020; Shu et al., 2020; Strange, 2020; Cushman, 2020; Myers, 2021; Prior, 2021; Moskalenko & Romanova, 2022; Eady et al., 2023). Although they do not always address the dimension of foreign interference, these studies contribute to showing that the LGBTIQ+ community, alongside women and immigrants,

is a constant target of FIMI and disinformation campaigns. At the same time, LGBTIQ+ civil society organisations such as ILGA have also expressed concern about the increase in disinformation campaigns targeting the community (ILGA-Europe Annual Review, 2020). In the US, a report released by the organisation GLAAD found that 40% of LGBTIQ+ adults and 49% of transgender and non-binary people in the country do not feel welcome or safe on social media, while 84% of respondents do not see enough protections on platforms to prevent discrimination, harassment or disinformation (GLAAD, 2022). However, some scholars argue that LGBTIQ+ issues represent an old trend when it comes to foreign interference. For example, during the Cold War, Soviet-infiltrated media spread narratives about young gay men being injected by the US government and being responsible for the AIDS crises (Boghardt, 2009).

The following section dedicated to the analysis of cases details the different categories of narrative used to target LGBTIQ+ people. By examining these narratives, it is possible to shed light on some of their potential impacts. First, FIMI targeting LGBTIQ+ communities can undermine equality and rights, influence public opinion and policy, create a hostile environment that endangers the lives and well-being of LGBTIQ+ people, fuel hatred and intolerance, perpetuate discrimination, reinforce stereotypes, and erode trust and credibility in reliable sources of information, including mainstream media, scholars, and organisations advocating for LGBTIQ+ rights. Second, these misleading and malicious narratives can also threaten a wide range of democratic values, such as the right to freedom of expression, equality, protection from discrimination, the right to political participation, privacy, trust in democracy, free and fair elections, and the right to accurate information.

ASSESSING FIMI CASES TARGETING LGBTIQ+ COMMUNITIES

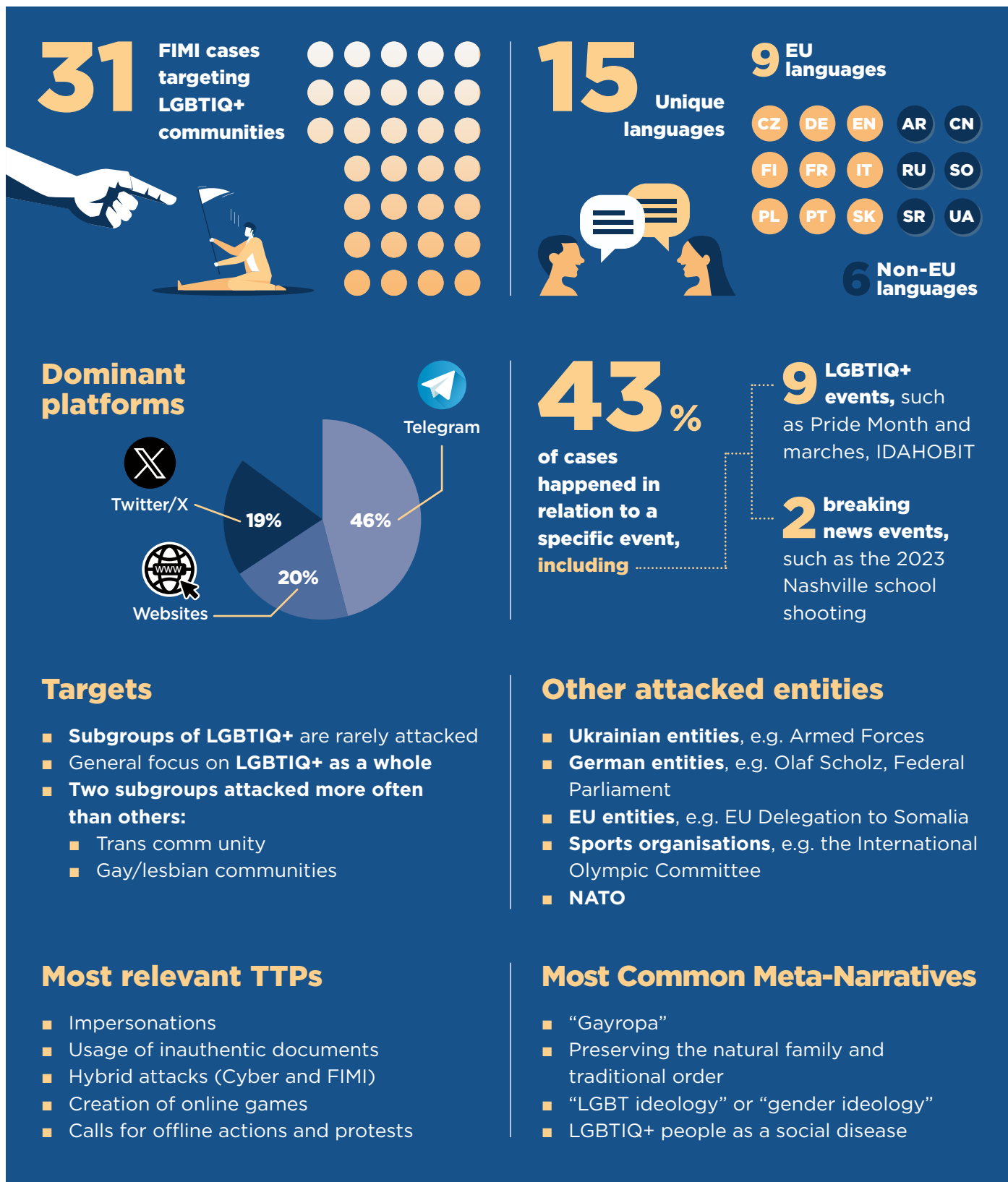


Figure 2: Key figures of findings across 31 incidents

This section outlines the findings of a systematic analysis of 31 FIMI incidents targeting LGBTIQ+ communities which were detected and documented between June 2022 and July 2023. Registered incidents covered a wide geographical representation, as FIMI instances were identified in 15 languages (Czech, English, Finnish, French, German, Italian, Polish, Portuguese, Slovak, Arabic, Chinese, Russian, Serbian, Somali and Ukrainian).

As a common feature, almost all detected incidents aimed at demeaning or humiliating LGBTIQ+ communities, along with other targets such as Western government entities, international organisations, geopolitical adversaries or political figures. Nearly 80% of documented incidents also targeted specific entities in relation to LGBTIQ+ rights and communities, such as Western governments, the Ukrainian government and non-governmental entities, the European Union, international organisations, and sports organisations.

The documented incidents also indicated the use of various FIMI Tactics, Techniques and Procedures (TTPs), ranging in particular from impersonating reputable and trusted information sources, fabricating inauthentic documents, and exploiting features and architectures of social media platforms, to more unusual techniques such as developing online games, promoting cyber-attacks and encouraging offline actions. In particular, this report highlights that the synthesis and diversity of TTPs and manipulative methods employed by FIMI threat actors underscore the need for robust, context-sensitive and adaptive counter-strategies, which will almost certainly rely on the ongoing sharing of information and lessons learned among stakeholders in order to effectively mitigate FIMI targeting LGBTIQ+ communities.

Documented incidents involved, or originated from, both foreign unattributed and foreign state-affiliated or state-linked channels across a range of platforms. Channels attributed to the Russian FIMI ecosystem and other unattributed channels frequently interconnected with content originating from sources attributed to Russia were involved in 55% of the documented FIMI cases. These channels fall into the following categories:

- *official communication channels*, such as state representatives', government and diplomatic channels;
- *state-controlled channels*, which are majority-owned or majority-controlled by a direct budget line of a state body/ruling party; and
- *state-linked channels*, sponsored by a state and/or ruling party through indirect budget lines or managed by state intelligence services.

While official communication channels were less active in the incidents, state-controlled and state-linked channels were involved in 25% and 45% of the incidents respectively. Nearly half (45%) of the incidents could not be attributed to a state actor through open sources, but show indicators of interaction with state-attributed channels.

In addition, the analysis revealed the systematic and opportunistic use of recurring elements for FIMI purposes, including specific meta-narratives and responses to real events and crises. In light of the analytical findings, the following subsections outline the notable behavioural patterns and recurring FIMI Tactics, Techniques and Procedures documented in the sample analysed. The analysis of the manipulative behavioural patterns also reveals the different target audiences, meta-narratives, platforms and real-life crises that were exploited in relation to the documented incidents.

UNDERSTANDING PATTERNS OF MANIPULATION AND FIMI TACTICS, TECHNIQUES AND PROCEDURES (TTPS) TARGETING LGBTIQ+ COMMUNITIES

The following FIMI TTPs and behavioural patterns are examples observed in the data collected as a result of dedicated efforts to detect and analyse FIMI incidents targeting LGBTIQ+ communities. Despite the relatively limited sample of cases, the first and foremost finding of this analysis is the variety and diversity of TTPs used to manipulate information spaces during documented incidents. The incidents analysed were carried out with a variety of tactical objectives as defined in the DISARM Red Framework and with a variety techniques used to achieve these objectives (Figure 3).

Such behavioural diversity is problematic for several reasons. First, similar to FIMI incidents and campaigns outside the scope of this study, FIMI actors appear to exhibit adaptive and evolutionary characteristics, continually refining and innovating their techniques to defeat FIMI defences and keep their strategies elusive and effective over time. Second, FIMI actors learn from experience and selectively employ different FIMI attack patterns to increase effectiveness, precision and operational flexibility. The use of different Tactics, Techniques and Procedures (TTPs) can also allow FIMI actors to effectively exhaust countermeasures and achieve sustainability of FIMI narratives, further increasing the range of online and offline harms through the perpetuation

Plan Strategy 2 techniques	Plan Objectives 13 techniques	Target Audience Analysis 3 techniques	Develop Narratives 7 techniques	Develop Content 9 techniques	Establish Social Assets 12 techniques	Establish Legitimacy 6 techniques	Microtarget 4 techniques	Select Channels and Affordances 12 techniques	Conduct Pump Priming 7 techniques	Deliver Content 4 techniques	Maximise Exposure 6 techniques	Drive Online Harms 5 techniques	Drive Offline Activity 5 techniques	Persist in the Information Environment 6 techniques	Assess Effectiveness 3 techniques
Determine Strategic Ends (1.1)	Cause Harm (1.1)	Identify Social and Technical Vulnerabilities (1.1)	Demand Insurmountable Proof	Create Hashtags and Search Artifacts	Acquire/Recruit Network (1.2)	Co-Opt Trusted Sources (1.3)	Create Clickbait	Blog and Publish (1.4)	Bait Legitimate Influencers	Attract Additional Media	Amplify Existing Narrative	Censor Social Media as a Political Force	Conduct Fundraising	Conceal Information Assets (1.5)	Measure Effectiveness (1.6)
Domestic Political Advantage	Defame	Find Echo Chambers	Develop Compelling Narratives	Develop Audio-Based Content	Acquire Botnets	Co-Opt Grassroots Groups	Create Localised Content	Bookmarking and Content Curation	Employ Commercial Analytic Firms	Comment or Reply on Content (1.7)	Cross-Posting (1.8)	Control Information Environment through Offensive Cyber-space Operations	Conduct Crowdfunding Campaigns	Change Names of Information Assets	Action/Attitude (1.7)
Economic Advantage	Intimidate	Identify Existing Conspiracy Narratives/Suspicions	Develop New Narratives	Deceptively Edit Audio (Cheap Fakes)	Build Network (1.9)	Co-Opt Influencers	Leverage Echo Chambers/Filter Bubbles (1.10)	Chat Anonymously (1.11)	Use Fake Reviews	Post across Disciplines	Post across Platforms	Block Content	Encourage Attendance at Events	Conceal Network Identity	Awareness (1.8)
Geopolitical Advantage	Spread Hate	Identify Existing Fissures	Integrate Target Audience Vulnerabilities into Narrative	Develop AI-Generated Audio (Deepfakes)	Create Community or Sub-Group	Compromise Legitimate Accounts	Create Echo Chambers/Filter Bubbles (1.10)	Use Unverified Chat Apps	Use Fake Experts (1.12)	Post across Social Media	Direct Users to Alternative Platforms	Conduct Server Redirect	Call to Action to Demand	Distance Reputable Individuals from Operation	Behaviour Changes (1.9)
Ideological Advantage	Cultivate Support for Ally	Identify Existing Prejudices	Leverage Conspiracy Theory Narratives	Develop Image-Based Content (1.13)	Create Organisations	Utilise Academic/Pseudoscientific Justifications	Exploit Data Voids	Consumer Review Networks	Use Take-Down Requests	Deliver Ad (1.14)	Traditional Media	Delete Opposing Content	Facilitate Logistics or Support for Attendance	Identify Individuals from Operation	Content (1.10)
Determine Target Audiences	Cultivate Support for Initiative	Identify Existing Media System Vulnerabilities	Amplify Existing Conspiracy Theory Narratives	Aggregate Information into Evidence Collages	Use Follow Trains	Create Fake Personas (1.15)	Use Existing Echo Chambers/Filter Bubbles	Anonymous Message Boards	Use Search Engine Optimisation	Post Content	Bots Amplify via Automated Forwarding and Reporting	Destroy Information Generation Capabilities	Organise Events	Launder Information Assets	Knowledge (1.11)
	Defend Reputation	Identify Target Audience Adversaries	Develop Original Conspiracy Theory Narratives	Deceptively Edit Images (Cheap Fakes)	Create Inauthentic Accounts (1.16)	Establish Inauthentic News Sites (1.17)	Purchase Targeted Advertisements	Email	Formal Diplomatic Channels	One-Way Direct Posting	Conduct Keyword Squatting	Harass (1.18)	Pay for Physical Action	Use Pseudonyms	Measure Effectiveness Indicators (or KPIs) (1.12)
	Energise Supporters	Identify Wedge Issues	Map Target Audience Information Environment (1.19)	Develop AI-Generated Images (Deepfakes)	Create Bot Accounts	Create Inauthentic News Sites (1.17)		Audio Stream (1.20)	Formal Diplomatic Channels	Post Violative Content to Provokes Take-down and Backlash	Conduct Keyword Squatting	Harass People Based on Identities	Use Shell Organisations	Conceal Infrastructure (1.21)	Message Reach (1.13)
	Justify Action	Recruit Members	Assess Degree/Type of Media Access	Leverage Existing Narratives	Create Cyborg Accounts	Leverage Existing Inauthentic News Sites		Video Stream (1.21)	Audio Stream (1.20)	Share Memes	Conduct Keyword Squatting	Threaten to Dox	Conduct Physical Violence	Conceal Sponsorship	Measure Performance (1.14)
	Dismay	Discredit Credible Sources	Conduct Web Traffic Analysis	Develop Memes	Create Inauthentic Social Media Pages and Groups	Prepare Assets Impersonating Legitimate Entities (1.22)		Media Sharing (1.23)	Audio Stream (1.20)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Obfuscate Payment	Content Focused (1.15)
	Deter	Discourage	Evaluate Media Surveys	Respond to Breaking News Event or Active Crisis	Develop AI-Generated Text	Assessing	Spoo/Parody Account/Site	Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	People Focused (1.16)
	Silence	Divide	Identify Trending Topics/Hashtags	Develop False or Altered Documents	Cultivate Ignorant Agents			Photo Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Shell Organisations	View Focused (1.17)
	Facilitate State Propaganda	Make Money	Monitor Social Media Analytics	Develop Inauthentic News Articles	Develop Owned Media Assets			Online Polls	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
	Extort	Generate Ad Revenue	Segment Audiences (1.24)	Develop False or Altered Documents	Develop Owned Media Assets			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
	Manipulate Stocks	Raise Funds	Demographic Segmentation	Develop Inauthentic News Articles	Develop Owned Media Assets			Photo Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
	Scam	Sell Items under False Pretences	Economic Segmentation	Develop Inauthentic News Articles	Develop Owned Media Assets			Online Polls	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
			Geographic Segmentation	Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
			Psychographic Segmentation	Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View Focused (1.17)
				Deceptively Edit Video (Cheap Fakes)	Develop Video-Based Content			Audio Sharing	Video Stream (1.21)		Conduct Keyword Squatting	Threaten to Dox	Encourage Physical Violence	Use Cryptocurrency	View F

challenges and potential harms to targeted organisations, groups and audiences. FIMI campaigns often aim to disguise their origin in order to avoid attribution. Impersonation of other entities adds a layer of difficulty in unmasking the origin or creator of disseminated content. In addition, some impersonation sub-techniques and procedures increase the risk of harm. The impersonation of certain groups, particularly in the context of human rights or existing political debates, can aim to further escalate tensions and increase social division, sometimes by increasing scepticism towards targeted entities. In addition, impersonation provides FIMI threat actors with tactical advantages, such as increasing the perceived legitimacy of a false claim by presenting it as coming from a reputable source.

Further categorisation of the documented incidents revealed various sub-techniques and procedures, which include impersonation as a central TTP. To leverage and support the narratives targeting LGBTIQ+ communities, different types of entity were impersonated, including legitimate and reputable media outlets, government officials, government entities, and non-governmental organisations. The second categorisation emerged from the preferred types of content used in the incidents, such as fake videos, fake images, fake magazine covers, fake social media posts from impersonated accounts, and even fake announcements on job portals. In later stages, the execution of the incidents and the distribution of the content were carried out through various

means, ranging from inauthentic social media accounts and websites to coordinated Telegram posts and publications by state-affiliated outlets controlled by FIMI actors.

Examples of documented FIMI incidents highlight the different patterns and procedures of impersonation that have been leveraged to further reinforce anti-LGBTIQ+ narratives. In multiple incidents, videos mimicking the logo, style and other visual elements of Western media outlets such as Euronews and Le Figaro, allegedly reporting on real events or statements about LGBTIQ+ communities, were disseminated across platforms (Figure 4). In other incidents, fabricated and relatively well-designed magazine covers impersonating Europe-based media were posted on social media, again to support similar meta-narratives.

In July 2023, a fake job vacancy impersonating a Ukrainian non-profit organisation was posted on a Ukrainian online job portal, advertising a fake position for a mentor for the Armed Forces of Ukraine (Figure 5). Among the requirements listed were “active sexual life”, “absence of venereal diseases” and “identifying hidden gays”. The post used specific derogatory language targeting LGBTIQ+ people vis-à-vis the Armed Forces of Ukraine. The screenshots of

Figure 4: Fabricated videos and magazine covers often impersonate Western media outlets to reinforce existing FIMI narratives targeting LGBTIQ+ communities



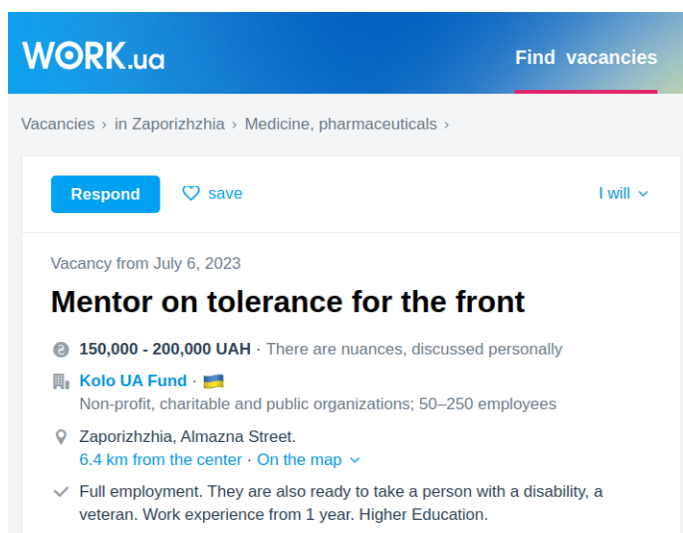


Figure 5: The job ad posted on a Ukrainian job portal, impersonating a Ukrainian NGO (text translated from Ukrainian to English)

the fake vacancy were later disseminated by the Russian state-linked accounts on different social media platforms. In another incident, a video with the logo of the Armed Forces of Ukraine was posted on Russian state-affiliated channels. In all cases, the content impersonating legitimate entities was combined with false claims or derogatory text targeting LGBTIQ+ communities, Western governments, or Ukrainian government entities.

Development and amplification of inauthentic documents or other offline content

The use of fabricated documents or other types of offline content such as fake flyers was another prominent pattern in the sample. This particular pattern also shares similarities with impersonation techniques, as fabricated documents also aim to increase the perceived legitimacy of the falsehoods spread in FIMI incidents. Overall, another similarity between the content and false claims amplified by impersonation and fabricated documents is the patterns documented in the execution phase of various incidents, mainly in the delivery of content or in maximising the exposure of target audiences to falsehoods. In both cases, the delivery and amplification were via deceptive messages and articles misattributing fabricated content to legitimate and trusted sources.

In addition, the prominent use of inauthentic documents and offline materials is likely derived from their perceived effectiveness in both the short and long term by FIMI threat actors. Strategically “leaked” or purportedly open source documents are often used to reinforce existing FIMI narratives tailored to specific FIMI campaigns,

mainly by claiming additional evidence originating from reputable sources. Fabricated documents or content, such as flyers, are also tailored to specific audiences or used to attack official entities, groups or individuals. The repeated and large-scale use of fabricated documents and offline content can also be aimed at eroding trust over time, as the debunking of such content and associated claims may lag behind their dissemination. Documents and other offline materials can also be used to bait unrelated entities such as reporters in different countries, which can contribute to the perceived authenticity and legitimacy of the fabricated content.

In addition to the aforementioned characteristic features, the examples of documented FIMI incidents indicate the use of fabricated documents and flyers to target specific audiences against LGBTIQ+ communities and their rights. In June 2023, in an incident targeting audiences in the Central African Republic, images of fake flyers, depicting two men kissing and purportedly promoting a French brewery, while explicitly claiming the “promotion of European values”, were disseminated by unattributed

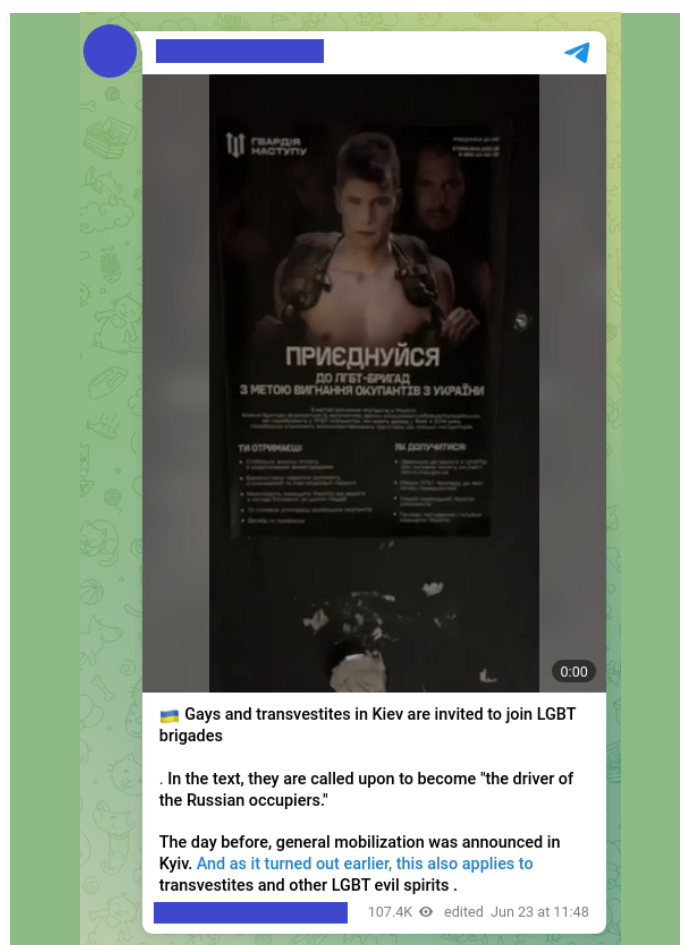


Figure 6: The video showing the inauthentic flyer (text translated from Russian to English)

Twitter accounts and Facebook pages. Later examination of the incident revealed that the same pages frequently promoted content from other Facebook pages linked to Russian private military companies.

Similarly, other incidents leveraged existing FIMI narratives about LGBTIQ+ communities to target and demean Ukraine or the Western policies towards Ukrainian refugees. In 2023, images showing a fabricated document misattributed to the Armed Forces of Ukraine, allegedly prohibiting gay people from having intimate relationships on the battlefield, were disseminated by unattributed websites and Telegram channels, which often amplify or mirror content from the Russian FIMI ecosystem (Figure 6). In July 2023, an image showing a deceptively altered page from an official German booklet addressed to Ukrainian refugee families, informing them about possible gender reassignment in German schools, was promoted through messages in Russian, Ukrainian and Polish. Most of the documented incidents took place across platforms and websites.

Exploitation of platform features: Cases of coordinated tagging and replies to other social media entities and combining “evidence collages”

Multiple incidents included FIMI Tactics, Techniques and Procedures (TTPs) that rely on the effective use and exploitation of features that are central to how social media platforms function and how their users interact. One such feature is the ability to tag, mention or reply to other social media entities often belonging to public figures, public institutions, or other publicly known figures such as political actors, journalistic entities, or individuals. Similar to other FIMI incidents outside the scope of this collection, incidents involving this behaviour exhibited strong signals of potential coordination based on a close examination of the activity observed and collected during these cases. Such incidents generally require multiple steps in the attack pipeline, ranging from target identification, message formulation and synchronisation of delivery to further amplification or flooding of the information space. If successful, such attacks can lead to the organic participation of other social media users, potentially resulting in feedback loops that further increase engagement.

The use of evidence collages or the combination of various multimedia contents, real or fabricated, to support corroborative visual narratives is another TTP used to legitimise and reinforce FIMI narratives directly or indirectly targeting LGBTIQ+ communities. Despite its simple and low-cost nature, this FIMI technique capitalises

I urge @EutmPio to sincerely apologize to the Somali people. Promoting LGBT is not acceptable in #Somalia. We don't consider 'homosexuality' as a human right. This is a clear desecration of our religion, culture and values.

Deleting this controversial tweet is not enough.



As anticipated @EU_in_Somalia and affiliated agencies i.e @EUNAVFOR @EutmPio attempted to hide their subversive actions by deleting tweets after #Somalis exposed their agenda. Somalis are awake to their #neocolonial aims which are against our #sovereignty and #religious identity.

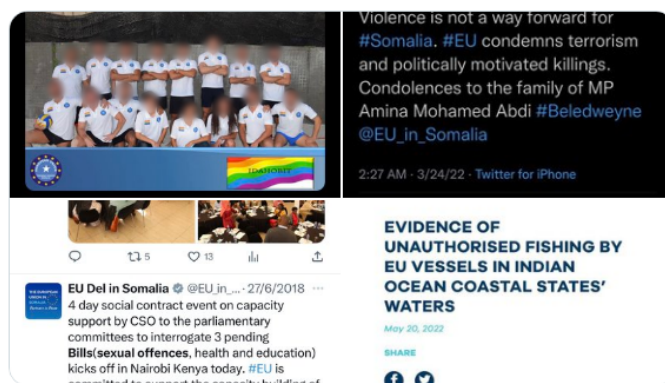


Figure 7: An example of a post tagging EUTM Somalia and the collage used in the FIMI incident

on cognitive biases to achieve increased credibility, authenticity and legitimacy of visual information. Similar to coordinated tagging and reply posts, this technique also requires multiple accompanying steps or techniques to achieve high performance, including identification, collection, context removal, composition, delivery and amplification.

Combined with other Tactics, Techniques and Procedures (TTPs) employed in the same incidents, both of these techniques are problematic for multiple reasons. In the context of LGBTIQ+ rights and people, coordinated tagging and replies often aim to intimidate and silence designated opponents or entities supporting genuine public debate and representation. Various previous experiences with similar patterns of behaviour point to characteristics of toxic content. By targeting public figures and institutions supportive of LGBTIQ+ rights, these attacks aim to undermine their credibility and possibly deter others from expressing support. Similarly, the use and combination of visual evidence collages aim to manipulate public perception via out-of-context visual elements as conclusive evidence. In the long term, repeated attacks of this nature aim to undermine advocacy efforts, erode support and distract attention from legitimate human rights concerns and dialogues.

In May 2023, a network of unattributed accounts swarmed the social media platform X (formerly Twitter) and Facebook, collectively tagging, quoting or replying to the official accounts of EU entities such as the EU Delegation in Somalia, the EU Training Mission in Somalia and EUNAVFOR in response to a tweet by the EU Training Mission in Somalia (EUTM Somalia) (Figure 7).

The EUTM Somalia post showed an image of a sports team with the rainbow flag on the occasion of the International Day Against Homophobia, Biphobia and Transphobia (IDAHOBIT). The participating accounts shared the screenshot of the EUTM Somalia tweet and accused the EU of undermining the culture and values of Somalia and disrespecting its religion. The activity was initiated and mainly carried out by unattributed accounts on Facebook and Twitter, using combinations of out-of-context images and screenshots to accuse the EU of dumping radioactive material in Somali territorial waters, facilitating illegal fishing, and intentionally promoting homosexuality in Somalia as part of a political agenda. Examination of this activity revealed the repeated use of the same content by the same accounts to promote the same or similar claims despite the unfounded and decontextualised nature of the content that allegedly constitutes “evidence”.

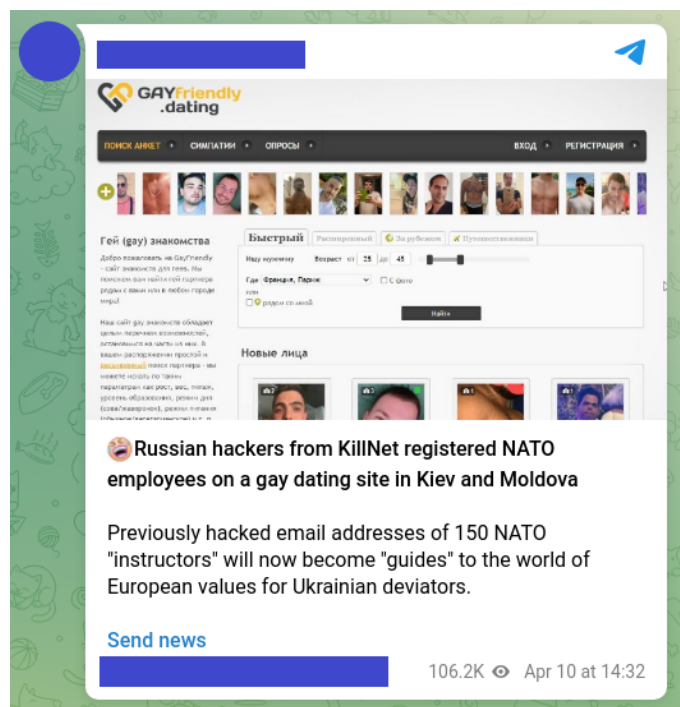


Figure 8: The post claiming the registration of NATO staff emails on a gay dating site (text translated from Russian to English)

Low-frequency, high-impact behaviours and TTPs

Within the documented set of FIMI incidents targeting LGBTIQ+, some TTPs stood out as outliers, while retaining the potential to pose unique short- and long-term challenges in terms of FIMI countermeasures. Those include the use and promotion of cyber-attacks against international entities, the development and sustained promotion of a web-based online game, and calls for offline actions and protests.

In the case of cyber-attacks and their promotion, as well as the allegedly stolen information, cyber threat actors, possibly in coordination with other FIMI actors, disseminated and promoted their self-proclaimed attacks and alleged personal information about individuals through dedicated information channels. Such attacks put LGBTIQ+ people and other targeted entities at risk of harassment, doxing, and other forms of online harm, while further reinforcing existing FIMI narratives.

On the other hand, the promotion of an online game in which players are encouraged to eliminate symbols of various adversaries, including the rainbow flag, normalised and trivialised hostility against specific targeted groups such as the LGBTIQ+ community. While FIMI actors primarily aim to reinforce existing narratives through the use of different TTPs, this specific FIMI technique can also be categorised



Figure 9: Screenshot of South Front's game "Smash the Nazis"

in terms of its dehumanisation and desensitisation effects, as well as its potential propagation of hate.

Similarly, particularly in the context of FIMI targeting LGBTIQ+, calls to offline action are particularly problematic for their additional presumed aims of suppressing voices supportive of LGBTIQ+ rights and potentially inciting real-world harm. Overall, the use of distinctive manipulative behaviours highlights the innovative ways in which FIMI actors can inflict harm and normalise prejudice, while constantly evolving and enhancing their toolkit and potentially increasing the complexity of countermeasures.

Killnet, a known Russia-aligned hacker group, have repeatedly claimed denial-of-service (DDoS) attacks, followed by the promotion of their self-proclaimed successful results via dedicated communication channels. Since the beginning of Russia's full-scale invasion of Ukraine in 2022, Killnet's attacks reportedly concentrated on government entities, public services, critical infrastructure and European companies, among others.

In April 2023, Killnet promoted a self-proclaimed and imminent attack against NATO. The promotion of the attack involved multiple Telegram channels. A few days after the first promotion, Killnet claimed a successful attack that allegedly took down 40% of NATO's cyber infrastructure.

In the aftermath of the alleged attack and claims of success, Killnet-related channels announced that the personal information, including names and emails of NATO-affiliated individuals, had been registered on a gay dating website (Figure 8). Throughout the timeline of the incident and following the aforementioned announcement, the content was further amplified by communication channels associated with the Russian FIMI ecosystem and infosphere, including state-affiliated and state-linked media. In this incident, the

Russian FIMI ecosystem and infosphere co-employed the TTPs in using cyber means, swarming online information spaces, and doxing individuals to degrade and humiliate both an adversarial international actor and LGBTIQ+ people.

In June 2022, South Front, an outlet tied to the Russian FSB, released a game called "Smash the Nazis" on its website, along with a mobile application file that could be downloaded and used on Android platforms (Figure 9). The game was similar to the popular Fruit Ninja game, but instead of fruit, players had to slash helmets with Nazi symbols, the NATO logo and rainbow flags. After the original website, southfront.org, was taken down in August 2023, South Front's new website, southfront.press, continued to feature the same game on its homepage. Both versions of the game included a button redirecting to a page collecting donations for South Front.

RESPONDING TO REAL-WORLD EVENTS AND CRISES

FIMI threat actors strategically respond to real-world events and crises in order to decontextualise unfolding situations, sow discord, and manipulate the perceptions of target audiences. To this end, FIMI actors exploit opportune moments and selectively promote divisive narratives, sometimes exploiting

The room where Audrey Hale lived, who carried out the shooting at the American school

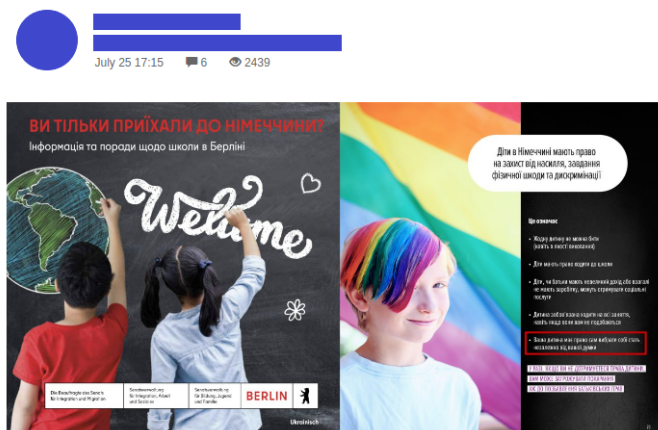
March 28 · 794 read



Mountains of garbage, flags of LGBT, NATO and American socialists: the room of 28-year-old Nashville resident Audrey Hale, who considered herself a trans man.

Figure 10: Post about the alleged bedroom of the Nashville school shooter (text translated from Russian to English)

Here is a booklet issued to Ukrainian refugees - parents in Germany:



"Have you just arrived in Germany? Do not interfere with the child to change sex!"

Figure 11: Examples of cases targeting minority communities in Germany (text of the brochure translated from Russian into English)

online echo chambers or social vulnerabilities. FIMI around real or breaking news events relies on exploiting emotional triggers and increasing susceptibility to manipulated information. These features particularly apply to incidents targeting LGBTIQ+ communities.

In the context of this analysis, 43% of documented incidents took place before, during or after a specific event. Most of these events were LGBTIQ+ related, such as Pride Month, Pride Marches in New York, Berlin, Munich and Lyon, and the International Day Against Homophobia, Biphobia and Transphobia (IDAHOBIT), as highlighted in other subsections.

However, some of the documented incidents followed seemingly unrelated crisis events. For example, shortly after the school shooting in Nashville, USA, on 27 March 2023, unattributed accounts on Twitter and Telegram circulated a photo showing a bedroom with a rainbow flag, a transgender flag, and a NATO flag on the walls, claiming that the image showed the bedroom of the school shooter (Figure 10). The same image and false claim were later posted on other platforms, including relatively new and smaller ones, and on Russian websites. In fact, the image was previously posted by a Twitter account that had nothing to do with the incident. The reuse and appropriation of old content, as well as conspiracy theories in line with other FIMI narratives, is a common and recurring TTP in different contexts.



SEGMENTATION OF TARGET AUDIENCES WITH LOCALISATION OF FIMI CONTENT AND NARRATIVES

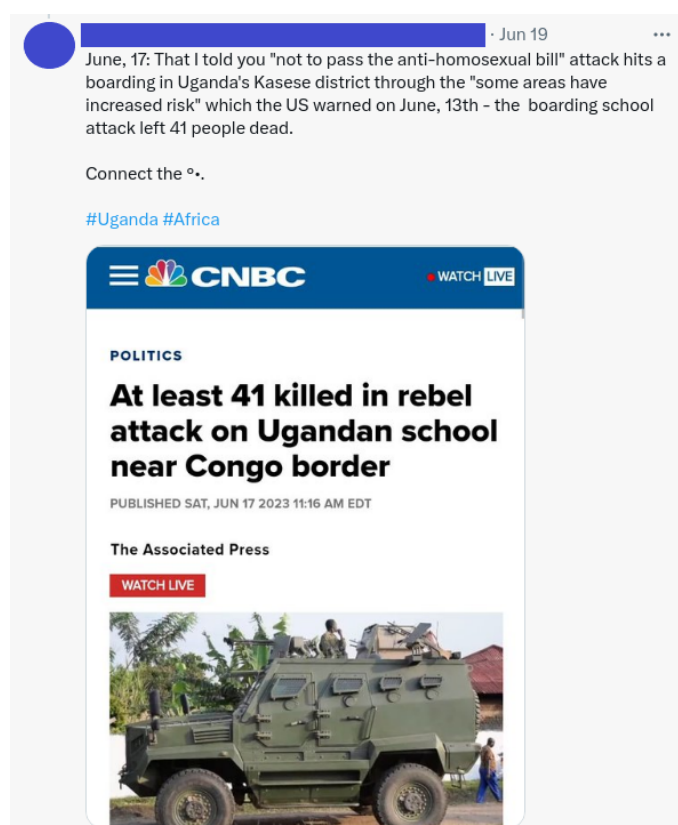
Although assessing the target audiences of the incidents documented in this report proved to be a non-trivial task, a common feature was the targeting of specific audiences, often in combination with the use of localised content and amplified narratives. In the context of FIMI, target audience segmentation and the use of localised content generally indicate a systematic and relatively sophisticated manipulation capability of FIMI threat actors, who use such TTPs to tailor messages and attack patterns to different audience subsets, mainly to increase the resonance, believability and strategic impact of FIMI.



Figure 12: Examples of content targeting African audiences

This sophistication can have particularly problematic implications in the context of FIMI targeting specific groups such as LGBTIQ+, as tailored or appropriated FIMI narratives often aim to undermine cohesive public discourse while reinforcing stereotypes and marginalising vulnerable groups.

Across the different cases analysed for this report, the use of specific languages, as well as content tailored to specific regions, countries or communities, was among the characteristics that signalled the segmentation of target audiences. For example, two incidents in the German context appeared to target the Muslim community and Ukrainian refugee families (Figure 11). In both cases, the German government was portrayed as aggressively pursuing the “LGBTIQ+ agenda” against minority families and children. In the first incident, a video showing German police removing a child from a Muslim family, allegedly because the family was teaching the child that homosexuality and transgenderism were unacceptable,



was widely disseminated across platforms and languages including Arabic, English, Russian and Serbian. The police later issued a statement saying that they had acted on a court order and in support of the youth welfare office. The other case targeting Ukrainian refugee families and informing them about possible gender re-assignments in German schools has been described in the previous subsections.

In other cases, the incidents specifically targeted African audiences in Somalia, the Central African Republic and Uganda (Figure 12). In an incident described in the previous sub-sections, a campaign was launched on Twitter accusing EU entities in Somalia of disrespecting Somali culture, religion and values by promoting a picture of a sports team and a rainbow flag. In a similar incident targeting audiences in the Central African Republic, a photo of a fabricated flyer was distributed on Twitter and Facebook. The flyer allegedly advertises the MOCAF beer company (part of the French Castel group) and shows two men kissing with the text “MOCAF, promotion of European values”. The accompanying commentary was that European values should be promoted in France and not in Africa. Lastly, in another case, unattributed accounts apparently linked to Somalia accused the US of enabling violent attacks on Ugandan schoolchildren and soldiers in response to Uganda’s adoption of the anti-LGBTIQ+ bill.

STRATEGIC USE OF META-NARRATIVES IN RELATION TO LGBTIQ+ COMMUNITY

Academic literature identified key FIMI and disinformation narratives about the LGBTIQ+ community coinciding with the documented incidents of the sample. The collection of cases demonstrates the consistent use of a set of meta-narratives to strategically target LGBTIQ+ communities, often in conjunction with other entities. By leveraging existing high-level narratives, FIMI threat actors and channels interweave manipulative content and other documented TTPs with recognised, overarching narratives, thereby increasing perceived credibility, relevance and resonance, especially when recurring FIMI patterns achieve long-term impact and performance. This allows FIMI actors to exploit pre-existing biases, stereotypes and prejudices to manipulate information spaces with various manipulative contents about LGBTIQ+ communities. The following examples highlight the common meta-narratives recorded in the sample of incidents analysed in this report.

“Gayropa”: Western authorities forcibly upholding the “LGBTIQ+ agenda”

A recurrent type of narrative suggests that LGBTIQ+ rights promotion is a disguised form of “colonisation” by the morally corrupt West. LGBTIQ+ equality is portrayed as “a neo-colonial project through which activists and their governments try to export their decadent values and secularise non-Western societies” (Kuhar & Paternotte, 2018, p. 8).

In the data collection, this meta-narrative emerged from the recurring use of several sub-narratives in relation to both domestic and international contexts. In domestic contexts, Western governments and authorities were repeatedly accused of forcing local communities to accept and comply with the “LGBTIQ+ agenda” or face enforced consequences. In the international context, this meta-narrative was repeatedly used to target specific regional audiences through localised FIMI content and the appropriation of previous content and narratives. In addition, this meta-narrative appears to be intertwined with notions of cultural sovereignty, national identity and resistance to perceived Western cultural imperialism and hegemony, making it a frequently used tool for further manipulation of perceptions of LGBTIQ+ rights and people. Some of the instances of this meta-narrative have been described in other subsections, where support for LGBTIQ+ rights has been portrayed as equivalent to political interference by Western governments in various countries.

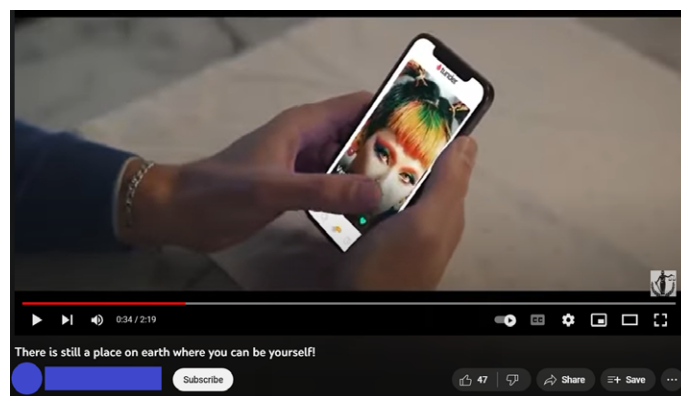


Figure 13: Video showing a man searching for a romantic partner

In December 2022, a sub-narrative under this category that “Western men can’t date ‘normal’ women anymore” was utilised in a video disseminated by the Russian House in Tel Aviv (Figure 13). The video depicted a man in search of a romantic partner finding it impossible to meet heterosexual women in Western countries. The video mocked LGBTIQ+ communities and promoted the notion that Russia still represents traditional values, while the West is in decline due to the aggressive “LGBTIQ+ agenda”.

Another frequent sub-narrative detected in the sample of cases was the alleged preferential treatment of LGBTIQ+ athletes in sports. Within the sample analysed, most of the incidents with this meta-narrative originated from a FIMI campaign that revolved around false claims and fabricated quotes accusing the International Olympic Committee and its president of imposing specific rules for each country participating in the Olympic Games. The incidents analysed originated from postings with content claiming to be from Western media outlets, while later incidents involved statements and publications from Russian state-affiliated information sources. Also in these categories, other incidents propagated sub-narratives such as “the Olympics is a political event and it promotes the LGBTIQ+ agenda”.

Preserving the “natural family” and the “natural order” while protecting children from LGBTIQ+ “sexual perversions”

According to this line of argument, the “liberal understanding” of gender and the expansion of sexual and reproductive rights pose a threat to “the traditional/nuclear/natural” families, consisting of a married man and woman who have children (Strand & Svensson, 2021). In addition, LGBTIQ+ people are presented as a threat to children due to their allegedly inherent “predatory behaviour” and desire to “convert children into sexual perversions” (Jarkovská,

2020). Analysing articles on sex education published on pro-Russian websites in the Czech and Slovak Republics between 2007 and 2016, Jarkovská (2020) noted how FIMI and disinformation narratives about the alleged sexualisation of children at school (e.g., teachers who teach children to masturbate in the classroom) are used to promote Russia as the “leader of a conservative revolution” (Jarkovská, 2020, p. 139) in post-communist societies in opposition to a certain “Western crisis of values”. This crisis is said to be rooted in a deep spiritual degradation, an accelerated loss of Christian identity, right-wing liberalism in the economy and left-wing liberalism in culture (Chebankova, 2012).

Within the sample analysed, the meta-narrative that portrays LGBTIQ+ identities and rights as inherently hostile to traditional and family values was a recurring theme. The use of this meta-narrative spanned incidents targeting different audiences. In the incidents taken as examples, video compilations were disseminated showing decontextualised scenes from various Pride marches and LGBTIQ+ events, implying that LGBTIQ+ specifically threatens the safety and well-being of children.

“LGBT ideology” or “gender ideology”

Opposition to an alleged “LGBT ideology” or “gender ideology” has been a recurring framework in this field (Strand & Svensson, 2021). The term “anti-gender” encompasses a broad opposition to women’s struggles for equality and LGBTIQ+ rights (Graff & Korolczuk, 2022; Paternotte, 2023). Underlying these forms of resistance is the belief that gender equality and sexual and reproductive rights undermine conventional, nuclear or “natural” family structures, which typically consist of a married heterosexual couple with their children (Kuhar & Paternotte, 2018). Many of these narratives present homosexuality and trans identities as “abominations” (Ayoub & Page, 2020), homosexuality as inherently “perverse, excessive and wicked” (Mršević, 2013; Van Klinken & Zebracki, 2016), and “LGBTIQ+ practices” as a threat to the social and moral order, as prescribed to man by God (Van Klinken & Zebracki, 2016; Strand & Svensson, 20212).

LGBTIQ+ people as a social disease to be countered

The references to medical vocabulary with the repeated use of terms such as “virus”, “contamination” and “disease” can also be found in many other narratives. For example, during the COVID-19 pandemic, one narrative spread by Kremlin-linked news media, first identified in the Middle East, claimed that COVID vaccines were capable of turning people LGBTIQ+ (Moskalenko & Romanova, 2022). Other narratives spread by the Russian government claim that sexual orientation is a contagious “disease” that can be transmitted through contact with LGBTIQ+ individuals and exposure to “LGBTIQ+ propaganda” including all kinds of LGBTIQ+ imagery and symbols (Cushman, 2020). These narratives portray LGBTIQ+ people as “dangerous,” “undesirable” and “perverse” individuals who pose a threat to society and therefore need to be “prevented” or “countered”.

SELECTION OF CHANNELS AND PLATFORMS TO DELIVER CONTENT

A variety of different online platforms were used to distribute the content recorded in the incidents, ranging from mainstream social media platforms, such as Facebook and YouTube, to alternative platforms focused on specific and regional audiences, such as the Russian VK.com and Zen platforms. However, the findings show the clear dominance of three platforms. The first is the instant messaging platform Telegram, with almost half (48%) of all content coming from Telegram. The second most common channel is the use of websites. One fifth of all content in the incidents is published on websites of various entities, including state-controlled and state-affiliated media. The third most observed platform is X (formerly Twitter) with 19% of all content published on the platform.

GAPS AND OBSTACLES TO BETTER UNDERSTANDING THE THREAT AND ACTIVATING RESPONSES

Research findings suggest that the main gaps in tracking, preventing and countering FIMI targeting the LGBTIQ+ community are related to the lack of coordination, cooperation and communication between stakeholders. Isolated initiatives, poor use of existing networks, low funding, deficit of spaces to bring together experts and little research specifically focused on the issue are also relevant challenges to overcome. In addition, wider access to evidence-based analysis could enable policymakers, civil society organisations, academics, international authorities and governments to collaborate and make better decisions.

Governments and diplomatic organisations:

- Participants from the public sector highlighted that a number of innovative responses have recently been launched, such as the EU Code of Practice on Disinformation, the EU's Foreign Information Manipulation and Interference (FIMI) Toolbox, and the Digital Services Act (DSA), which can serve as a benchmark for advancements in legislation for policy makers and partners in other territories.
- It was noted during the workshop that knowledge of these instruments among involved stakeholders, and civil society in particular, is often insufficient. Simpler, more direct and effective communication about these initiatives could increase their impact and help create a more coherent transnational network of actors committed to combating FIMI.
- However, when it comes to understanding, tackling and mitigating the effects of specific forms of FIMI (e.g., FIMI targeting LGBTIQ+), not all respondents seem to be convinced of the need for actions focused exclusively on specific communities. Therefore, there still seems to be a need to raise awareness among stakeholders at all levels about the harmful effects of FIMI on the LGBTIQ+ community and other types of identity, and its correlation with a threat to universal human rights and democracy.

Private sector:

- Professionals working in social media companies may find it challenging to track, identify and counter FIMI targeting LGBTIQ+ communities in so many different legal, cultural and linguistic contexts.
- Given the increasing amount of content that platforms need to monitor on a daily basis, the variety of behaviours and techniques used by perpetrators and its continuous evolution, these professionals would benefit from better guidelines to support the rapid detection of narratives, behaviours and TTPs that characterise FIMI targeting the LGBTIQ+ community.
- It also appears that many companies are struggling to establish a more direct dialogue with LGBTIQ+ civil society organisations and academics. These are missed opportunities, given that building common frameworks for threat detection also depends on the expertise of researchers and organisations working close to LGBTIQ+ communities or of the community itself.

Civil society:

- Due to a lack of resources, infrastructure and support from governments and diplomatic organisations, LGBTIQ+ organisations and communities are often overwhelmed by multiple demands. As a result, they are rarely able to focus exclusively on countering information manipulation, even though they often have to deal with its negative effects.
- As a consequence, for many organisations, it is difficult to recognise the extent of foreign interference when it comes to the many disinformation campaigns currently targeting the LGBTIQ+ community.
- In contexts where politicians feel pressured by the impact of identity-based FIMI and disinformation, LGBTIQ+ organisations report a systematic lack of political will on the part of governments and MPs. The absence of cooperation often delays the passage of bills and the development of public policies that could help protect the community.

Academics:

- There is a lack of resources for advancing innovative research on disinformation and foreign interference as such, and in particular with regard to the identity-based FIMI.
- Studies also point to the difficulties in accessing reliable data, particularly from digital platforms, as one of the main barriers to advancing research in this field.
- The political context, permeated by anti-gender and anti-woke campaigns, also threatens freedom of thought, professorship and research.

These gaps suggest that the lack of coordination and cooperation among stakeholders has contributed to the poor circulation and distribution of the pool of already existing knowledge of FIMI cases targeting the LGBTIQ+ community, and of resources to address and counter FIMI in different

regions. Fragmentation and the absence of cooperation mechanisms have also affected the general understanding of the current political context and how issues of gender and sexuality have become crucial elements of the democratic process, including at the geopolitical level.

While LGBTIQ+ issues have been consistently weaponised by state and non-state actors to achieve a range of political objectives, this instrumental character should not obscure the different views on gender and sexuality observed in the cases analysed in this report. **The evidence-based analysis provided by the EEAS sheds light on the persistence of discrimination against LGBTIQ+ people as a global problem that needs to be urgently addressed by governments and diplomatic organisations. From a societal point of view, this seems to be the best way to ensure that citizens are less inclined to engage with biased information about the LGBTIQ+ community in the future.**

RECOMMENDATIONS FOR RESPONDING TO AND COUNTERING FIMI TARGETING LGBTIQ+

This section presents a series of recommendations for policy makers, governments, international organisations, civil society, academia, the private sector and other stakeholders interested in countering or mitigating the impact and harm of FIMI on LGBTIQ+ communities. Recommendations are addressed to specific groups of stakeholders and, where possible, suggest joint work among them. They are divided according to the four pillars of the FIMI toolbox.

Given the mandate of the EEAS, the recommendations focus mainly on the foreign interference aspects of information manipulation related to LGBTIQ+ communities. However, the spread of information deliberately manipulated by state or non-state actors constitutes a multidimensional problem

that touches upon internal and external affairs, human rights, democracy and security issues. Despite the focus on the foreign relations dimension, the recommendations do not necessarily neglect the other dimensions of the problem.

For the experts consulted during the research, ensuring the protection of the LGBTIQ+ community and other discriminated communities is a fundamental part of strengthening democracy. When they neglect specific dimensions present in FIMI and disinformation campaigns, governments and international organisations miss the opportunity to develop actions capable of overcoming divisions at the grassroots of society. More political action is needed to take on this task and to prevent the rights of the LGBTIQ+ community from being constantly weaponised.

General recommendation:

1. To strengthen the fight against FIMI targeting LGBTIQ+, it is necessary to adopt a multi-stakeholder approach encompassing governments, international organisations, media, publishing houses and PR agencies, fact-checking organisations and academic research, and always to involve the LGBTIQ+ civil society groups.

Recommendations for policy makers, including governments and international organisations:

2. Support the development of regulatory frameworks protecting the LGBTIQ+ community, in partnership with civil society, academia and the private sector.
3. Train government officials, policy makers and media professionals on the complexity of issues facing the LGBTIQ+ community in the context of geopolitics, in order to equip them to identify and counter FIMI and disinformation, as well as to respond and communicate about it.
4. Establish dedicated tasking within government departments to monitor FIMI and disinformation campaigns targeting LGBTIQ+ communities.
5. Increase investment in media literacy, with a strong focus on digital media and human rights, including LGBTIQ+ rights and other identity-based rights.

6. Involve LGBTIQ+ communities from the early stages of the planning phase of the awareness raising campaigns, taking into account specific context and the risks that may result from further exposing LGBTIQ+ communities to attacks and sanctions.

Recommendations to the private sector:

7. Develop a common framework for moderating harmful content, particularly content targeting the LGBTIQ+ community, considering international differences in legislation.
8. Use algorithmic triggers to display educational pop-ups when users encounter potential disinformation, providing quick tips on how to evaluate information.
9. Remove harmful content, and block channels promoting online operations, as quickly as possible, by investing in content moderation and machine learning technologies.

Recommendations for civil society and academia:

10. Develop clearer and harmonised definitions of FIMI, LGBTIQ+ FIMI, disinformation, gendered disinformation, misinformation and malinformation.
11. Collaborate with social media platforms to develop frameworks and other solutions to improve content monitoring.

RESPONDING TO FIMI TARGETING LGBTIQ+

To address these challenges, the EEAS has been working with other European institutions, EU Member States and international partners, as well as civil society and private sector stakeholders, to improve the European Union's resources and capabilities to prevent, deter and respond to all types of FIMI, regardless of the source and the region where it occurs. The systematisation and analysis of the recommendations generated by this study followed the structure proposed by the FIMI Toolbox. The toolbox

consists of four main scopes: situational awareness, resilience building, disruption and regulation, and the role of EU External Action, divided into different types of specific responses. Through analysis provided by experts on gender, sexuality and LGBTIQ+ rights, the responses also seek to cover the specificities and cultural variations of the LGBTIQ+ community.

Figure 14: The Toolbox makes it possible to understand the different instruments that the EU and its partners have at their disposal to prevent, deter and respond to FIMI, and which instruments still need to be developed (EEAS, 2022).



For example, in countries where LGBTIQ+ rights and activism are curtailed, civil society organisations have insisted on the need to listen to local communities and their organisations before launching any public campaigns that could further expose LGBTIQ+ communities to attacks and sanctions. Responses also need to be adapted, as each country has its own linguistic communities, culture, and political movements.

This is an important point because, as noted in the academic literature and confirmed by case analysis, foreign actors engaged in FIMI have made efforts to adapt their Tactics, Techniques and Procedures (TTP) to the cultures and languages of the target countries. The detection and analysis of FIMI targeting LGBTIQ+ may also require an understanding of the specific cultural and linguistic aspects of the regions analysed, at the risk of producing analyses solely focused on dominant languages (e.g., English, French, Russian) and Westernised categories (e.g. gay, lesbian, LGBTIQ+) that do not always reflect the way this type of content circulates and resonates with people.

In countries where hate speech and hate crime legislation lacks protection for LGBTIQ+ people, there is a need for greater support for the adoption of a law aimed at protecting the community from violent and hateful behaviours. The law can provide legal mechanisms for LGBTIQ+ communities to deal with some of the effects of FIMI (when intentionally manipulated information leads to an increase in hate speech and hate crimes) and to raise awareness in society about issues such as discrimination, inequality and exclusion.

1. Situational awareness

For many stakeholders, the impact of FIMI and disinformation is symptomatic of a growing lack of trust in democratic institutions. At the same time, both have contributed to deepening the problem by fuelling social divisions, delegitimising the work of journalists and media companies, and increasing distrust in electoral processes. Consulted experts believe that currently available research does not sufficiently answer the questions raised by society on this issue. For example, how can we explain the similarities between narratives and tactics identified in different countries? Despite advances in methodological development for case detection, it is still unclear how these narratives and tactics “travel” between territories, languages and political contexts.

The data analysed seem to point to well-established official and unofficial communication channels that facilitate coordination between state and non-state actors located

in different territories. However, it is also possible that some of them are simply learning from each other via the Internet (e.g., from insertion into ecosystems of FIMI) or from the amplification of FIMI incidents by the mainstream media. It is precisely the complexity of these information networks that requires more analytical effort. Finally, given that FIMI tends to focus on contentious issues with great potential to divide society and engage people (e.g. LGBTIQ+ rights, especially trans rights and other gender issues, child protection and education, and reproductive rights), more research is still needed to understand specific types of FIMI and its impact both on communities with vulnerabilities and on the democratic process.

Recommended responses:

- **Develop clearer and harmonised definitions of FIMI, LGBTIQ+ FIMI, disinformation, gendered disinformation, misinformation and malinformation.** Without clear definitions, based on strong evidence, developed with the support of civil society organisations, internationally recognised and discussed by the academic community, it will be more difficult to develop efficient public policy. However, this work is largely dependent on increased funding for research activities in a context in which researchers and organisations working on gender equality and sexual and reproductive rights are under constant threat. The work of the EEAS can be a good start for this effort.
- **Develop a unified, multi-stakeholder approach that combines existing standardised methodologies and frameworks** while broadening their reach beyond specialised circles. This would require the concerted efforts of academia, civil society organisations, governments, international organisations and the private sector.
- **Foster permanent discussion forums to consolidate communities** of entities (private sector, academia, civil society) working together to counter FIMI in the context of LGBTIQ+: initiatives, such as the Disinformation Information Sharing and Analysis Center (ISAC) proposed by the EEAS, to exchange analytical frameworks and data to defend against digital information threats. The inclusion of organisations specialised in the analysis of LGBTIQ+ disinformation could lead to a more pluralistic representation of the topic.
- **Strengthen monitoring actions.** Establish dedicated units within government departments to monitor FIMI and disinformation campaigns targeting LGBTIQ+ people.

- Encourage use of **open-source data and analytical standards to enable civil society and the academic community to develop further research**. By encouraging the creation and use of open and standardised practices, authorities can ensure that different members of the community are able to produce interoperable knowledge that can subsequently inform decision-making and risk mitigation actions. It can also facilitate civil society's understanding of TTPs, behaviours, narratives, trends and the functioning of the actors' ecosystems involved in foreign interference activities.
- Promote the **exchange of data and information** between different members of the community **using data sharing standards**. Create a common database of cases and narratives targeting LGBTIQ+ people.
- Develop a streamlined **user interface that allows individuals to report suspected disinformation content for further review**. Media companies and social media platforms should enable users to report abuse and harmful content more easily. In addition, reporting channels and tools remain poorly publicised and accessible only to a more aware public. Empower local communities to engage in alert, reporting and awareness-raising activities against FIMI and disinformation.
- **Pool knowledge, so as to be ready to react**. The existing responses tend to be very reactive, addressing past incidents whose impact on society can only be partially mitigated. Based on data from previous research, authorities can try to anticipate trends. For example, Pride Month tends to register a high number of incidents related to the circulation of FIMI targeting the LGBTIQ+ community in many areas. An analysis of previous incidents can support the development of plans to raise awareness of this type of FIMI and to ensure the safety of citizens participating in these events.
- **Exchange first-hand information with victims of FIMI and disinformation**. This could help to develop protocols for handling incidents and encourage citizens to report cases to the authorities working to track and deter FIMI activities.
- Develop **high-quality research on different topics related to disinformation targeting LGBTIQ+** (media and digital literacy, monitoring technologies, analytical models or strategic communication). Researchers can also contribute to improving existing concepts and models.

By doing so, they can produce significant impacts on the analytical community in this field, on policymakers' work and on decision-making processes.

- **Increase funding for research on FIMI targeting the LGBTIQ+ community**. Stakeholders should have easier access to EU funding to develop projects to study and counter FIMI. Civil society organisations point out that these actions are largely dependent on a greater volume of funding, which is not always available in contexts where LGBTIQ+ movements are under attack from governments and opponents working with much more structure and resources.

2. Resilience building

The cases analysed in this report touch on some of the common patterns highlighted in the literature on disinformation and FIMI. Frequent patterns could be more easily identified if citizens had better critical resources to navigate the current media landscape. The experts consulted stressed the importance of media literacy as a long-term strategy to counter FIMI. This measure should cover the whole of society, but the focus on new generations needs to be considered. Children and teenagers are growing up in a new and complex information environment that combines disinformation, distrust of traditional media and wide access to mobile devices and social media platforms. Ensuring they can cope with these challenges means preparing the next generations to protect democracy. Educational measures could also raise awareness of gender and sexuality issues, addressing how FIMI and disinformation campaigns exploit contentious topics to attract audiences. Ensuring a strong and independent media market, committed to the democratic process and dismantling FIMI and disinformation, can also help build a society more resilient to FIMI threats. Several experts mentioned that adherence to disinformation and FIMI tends to increase when the media companies suffer attacks and sanctions from authoritarian governments. Another relevant element is the lack of funding for independent journalism and fact-checking. Finally, experts were cautious about restrictive measures such as the removal of television channels or media outlets identified as part of the FIMI ecosystem.

Moreover, preparing citizens to improve their ability to evaluate information sources is one of the key responses, preventing new incidents and filling historical gaps.

A good example of practice from civil society is the free online course on disinformation targeting the LGBTIQ+ community launched in 2023 by SOGI Campaigns. The

course consists of seven in-depth lessons, comprehension quizzes and case studies and can be accessed by anyone, from ordinary citizens to activists and industry professionals.

Recommended responses:

- **Provide trustworthy and legitimate information about the LGBTIQ+ community.**
- **Develop public campaigns to raise citizens' awareness** of the most common types of false narrative and TTPs on FIMI targeting LGBTIQ+.
- Use **regional networks** that act on the ground to exchange information with local LGBTIQ+ communities and other stakeholders. In doing so, these organisations can collaborate to strengthen existing transnational networks fighting FIMI. They can also raise the awareness of international partners, Member States and European institutions about threats involving FIMI targeting LGBTIQ+ communities abroad.
- **Take advantage of existing networks.** European and international LGBTIQ+ civil society organisations (as well as academics) already have their own networks. Instead of creating new networks, the existing ones can be included and improved with more resources and coordination.
- **Strategic media exposure and grounded actions.** In contexts and regions where LGBTIQ+ representation in the media is almost non-existent and LGBTIQ+ civil society organisations are mainly present in urban areas, increasing the presence and reach of LGBTIQ+ organisations in local media and communities can also contribute to changing deep-rooted prejudices. To reach a wider audience, activists can resort to traditional media such as radio and TV. These means of communication are still widely used by people who live far from urban centres and rapid technological changes. Journalistic programmes and entertainment TV shows can be considered strategic spaces in this sense.
- Continue supporting **campaigns on LGBTIQ+ rights in partnership with experts from academia and civil society.** Specific contexts require specific responses. This means that traditional public campaigns may not work in some countries. On the contrary, they may expose the LGBTIQ+ community to more risks. Authorities need to learn how to support by listening to those who understand the challenges faced by local communities.



SOGI CAMPAIGNS

[A global Resource and Training hub for creative campaigners](#)



Figure 15: SOGI Campaigns free online course

- **Capacity building on FIMI targeting LGBTIQ+.** Train government officials, policy makers and media professionals on the complexity of issues facing the LGBTIQ+ community in the context of geopolitics, so that they are better equipped to identify and counter the threat.
- **Invest in media literacy.** In addition to financially supporting projects in this area, governments and international institutions can work with civil society, academia and the private sector to help develop innovative solutions to reach different audiences and age groups. Several experts also highlighted the need to make media literacy a public policy and to include it in the school curriculum for children and teenagers.
- Offer a **“Learn More” option in search results or browser settings that directs users to resources on media literacy and disinformation identification.** In

addition to the flagging approach, platforms could redirect users to websites with reliable educational information in their languages.

- **Gamification.** Provide “Spot a fake” training (e.g. in the form of a game) for users of social media platforms on how to detect and deal with misleading and harmful content on the platform, including FIMI and disinformation targeting LGBTIQ+ communities.
- **Support independent journalism** to increase the supply of reliable, critical and high quality information. Considering that many citizens are now looking for “alternative” sources of information, it is relevant to raise the profile of media partners who can meet this demand responsibly. Independent journalism is a high-cost activity that requires solid funding and support from governments and civil society.
- **Encouraging media and journalism ethics.** Encouraging ethical reporting and responsible journalism can help prevent the spread of disinformation. Journalists’ adherence to deontological codes and standards can increase the credibility of news sources and so contribute to improving the information environment.
- **Support independent fact-checking projects.** Forms of support can include both training and funding. Fact-checking professionals must also be a relevant partner in forums and networks against FIMI and disinformation.
- **Improve communication on EU action to combat FIMI and disinformation.** Moreover, online platforms that have signed the Code of Conduct on Disinformation produce regular reports on the implementation of the Code. They could disseminate more actively the main findings of the reports on their own platforms, thereby raising awareness among users of their efforts to counter misleading content and making them more aware of the harmful content circulating in digital environments.
- **Improve communication on access to funding** for academic and civil society projects aimed at countering FIMI and disinformation on LGBTIQ+ issues. Some institutions already have specific funds for this purpose. However, several experts agree that researchers and activists are not always aware of them or how to access them. Governments and international organisations need to increase communication about their funding mechanisms. They can also raise awareness of the general funding landscape.

3. Disruption and regulation

Stakeholders can also enable actions to disrupt the spread of disinformation and propose regulations to counter immediate threats (killchain approach). On the one hand, several tech companies have implemented mechanisms to track and remove misleading content. These include algorithms to detect and limit the reach of disinformation, fact-checking partnerships, crowdsourced knowledge, and measures to remove or label this type of content. On the other hand, the EU’s Digital Services Act is now putting more responsibility on big social media platforms, while governments and regulatory bodies in several countries (both EU and non-EU) have introduced or proposed regulations to hold social media platforms accountable.

Experts highlighted several concerns on this topic, arguing that state and non-state actors spreading FIMI and disinformation are constantly adapting their tactics, making attempts at regulation quickly outdated. The same happens with disruption strategies, which should evolve rapidly to keep up with these changes. Finally, policy makers may face many challenges while trying to find a balance between regulation and the protection of fundamental rights such as freedom of expression and the right to access information. LGBTIQ+ civil society organisations have expressed concern that overly restrictive measures could backfire on local communities or even be appropriated by opponents of LGBTIQ+ rights. There is also growing concern about how the popularisation of artificial intelligence and deep fakes can enhance techniques to spread FIMI and disinformation about the LGBTIQ+ community.

Recommended responses:

- Support the **construction of legal or regulatory frameworks in partnership with civil society, academia and the private sector.** Evidence-based analysis, such as the cases analysed in this report, offers a variety of data on behaviours, TTPs and narratives targeting LGBTIQ+ that can serve as a basis for building future policy responses.
- **More research and information exchanges about existing international instruments to counter disinformation.** Organisations with prior expertise in this topic can contribute to exchanging good practices. The analysis of good practices and successful experiences, as well as the main milestones faced in different contexts, can contribute to improving the work of policymakers.

- **Work to strengthen institutions and the rule of law.** Legal processes and institutions are fundamental to ensuring that actions against FIMI and disinformation are consistent and fair, reducing the perception of bias in content moderation and regulation. They also enhance public trust in efforts to address this growing challenge.
- **Protection of fundamental rights in the digital space.** Governments should support regulation and compliance to guarantee a safer digital space. The EU's Digital Services Act (DSA) and Digital Market Act (DMA) are initiatives that can serve as a model for policymakers to propose regulatory responses in their respective regions.
- **Protect fundamental rights online and offline.** Actions considered illegal in an offline context must be treated the same way in an online environment. Equally, digital platforms should acknowledge that harmful content affects the integrity and dignity of citizens offline.
- **Protect human rights defenders.** In many countries, there are difficulties in ensuring legal mechanisms to protect those who fight for human rights. LGBTIQ+ activists working to counter FIMI and disinformation can be targets of various threats. They need to be better protected to keep democratically working for change.
- **Improve rapid and automated identification of harmful content.** One way to remove the workload from moderation teams would be to keep investing in machine learning systems. However, the cost of keeping this technology up to date is high. It requires constant training and updates to minimise errors and keep learning the new TTPs employed by FIMI perpetrators.
- **Remove harmful content and block websites promoting harmful content as quickly as possible.** By investing in content moderation and machine learning technologies, social media platforms can also respond more quickly to the spread of disinformation. In addition to removing this type of content, they can also make it less accessible to users by algorithmically controlling the flow of information that enters their information feeds. After sufficient verification, tech companies could also block websites that have been proven to disseminate disinformation, redirecting users to a page explaining the reason for the block.
- **Improve content moderation.** Social media platforms must adapt to a reality in which this activity will become more and more complex. It is necessary to increase investment in moderation teams and train them to deal with human rights issues, including topics related to gender and sexuality.
- **Develop a common framework for moderating harmful content,** particularly content targeting the LGBTIQ+ community. Stronger cooperation among platforms could enable the development of a common framework, in their Terms of Service, to define actions against harmful behaviours targeting the LGBTIQ+ community.
- **Labelling of content by state actors.** Regarding FIMI, one of the main difficulties is identifying that certain content comes from networks linked to state actors. By alerting users to the nature and origin of this content, social media platforms can help promote a critical reading of sources.
- **Algorithmic accountability and increased transparency:** Social media platforms should allow public authorities access to algorithms and allow users to know how content recommendation systems work. There is still a lot to be learned about how platforms work and, considering the threats to the democratic process, this should be made public. In addition, users should have the right to choose content options not only based on profiling.
- **Impact assessment of EU instruments** such as the DSA and the Code of Practice on Disinformation. By making the results of these assessments public, Member States and EU institutions can better influence the international community and strategic partners to adopt similar measures. A more harmonious regulatory landscape would benefit future transnational cooperation to counter FIMI.
- **Use algorithmic triggers to display educational pop-ups** when users encounter potential disinformation, providing quick tips on how to evaluate information. During the pandemic, some platforms flagged disinformation about COVID-19 vaccines, offering users the opportunity to access reliable information. Misleading content about the LGBTIQ+ community could also receive the same flagging approach.
- **Strengthen measures that reduce financial incentives for purveyors of disinformation.** By establishing partnerships, developing guidelines and proposing solid regulation of the advertising sector, authorities can prevent FIMI and disinformation from reaching specific audiences through targeted ads.

- **Impose financial and diplomatic sanctions** on countries and non-state entities (e.g. companies) found to be actively spreading FIMI and disinformation against the LGBTIQ+ community. This could encourage tech companies and other entities to find more effective ways to contain manipulation and interference by foreign actors. These sanctions could generate funds for new actions to counter FIMI and disinformation.
- **Imposing costs on perpetrators and their disinformation networks.** By cutting off transnational funding sources, local and international authorities can significantly reduce the work of perpetrators and its impact.

4. The role of EU external action

The EEAS has been a pioneering institution in countering FIMI, including disinformation, and promoting security and democracy. However, many stakeholders and potential partners are not aware of the role the EEAS can play. In this sense, some recommendations suggested throughout the research can contribute to taking external action further.

Recommended responses:

- **Increase and tailor diplomatic responses.** Use diplomatic negotiations to encourage countries to clamp down on FIMI and disinformation targeting LGBTIQ+ communities. However, these responses need to be designed with different political and social contexts in mind. For example, in regions where public debate on LGBTIQ+ is still a taboo, silent diplomacy approaches may be a better alternative to protect local LGBTIQ+ communities.
- **Strengthen diplomatic support.** Continue to provide technical and political support to authorities and civil society around the world. This type of action will help strategic partners to develop the same technical and political capacity to counter disinformation as is being developed in the EU.
- **Increase support for civil society organisations fighting for LGBTIQ+ rights.** By supporting these organisations, the EEAS can contribute to raising awareness, building resilience and advancing legislative measures protecting LGBTIQ+ communities. Strengthening the rights of the LGBTIQ+ groups in different regions can lead to a scenario of greater harmonisation of laws, making it easier for governments, diplomatic institutions and civil society to cooperate.
- **Establish a framework and best practices within the EU and partners on countering FIMI targeting the LGBTIQ+ community.** The EEAS's work in this field can provide resources for creating instruments that aim to facilitate coordinated work among different diplomatic and security institutions.
- **Deepen international partnerships to standardise regulations and approaches to combating FIMI and disinformation.** This includes coordinating with the EU institutions and Member States, as well as international bodies, to conduct joint operations to exchange knowledge about FIMI and disinformation targeting LGBTIQ+ communities. This work may also include the development of frameworks and processes to facilitate joint work among institutions with different expertise (e.g. human rights, foreign affairs, home affairs).
- **Communication and education.** The EEAS must improve the dissemination of its research findings. The perpetrators of online and offline FIMI campaigns, as well as the TTPs they use, should be consistently exposed. Educational campaigns can be an effective response if developed in partnership with stakeholders and adapted to specific political, social and cultural contexts.
- **Media literacy with a focus on digital media and human rights.** Continue to promote media literacy with a focus on digital media, also addressing patterns of FIMI and disinformation targeting discriminated communities.
- **Invest in more research.** In partnership with the private sector, academia and civil society, the EEAS must continue to invest in research to deepen understanding of FIMI attacking the LGBTIQ+ community and other forms of FIMI. Research should also focus on developing more innovative responses at the technical, policy, educational and analytical levels (e.g., new forms of strategic communication, storytelling, and re-discussion and refinement of concepts).

CONCLUSIONS

The FIMI case studies examined in this report illustrate some of the ways in which FIMI focuses on potentially existing vulnerabilities that create divisions within societies. The impact of FIMI contributes to a decline in trust in democratic processes, while also fuelling social divisions and undermining the work of journalists, security teams and civil society actors and trust in the platforms.

There remains an urgent need for more research on FIMI targeting LGBTIQ+ and its impact on local communities and the wider democratic process. Experts consulted in the course of this research also highlighted other questions, such as: how can we explain the similarities between narratives and TTPs identified in different countries? How do narratives “travel” between countries? And to what extent do state and non-state actors coordinate across territories to directly share their *modus operandi*?

The recommendations in this report are the beginning of a longer process. During this process, societies will need to come together to build consensus on key questions such as: How can a balance be struck between freedom of speech and the right to credible, factual information? To what extent should platforms restrict or moderate content on their sites? Should platforms be held accountable by governments if their moderation efforts fail to meet basic standards, and if so, how? How do we ensure that legislation is fit for purpose, implemented within a reasonable timeframe and not easily circumvented by FIMI threat actors? How do we, as democratic societies, balance the tension between upholding democratic values and allowing critics of those values to express their views freely?

There is also an emerging need to reframe the conversation around responses, from one in which countermeasures are portrayed as a threat to freedom of speech and the suppression of legitimate debate, to a better articulation of the desired end state, such as encouraging people to vote in an election, building trust in democratic processes, educating people about the bias and reliability of media sources, or the motivations of FIMI threat actors. To this end, the recommendations in this report highlight the need to continue to develop robust media literacy training for all and to ensure the continued viability of strong and independent journalism.

The recommendations also point to the role of platforms in disrupting the spread of FIMI. For this to be effective, stakeholders will need to overcome significant barriers, such as by agreeing to cooperate rather than compete, or investing in potentially expensive product features that improve information gathering and moderation efforts, but do not necessarily generate revenue. Any government regulation of social media platforms must also find ways to balance the need to ensure that platforms do not host or promote illegal or harmful content with the expectation of political neutrality in content moderation decisions.

Technology continues to evolve at a rapid pace. In response, democratic societies need to find ways to continue to articulate their values to their citizens, support strong independent media, allow all communities to voice their concerns while encouraging respectful debate, and reverse the erosion of public trust in democratic processes. Given a wide array of ways FIMI threat actors use to create narratives of division, we must seek innovative ways to communicate the values of democracy and the benefits of the freedoms and equal opportunities that democracy brings.

APPENDICES

APPENDIX 1: LIST OF ORGANISATIONS PARTICIPATING IN THE EXPERT DISCUSSIONS AND INTERVIEWS (31 AUGUST 2023 - BRUSSELS)

- Atlantic Council's Digital Forensic Research Lab (DFRLab)
- C-dev
- European Commission – DG COMM
- European Commission – DG CONNECT
- European Commission – DG JUST
- EL*C - Eurocentralasian Lesbian* Community
- EPF - European Parliamentary Forum for Sexual and Reproductive Rights
- European Parliament (EP)
- Forbidden Colours
- GENDERDOC-M Information Centre (Moldova)
- ILGA-Europe
- Media April / The Georgian Charter of Journalistic Ethics (Georgia)
- Media Development Foundation (Georgia)
- Oxford Internet Institute/International Panel on the Information Environment
- Pagella Politica/Facta (Italy)
- Stockholm University
- Tbilisi Pride (Georgia)
- Twitter / X
- Université libre de Bruxelles
- Uppsala Universitet

REFERENCES

TERMINOLOGY

Books and articles:

- Bardall, G. (2022). Nasty, Fake and Online: Distinguishing Gendered Disinformation and Violence Against Women in Politics. In *Gender and Security in Digital Space* (pp. 109-123). Routledge.
- Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122-139.
- Boghardt, T. (2009). Operation INFEKTION. *Studies in Intelligence*, 53(4), 1–24.
- Chebankova, E. (2012). Contemporary Russian Multiculturalism. *Post-Soviet Affairs*, 28(3), 319-345.
- Cheskin, A. (2017). Russian soft power in Ukraine: A structural perspective. *Communist and Post-Communist Studies*, 50(4), 277-287.
- Crilley, R., & Chatterje-Doody, P. N. (2020). Emotions and war on YouTube: Affective investments in RT's visual narratives of the conflict in Syria. *Cambridge Review of International Affairs*, 33(5), 713-733.
- Cushman, E. G. (2020). Eurosodom: Examining weaponized sexuality and gender-based narratives in Russian and pro-Russian disinformation [Doctoral Thesis, The University of Texas at Austin].
- Eady, G., Paskhalis, T., Zilinsky, J., Bonneau, R., Nagler, J., & Tucker, J. A. (2023). Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior. *Nature Communications*, 14(1), 62.
- Edenborg, E. (2020). Russia's spectacle of "traditional values": Rethinking the politics of visibility. *International Feminist Journal of Politics*, 22(1), 106-126.
- Edenborg, E. (2022). Disinformation and gendered boundarymaking: Nordic media audiences making sense of "Swedish decline". *Cooperation and Conflict*, 57(4), 496-515.
- Fallis, D. (2014). A functional analysis of disinformation. *I Conference 2014 Proceedings*.
- Gerbaudo, P. (2018). Social media and populism: an elective affinity?. *Media, culture & society*, 40(5), 745-753.
- Graff, A., & Korolczuk, E. (2022). Anti-gender politics in the populist moment. Taylor & Francis.
- Herrero-Diz, P., Pérez-Escolar, M., & Sánchez, J. F. P. (2020). Gender Disinformation: Analysing Hoaxes on Maldito Feminismo. *Icono 14* 18(2): 188–215. <https://doi.org/10.7195/ri14.v18i2.1509>.
- Innes, M., Innes, H., Roberts, C., Harmston, D., & Grinnell, D. (2021). The normalisation and domestication of digital disinformation: on the alignment and consequences of far-right and Russian State (dis) information operations and campaigns in Europe. *Journal of Cyber Policy*, 6(1), 31-49.
- Jarkovská, L. (2020). The European Union as a child molester: sex education on pro-Russian websites. *Sex Education*, 20(2), 138-153.
- Jones, T. (2020). Double-use of LGBT youth in propaganda. *Journal of LGBT Youth*, 17(4), 408-431.
- Keating, V. C., & Kaczmarek, K. (2019). Conservative soft power: liberal soft power bias and the "hidden" attraction of Russia. *Journal of International Relations and Development*, 22, 1-27.
- Korolczuk, E., & Graff, A. (2018). Gender as "Ebola from Brussels": The anticolonial frame and the rise of illiberal populism. *Signs: Journal of Women in Culture and Society*, 43(4), 797-821.
- Kuhar, R., & Paternotte, D. (Eds.). (2018). Campagnes anti-genre en Europe: des mobilisations contre l'égalité. *Presses universitaires de Lyon*.
- Lentin, A., & Titley, G. (2011). The crises of multiculturalism: Racism in a neoliberal age. *Bloomsbury Publishing*.
- Lovari, A. (2020). Spreading (dis) trust: Covid-19 misinformation and government intervention in Italy. *Media and Communication*, 8(2), 458-461.
- Luciani, L. (2021). Where the Personal is (Geo) Political: Performing Queer Visibility in Georgia in the Context of EU Association. *Problems of Post-Communism*, 1-12.
- Moskalenko, S., & Romanova, E. (2022). Deadly Disinformation: Viral Conspiracy Theories as a Radicalization Mechanism. *The Journal of Intelligence, Conflict, and Warfare*, 5(2), 129-153.
- Mršević, Z. (2013). Homophobia in Serbia and LGBT rights. *Southeastern Europe*, 37(1), 60-87.
- Myers, O. (2021). A Historical and Contextual Analysis of Soviet and Russian "Active Measures": How Russian Political Warfare Efforts in Foreign Presidential Elections Have Transformed in the Information Age. *University of Mississippi*.
- Paternotte, D. (2023). Victor Frankenstein and his creature: the many lives of 'gender ideology'. *International Review of Sociology*, 1-25.

- Prior, H. (2021). Digital populism and disinformation in post-truth times. *Communication & Society*, 34(4), 49-64.
- Rosińska, K. A. (2021). Disinformation in Poland: Thematic classification based on content analysis of fake news from 2019. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 15(4).
- Serrano, C. S. (2020). From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does International Law provide?. *SYbIL*, 129, 154.
- Shevtsova, M. (2020). Fighting “Gayropa”: Europeanization and instrumentalization of LGBTI rights in Ukrainian public debate. *Problems of Post-Communism*, 67(6), 500-510.
- Shu, K., Wang, S., Lee, D., & Liu, H. (2020). Disinformation, misinformation, and fake news in social media. *Cham: Springer International Publishing*.
- Strange, S. M. (2020). Speaking in stolen voices: Impersonated propaganda and use of Queer and Muslim identities by the Internet Research Agency [Unpublished monography, Simon Fraser University].
- Van Klinken, A., & Zebracki, M. (2016). Porn in church: moral geographies of homosexuality in Uganda. *Porn Studies*, 3(1), 89-92.
- Walker, A. S. (2019). Preparing students for the fight against false information with visual verification and open-source reporting. *Journalism & Mass Communication Educator*, 74(2), 227-239.
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking (Vol. 27, pp. 1-107). *Strasbourg: Council of Europe*.

Reports:

- Canada, the European External Action Service (EEAS), Germany, Slovakia, the United Kingdom, and the United States (2023). Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors. Available at: <https://www.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors/>
- GLAAD (2022). Social Media Safety Index. Available at: <https://sites.google.com/glaad.org/smsi/platform-scores>
- ILGA-Europe (2020). Annual Review of the Human Rights Situation of Lesbian, Gay, Bisexual, Trans and Intersex People in Europe and Central Asia 2020.
- Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. & Kaufmann, Z. (2023). Malign Creativity: How gender, sex, and lies are weaponized against women online. Wilson Center: Science and Technology Innovation Program.
- Marwick, A. E., & Lewis, R. (2017). Media manipulation and disinformation online. *Data&Society*.
- OSCE/ODIHR (2009). Hate Crime Laws: A practical guide. *OSCE Office for Democratic Institutions and Human Rights (ODIHR)*.
- Strand, C., & Svensson, J. (2021). Disinformation campaigns about LGBTI+ people in the EU and foreign influence. *European Parliament*.
- The European External Action Service – EEAS (2023). 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence. Available at: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

RECOMMENDATIONS TO RESPOND TO FIMI:

- European External Action Service. (2023). 2022 Report on EEAS Activities to Counter FIMI. EEAS. SG. Strategic Communication, Task Forces and Information Analysis Division (SG.STRAT.2).
- SOGI Campaigns. (2023). Fighting back disinformation campaigns. Online course and seminar. Sogi Campaigns.

ENDNOTES

- 1 <https://edmo.eu/2023/05/30/rights-in-the-time-of-conspiracies-and-fake-news-disinformation-against-lgbtq-in-the-eu/>
- 2 <https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/>
- 3 <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>
- 4 <https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720>
- 5 <https://disarmframework.herokuapp.com/>
- 6 <https://oasis-open.github.io/cti-documentation/stix/intro>
- 7 Recommendation CM/Rec(2022)16 of the Committee of Ministers to Member States on combating hate speech. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a67955
- 8 The concept of moral panics, proposed by Stanley Cohen in his book *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, in the early 1970s, has since been widely used in the social sciences. The original concept focuses more on the moral dimension of alarmist social reactions and does not define what "panic" is. More recent definitions, however, are much clearer. According to Ben-Yehuda (2008), the concept refers to "the creation of a situation in which *exaggerated fear* is manufactured about topics that are seen (or claimed) to have a moral component. Moral panics have to create, focus on and sustain powerfully persuasive images of folk devils that can serve as the heart of moral fears. Such imaginary and highly overstated fears have typically focused on gang activities, youth, illicit psychoactive drug usage, pornography, prostitution, and the satanic kidnapping of children."

