International School of Economics

Barlybaikyzy Zh.

Duisen A. T.

The EU Approach to Counter Foreign Digital Interference

Thesis submitted for

the degree of Bachelor in

6B03103 International Relations

Supervisor: Ikboljon Qoraboyev

Astana 2025

Abstract

The rising threat of foreign digital interference presented as a strategic and intentional use of digital tools, poses a significant threat to democratic principles. Threat actors are now able to interfere in another state's political processes, utilizing information manipulation techniques that may not be illegal by nature but are nonetheless harmful. These malicious activities can lead to substantial regional destabilization and disruptions. The European Union (EU) has emerged as a frontrunner in conceptualizing and institutionalizing countermeasures against these hybrid challenges. In particular, the joint efforts of the EU Commission's departments, particularly its diplomatic service, the European External Action Service (EEAS), have introduced proactive measures and frameworks aimed at fostering a common understanding of the danger and devising preventive measures. As part of this initiative, the EEAS has produced three comprehensive reports on the phenomenon of Foreign Information Manipulation and Interference (FIMI). This study examines the evolution of the EU's countermeasures, the exploration of its gradual progress in the articulation of key concepts, the institutional mechanisms, and the critical perspectives on the EU's approach. The study employs a thematic analysis of official policy documents, annual EEAS reports on FIMI, and academic literature to trace the shift from traditional cyber threats to complex, non-illegal forms of information manipulation. The findings outline the demand for ongoing enhancement of more punitive and systemic counter mechanisms stemming from the rapidly evolving state of FIMI, regardless of the EU's progress in building institutional resilience. The scrutiny concludes by reflecting on the implications of the EU's experience for other states, such as Kazakhstan, which face similar threats in this open information space.

Table of contents

Introduction

In recent years, a significant threat of foreign information interference has become an alarming concern affecting political processes across the globe. The actors can now more swiftly and intensely manipulate the information landscape of any targeted state. Such malicious interference is done through advertisements on social media, impersonated media outlets, and other deceitful audio-visual materials generated by Artificial Intelligence, among other tools.

The European Union, by establishing a structured framework known as Foreign Information Manipulation and Interference (FIMI) has taken a leading role in countering threats presented by the information landscape. For Kazakhstan, examining the experience of the EU could prove invaluable due to the presence of neighboring countries such as Russia and China, which are influential and active actors of FIMI. This situation necessitates Kazakh policymakers and academics to be mastered well in this topic.

The study begins by situating the issue within its broader context, tracing the historical and conceptual trajectory of cyber and digital threats. This then continues with the examination of EU policy sources and analysis of FIMI behaviors and techniques, with particular emphasis on the roles of Russia and China as key actors. Further, the overview of EU responses includes examination of institutional mechanisms, operational tools, and the official annual reports. The inquiry then shifts to the critical perspectives that scrutinizes the EU's approach by engaging with academic and policy critique. Finally, the discussion section synthesizes these findings, revisiting the broader implications of EU policy measures, the persistent challenges posed by the fluid and adaptive nature of FIMI, and the relevance of the EU's experience for other states, including Kazakhstan.

Context and Background

1. Early age of cyber challenges

With the rise of technologies capable of disrupting operational systems, and destroying and corrupting important data, namely viruses, the cyber attack landscape has been rapidly evolving. The 1990s brought more and more complex viruses to the world, including the famous Chernobyl virus, also known as the CIH virus, which had the capability of damaging the very computer hardware (Kovalchuk, 2024). This enormous potential for damage via such cyber attacks attracted many cyber criminals. Over the years, malware techniques have been enriched with new tactics such as worms, trojans, and rootkits (Kovalchuk, 2024). These new forms of malicious software became more sophisticated and difficult to detect. Rather than focusing solely on financial gain, many incidents of the 2000s took on political motivations, as evidenced by the notable Distributed Denial of Services (DDoS) attack on Estonia made by Russia in 2007 (Ottis, 2008). During these attacks, government portals, major banks, news outlets, and other critical infrastructures were under a series of attacks over a total of 22 days (Ottis, 2008). The discussion surrounding politically motivated cyber attacks must cover the following infamous cyber activities targeting Georgia in 2008, and the ongoing attacks on Ukraine that began in 2014 (Rashid et al., 2021). Later, these tactics have been employed to destabilise nations or to elect officials favourable to foreign actors. In this cyber landscape, Russia has been a predominant player, along with other state actors such as the US, China, India, Israel, and North Korea (Rashid et al., 2021). The similar trend of targeting high-profile infrastructures continued to be part of the well-known Stuxnet worm in 2010, which also has been used to target Iranian nuclear facilities. These types of attacks were seen as a cost-effective means of achieving political objectives without causing harm to innocent civilians (Farwell & Rohozinski, 2011). Conjointly,

these incidents could illustrate how cyber attacks have evolved from initial broad-brush and disruptive to becoming more intricate and financially incentivized by state actors (Falowo et al., 2024).

2. Evolution of cyber threats from hard threats to digital interference

The Falowo et al. analysis revealed that approximately 86% of DDoS attacks over the decade beginning in 2013 were directed at strategically significant high-profile infrastructures capable of disrupting or incapacitating entire state entities, which could result in substantial economic losses for the state (2024). The same longitudinal study found noticeable spikes in DDoS and malware incidents in 2020 and 2022. As suggested by the authors, the initial increase could be attributed to the increased online activity during the COVID-19 pandemic period, while the following surge in 2022 could be due to technological advancement and the resulting exposure of vulnerabilities (Falowo et al., 2024). Alongside the spike in 2022, the Falowo et al. study outlines a significant dip in 2023, which could suggest an improvement in defensive measures against cyber attacks or the shift towards other forms of cyber/digital threats (2024). Hence, many actors may shift to utilize digital information manipulation tactics due to their non-illegal but potentially harmful nature, which presents a significant threat to political processes while being less financially demanding compared to traditional cyber assaults. With this shift, the evolution of cyber threats can be traced from being overtly harmful and illegal to the emergence of a more fluid category of digital threats, which this study particularly characterizes as foreign digital interference. While the concept of propaganda and information manipulation is not novel, the ability to digitally distort reality through cyber dissemination techniques introduces an unfamiliar aspect to the recent threat (Van Niekerk, 2018).

3. Global reactions

Under these circumstances, the international community is expressing deep concerns about the rising digital challenges. Organizations, such as the United Nations and NATO, have been raising alarms about the growing complexity of digital threats, urging interstate cooperation and joint action to reinforce digital resilience at both national and global levels. The 78th session of the UN General Assembly adopted a resolution on the *Promotion and Protection of Human Rights in the context of digital technologies,* which called upon member states to combine efforts "to share expertise, knowledge, and effective practices in addressing disinformation" (A/RES/78/213). Moreover, the UN is currently on the go of developing the *Code of Conduct for Information Integrity on Digital Platforms,* aimed at establishing a normative "gold standard" for the responsible use of digital platforms to mitigate threats stemming from mis- and disinformation, and hate speech, for the safeguard of human rights (The United Nations, 2023). Meanwhile, NATO has also acknowledged the challenge of information threats, response measures of which include a multitemporal approach based on four key functions: Understand, Prevent, Contain and Mitigate, and Recover, as well as the establishment of a NATO Cyber Security Centre (NATO, 2025). The strong concern of the global community with digital and cyber threats showcases the recognition of the intensifying impact of the problem, with the potential to undermine core values of democracy and jeopardize security and digital space integrity.

Similar concerns regarding foreign digital interference are shared on a state's level. France, for instance, has established a dedicated department for vigilance and protection against foreign digital interference, called VIGINUM (SGDSN, 2022). As part of France's response measures, they publish reports aimed at refining definitions and detection mechanisms with the

help of multidisciplinary experts; the recent report focuses on a particular case of Romanian elections in 2024 (Ministry for Europe and Foreign Affairs, 2025). In 2018, Canada launched a similar initiative, known as the G7 Rapid Response Mechanism (G7 RRM), aiming to create common standardized tools to examine foreign information manipulation across the G7 (Canada, 2025). They also publish annual thematic reports starting from 2021. Comparable efforts are seen by the United States, exemplified by the State Department's R/FIMI office (Guo, 2025).

4. The EU as a frontrunner

The focus of the present thesis is precisely given to the European Union. The EU is widely regarded as a frontrunner in addressing foreign information manipulation and interference (FIMI), actively taking steps to confront the growing challenges since 2022. It is worth mentioning that the United States has also been using this specific term of FIMI; specifically, the State Department has established the R/FIMI office, which was reorganized from the initial Global Engagement Center at the end of 2024, though the office was eliminated in April 2025 (Guo, 2025). Nonetheless, the EU succeeded in coining and institutionalizing the term of FIMI first. In particular, the European External Action Service (EEAS) – the EU's diplomatic service and foreign policy and security arm – has taken a leading role in this matter. Ever since the first call in 2015 from the Member States to address emerging disinformation campaigns from Russia, the EEAS has fortified its abilities to detect and respond to disinformation and digital interference threats (EEAS, 2025). Since 2023, the EEAS, specifically the division of Strategic Communications, has been annually reporting on FIMI, taking a notable part in conducting thorough analyses of FIMI incidents, as well as developing a structured, holistic approach to building resilience.

Theoretical and Conceptual Frameworks

This section outlines the theoretical and conceptual frameworks of our research. The nature of the phenomenon of digital interference relates to efforts to shape actor preferences and it necessarily requires cooperation involving state and non-state actors. Liberal institutional theory constitutes the basis of our theoretical framework. This research aims to understand how the EU is addressing a specific type of digital threat - foreign digital interference, which it identifies as Foreign Information Manipulation and Interference. As it can be seen, conceptual understanding is an essential part of our research. Hence, this section also articulates the conceptual framework of our work.

1. Theoretical framework

Outlining a theoretical framework is important in managing a large amount of information by excluding irrelevant data and, depending on the theory, articulating the perspective of the international system. The domain of International Relations (IR) highlights, though not limits to, the perspectives of three predominant classical schools of thought, namely realism, liberalism, and constructivism. Building on the historical patterns, major IR theories offer well-grounded explanations of global affairs dynamics. The establishment of dominant IR theories dates back centuries, and to avoid obsolescence and maintain their relevance, the theories adapt to ever-changing global conditions, incorporating new elements into the paradigm. Therefore, it is worth mentioning that the focus of the analysis is precisely given to the revised version of classical liberalism - liberal institutionalism.

The main tenet of liberal institutionalism suggests that the way towards peace, economic growth, and cooperation lies within global governance, seeing both domestic and international institutions as mediators and the main forces in the international system. (Baylis, 2008). Liberal

institutionalists argue that prosperity can be achieved through the so-called 'integrated communities' (Baylis, 2008). The idea of 'integrated communities' derives from the opportunity cost of independent states giving up some sovereignty in favor of shared goals. (Baylis, 2008) The EU is a primary example of a sui generis entity and integrated regional community, demonstrating that stability and progress can be achieved through institutional action, multilateral cooperation, and interconnectedness.

In this sense, the member states appear to be prioritizing an institutional approach in countering foreign interference. The EU's reliance on bodies, such as the EEAS, in managing digital challenges demonstrates its assertiveness in institution-based resilience. The EEAS in its reports heavily recommends and stands for a collaborative and "whole-of-society approach to tackling FIMI", which reflects hallmarks of liberal institutionalist thinking. (EEAS, 2023).

2. Conceptual framework

Due to the fluidic nature of the concepts, applying a conceptual framework is critical in this research in order to eliminate inappropriate interpretations and assumptions about the definitions and concepts. It is worth clarifying that this study focuses on the specific category of challenges rather than all digital challenges. Cyber threats present a wide range of misuse of digital technologies, including Artificial Intelligence (AI) risks, cyber attacks, malware, disinformation, etc. However, the major aspect of the work is centered around the concept of foreign digital *interference* and *information manipulation*. As stated in the second EEAS report, FIMI has a "stronger socio-cognitive component" which distinguishes it from the "technical dimension" of cyber (EEAS, 2024). This means that the previously described in the context and background section cyber-related domain is out of the scope of this analysis when referring to digital threats and/or digital challenges.

The study utilizes concepts that may have similar meanings to each other, however, it is important to differentiate between them. Therefore, within the framework of this research, *foreign digital interference* is described as an umbrella term that refers to any malicious use of digital tools, platforms, or technologies by foreign actors to interfere in another state's internal affairs. At the same time, *Foreign Information Manipulation and Interference (FIMI)* solely refers to the concept developed and used by the EEAS. According to the glossary from the EEAS reports, FIMI is identified by its

> "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, by state or non-state actors, including their proxies inside and outside of their own territory"
>
> (EEAS, 2025).

Thus, the theoretical and conceptual frameworks inform the readers of the study's boundaries, limiting it to the EU's institutional responses to the specific challenge of foreign information manipulation and interference.

Methodology

The research adopts an exploratory method, aiming to examine the new concept of foreign digital interference. Although the underlying phenomenon itself that the concept describes, such as disinformation, interference, and propaganda coming from foreign actors, has been a topic of public discourse for years, its current form as FIMI in the EU's official articulation is of very recent origin, as it has been in institutional use only since 2022. The type of 'prestudy' allows researchers to conduct a tentative analysis on emerging matters, helping to generalize an understanding of it. This method is particularly suitable for topics that are

understudied and require further exploration (Swedberg, 2020). This is due to the fact that standard methodologies may prove impractical for examining emerging subject matters, as existing literature may not provide the necessary information needed for conducting traditional procedures. Given the study's focus, quite an unprecedented foreign digital interference concept, an exploratory method is found to be appropriate to be guided for this research.

The core of our scrutiny is the three comprehensive EEAS reports that are particularly focused on the FIMI concept. These reports conjointly offer a substantial amount of data, documenting all FIMI incidents from the end of 2022 to the end of 2024, with the most recent third report being published on March 19, 2025 (see Annex). The average length of each report is 39 pages. Primarily, these documents conceptualized FIMI, familiarizing the EU with it and facilitating its detection. Late efforts were centered on the development of the analytical tool called the FIMI Exposure Matrix. While predominantly working with these three reports, it is worth being aware of how EU institutions function. Each body represents different stakeholders: the EU Council reflects member states' interests, the Commission represents the EU as an organisation, and the Parliament speaks on behalf of the EU populace. We recognize that the EEAS, as part of the EU Commission, expresses the viewpoint of the EU as an organization. Due to the interconnected character of all EU institutions, this study will include relevant reports produced by these institutions. Beyond these official reports, our analysis incorporates academic literature that raises critical questions relevant to our study. The existing body of literature primarily focuses on assessing the effectiveness of EU policy measures, which allows us to employ a literature review method to identify recurring themes.

Thematic analysis will serve as a guiding framework for our study, enabling us to work with all the collected data effectively. One of the primary advantages of this method is its

flexibility, which is essential for exploring the dynamic topic of foreign digital interference. Its purpose extends beyond merely summarizing the data, as it seeks to analytically trace thematic pathways, allowing researchers to recognize overlapping pieces of information (Clarke & Braun, 2016). In particular, the study employs an inductive thematic analysis, where data is gathered from specific pieces of content—reports, in our case—to then derive broader generalizations (Alhojailan, 2012). Such a method enables researchers to keep all themes effectively connected to the available data. Hence, this method will be most relevant for our investigation due to the emergent nature of the subject, which requires initial exploration and explanation of the various information at hand. This brings us to the final stage of our study: interpretations. Owing to the flexible nature of the inductive analysis, there is a need for precise framings and explanations of main findings, and this is where interpretations become essential in any qualitative research (Alhojailan, 2012). Thus, the interpretative qualitative analysis, as the concluding subsection, will assist us in explaining and generalising the analytical observations made in the earlier stages. The discussion section will encapsulate all findings with interpretations of the main thematic patterns observed across annual reports and academic literature.

Main findings

1. Conceptual clarity: A necessary element for designing the EU response to digital threats

While the very nature of foreign interference is far from being recent, such processes as globalization and digitization transform the dynamic in which it operates in the most groundbreaking ways (Dowling, 2021). The fluidity, along with the ever-changing character of the realm, challenges the EU with the development process of a singular understanding of what it is and how it should be addressed. Berzina and Soula (2020) brought to attention the conceptual

issue of foreign interference, arguing that defining it comes with the risk of either being too broad, which might reflect on right-restrictive implications, or too narrow to cover specific and newly emerging forms of interference, hindering the effectiveness of the resilience. Authors also highlighted the lack of a unified consensus and clarity on the definitions within the Union and institutions, which might complicate and prolong the efforts of policymakers in establishing laws against the threat. (Berzina and Soula, 2020). Likewise, scholar James Pamment (2020) believed that the ambiguity in the definitions comes between a forceful defense, stating that "the EU and many of its affiliated bodies should adopt commonly held terms for discussing the challenges they face".

The uncertainty in the definitions can be seen in several examples. For instance, "disinformation" can often be used as a catchall term, creating confusion between different degrees of interference. Both Pamment and the EEAS distinguish between "disinformation" and "misinformation", highlighting that each presents a different problem that requires tailored approaches in terms of their effectiveness and suitability (EEAS, 2023). To more clearly understand their difference, the former refers to "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm", as stated in the first report (EEAS, 2023). Misinformation, on the other hand, is referred to as "false or misleading information shared without harmful intent, though the effects can be still harmful" (EEAS, 2023). Below, Table 1 illustrates key comparative characteristics between the definitions of "disinformation" and "misinformation" based on the EEAS's utterance. Thus, setting clarity in terms of intent and deliberateness is crucial when applying policy measures to align with the corresponding responsibilities of actions.

Feature	Disinformation	Misinformation
Nature of content	Verifiably false, misleading information	False, misleading, outdated information
Intent	Shared with the intent to manipulate the information environment and deceive the public	Shared without harmful intent; may result from ignorance or error
Spread	Deliberately coordinated spread (bots, inauthentic accounts)	Uncoordinated, accidental spread
Potential harm/ effect	Designed to cause harm (election interference, social division, threat to democratic political processes)	May have harmful effects, though with no intent (public confusion, weakened public trust)

Table 1. Comparative Characteristics of Disinformation and Misinformation. *Prepared by the authors based on EEAS reports.*

Similar logic can be attributed to the difference between terms of "interference" and "influence". The term "interference" by its definition implies one's unwanted involvement in the situation, carries a more negative connotation, and "should not be used to describe benevolent, benign, or neutral nation-state activity beyond its borders". (Berzina and Soula, 2020). The negative undertone of describing interference is often followed by additional adjectives, such as "malicious", "malign", "manipulative", and is especially noticed in the institutional discourse of the EU (Fridman, 2024). "Influence", on the other hand, "encompasses any type of interaction between two political actors – whether it is honest cooperation based on shared democratic values, or an act of war" (Fridman, 2024). This way, interference constitutes a part of a broader definition of influence and can be characterized by the perception of one's national power as conflicting with existing values and standards. (Fridman, 2024).

The fluidity of the foreign digital interference phenomenon is also evidenced by the EU's description of it as existing in a "gray zone/area" and being "non-illegal". This suggests activities that stay tolerated and do not cross the border of being explicitly unlawful yet still can pose a threat to political systems, undermine core values, and cause public harm. The specific articulation of foreign interference as being "non-illegal" behavior instead of just "illegal"

covertly implies the existence of a blurred line between foreign influence and illegitimate manipulation in which the phenomenon operates (Ördén and Pamment, 2021).

1.1. Gradual articulation of the concepts of foreign interference and information manipulation

Given the mentioned nuances in establishing the approach towards conceptualization, the EU has undergone significant changes in how it describes and defines the threat it faces. The issue first entered the EU's political agenda and discourse in 2015, after the geopolitical shifts triggered by the annexation of Crimea. At the time, the terms "disinformation", "disinformation campaigns", and "propaganda" were most noticeable in the EU's official language to describe the ongoing events and address the problem, early references of which can be seen in the European Council conclusions of 2015 (European Council, 2015). For this reason, the communication team of East Strategic Communication Task Force, also known as EUvsDisinfo, was established by the EEAS, dedicated and targeted to fight specifically against the disinformation threats and propaganda coming from the eastern great power neighbour. (EUvsDisinfo, n.d.). Yet, the earliest observed detailed definition of disinformation was provided only in 2018 from the report by the Commission's High Level Expert Group (HLEG) on Fake News and Online Disinformation. According to their articulation, disinformation is referred to as "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit" (European Commission, 2018a). The report clearly stated the boundaries within which the term applies, excluding already illegal by the regulatory remedies online content, and deliberate but not misleading content, such as satires and parodies. (European Commission, 2018a). The same year, the definition was further elaborated by the European Commission's Communication, defining it as "verifiably false or misleading information that is created,

presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm" (European Commission, 2018b). The Commission's interpretation of disinformation also "does not include reporting errors, satire and parody, or clearly identified partisan news and commentary" (European Commission, 2018b).

The EU's vocabulary continued to expand as the digital realm evolved, and in 2016 the concept "hybrid threats" emerged in the official language of the Commission, which encompasses a mixture of conventional and unconventional methods, such as cyberattacks, terrorism, disinformation etc, is used by state or non-state actors, includes coordinated, coercive and subversive behavior, pursues strategic goals while avoiding the triggering of a formal warfare (European Commission, 2016). This expansion of the concept beyond just disinformation can be explained by the need to adopt and respond to new and more sophisticated forms of danger, since the previous understanding no longer captures the scale and complexity.

However, the scope of the concept was then depicted as too broad to identify what exactly constitutes the malignant activity. For some time, the EU continued to utilize "disinformation" and "hybrid threats", which can be noticed in the 2018 Action Plan against Disinformation, until in 2020 the Commission in its European Democracy Action Plan (EDAP) introduced the concepts of "foreign interference in the information space" and "information influence operation". According to the document, foreign interference is "often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents". (European Commission, 2020). Whereas, information influence operation refers to "coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in

combination with disinformation." (European Commission, 2020). This shift toward a more precise understanding is not just semantic, but is a reflection of the EU's consolidation in its efforts to define and address the problem.

1.2. FIMI as the cornerstone of the EU toolbox to address foreign interference in the field of information space

As a part of attempting to set clear definitions, the EEAS in 2022 established the conceptual notion of what is now classified as foreign information manipulation and interference, or FIMI. The earliest institutional formulation of the concept as foreign information manipulation and interference appeared in March 2022 with the adoption by the EEAS of a long-term roadmap - the Strategic Compass for the Security and Defense. However, the document did not provide any definitions, but rather explained further actions for countermeasures to the threat. In February next year, the EEAS released its first report on FIMI, which was deliberately structured to provide a conceptual basis for the term.

As previously discussed in the conceptual framework, the definition of FIMI by the EEAS suggests non-illegal, manipulative, intentional, and coordinated activities by foreign state or non-state actors, aiming to undermine values, procedures, and political processes. (EEAS, 2023). The report suggested that the ABCDE framework, introduced by Pamment (2020), can serve as a criteria methodology for policymakers to distinguish between similar terms, assess, report, and design protective measures. Comprising five key components—Actor, Behavior, Content, Degree, and Effect—the framework deconstructs the problem into smaller elements, enabling a more comprehensive and structured approach to combat FIMI (EEAS, 2023). The ABCDE framework allows to more precisely define the involvement of a particular behavior to FIMI: whether the actor is of foreign or domestic origin, whether the behavior is coordinated and

followed by malicious intent, the type of content that is being disseminated, its reach, and political and societal effect (EEAS, 2023). Drawing on these criteria, it becomes possible to determine whether the actions observed can be qualified as attributed to FIMI.

2. Sources of the EU policy

Back in 2015, following the increased concern about Russia's disinformation campaigns on the Crimea annexation matter, the European Council conclusions highlighted the urgent need to challenge the growing problem, marking its very first steps in addressing the hybrid threat by establishing a communication team. (European Council, 2015). Consequently, the EUvsDisinfo was created as a flagship project of the EU's diplomatic service (EEAS), aiming to address, respond, and raise awareness of the information manipulation operations stemming from the Kremlin (EUvsDisinfo, n.d.).

Presented at the end of 2020, the European Commission introduced its European Democracy Action Plan, aimed at confronting challenges undermining democratic systems and building resilience among citizens (European Commission, 2020). The Action Plan laid out measures based on three pillars, one of them being *Countering Disinformation.* In particular, listed actions to countering disinformation included two key to this section points: (1) to "develop the EU toolbox for countering foreign interference and influence operations"; and (2) to "develop a common framework and methodology for collecting systematic evidence on foreign interference" (European Commission, 2020). Following as a response, in 2022, the EEAS published a Strategic Compass for Security and Defence that "sets out concrete actions - with clear deadlines to measure progress" (EEAS, 2022). By the year of 2030, the ambitious plan for strengthening the EU's security and defence policy demonstrated a commitment to four work strands: Act, Secure, Invest, Partner. As it was called for in the European Democracy Action

Plan, the diplomatic service's Strategic Compass devotion, as part of the *Secure* strand, to "develop the EU toolbox to address and counter foreign information manipulation and interference", served as a soil for the establishment of the counter-mechanism in the form of the EEAS FIMI reports (EEAS, 2022).

2.1 Thematic analysis of the EEAS reports

The EEAS evidence-based reports serve as a blueprint for the so-called "*defender community"* - a wide range of diverse actors who try to unfold the nature of FIMI, identify its common trends, and build appropriate measures to counter it (EEAS, 2023). This section examines all three existing reports at this moment, tracing through the evolution points and providing an overview of their key elements, differences, and thematic overlaps.

Table 2. Comparative analysis of the EEAS reports on FIMI.

Aspect	1st report (2023)	2nd report (2024)	3rd report (2025)
Scope	100 incidents	750 incidents	505 incidents
Threat origin countries	Russia, China	Russia, China, Iran	Russia, China
Key targets	Ukraine, EU, US	Ukraine, EU, NATO, NGOs	Ukraine, France, Germany, Africa, global events
Tactics, Techniques, Practices (TTPs)	Impersonation, images, multilingual ops	AI/deep fakes, election interference, networked campaigns	Bot networks, AI, inauthentic news, coordinated inauthentic behavior
Frameworks	Kill chain, DISARM, STIX	Four-phase response, FIMI-ISAC, election protocols	FIMI Exposure Matrix, network analysis
Response	Conceptual, foundation-laying	Standardized, operationalized	Regulatory, punitive, coordinated with allies

Table 2. Comparative analysis of the EEAS reports on FIMI. *Prepared by the authors based on EEAS reports.*

Table 1 demonstrates a comparative outlook of the three available report editions, divided into several categories: the scope of the FIMI, their main actors and targets, key tactics, techniques, and practices (TTPs) implemented, frameworks, and character of responsive measures introduced by the EEAS.

Over the period from 2023 to 2025, the reports have shown a clear advancement in the EU's approach to countering FIMI, building upon each other through a constructive dialogue and incrementally refining the understanding and proposed countermeasures to the threat. The advancement reflects both the sophistication of threat actors' TTPs and the institutional maturation of responses. For instance, serving as a pilot project, the first report laid a foundation for the defender community, sampling 100 FIMI incidents from late 2022, analyzing adversarial behavior and introducing conceptual frameworks, such as DISARM, Kill Chain, and STIX, which will be later detailed in the EU responses section. Whereas the latest report of 2025 demonstrates vivid progression, significantly expanding the scale of detected incidents, operationalizing the frameworks and moving towards regulatory and punitive measures, such as sanctions imposing and predictive infrastructure mapping through the introduced FIMI Exposure Matrix. Nevertheless, all three reports meet in identifying China and, in particular, Russia, as the primary FIMI actors, and Ukraine as the continuous target.

2.2. Challenges faced by the EU

First and foremost, democracy stands at the heart of the EU's values, along with the rule of law and fundamental human rights (European Commission, 2020). Both the global community and the EU are deeply disturbed by the threat that disinformation and information manipulation pose to democratic societies. Democracy significantly relies on a free and open digital environment, places a strong value for information integrity, and upholds freedom of expression (European Commission, 2020). However, the very freedoms of expression and open information space are now being misused by foreign actors for public opinion manipulation and reality distortion, increasing the risks of society destabilization and fueling polarization. Over the last decade, the EU has reportedly been facing multiple ongoing disinformation campaigns of

pro-Kremlin views. As mentioned earlier, the starting point of such deliberate and coordinated spread of falsifiable information can be traced back to the events of 2014, in particular, Russia's annexation of the Crimean peninsula. Ever since, the EU has been actively making efforts to address the issue and protect the core values the Union strongly commits to.

At the same time, misuse of open information space and freedom of speech comes with implications for the backbone of democracy - free and fair electoral processes. The earlier and most prominent incident of foreign digital interference dates back to the U.S. Presidential elections in 2016. The case was reported by the U.S. Intelligence Community Assessment (ICA), which confirmed Russia's involvement in its elections influence campaign through the government-supported troll farm - Internet Research Agency (Office of the Director of National Intelligence, 2017). This incident served as a wake-up call for liberal democracies, especially for the EU, which became "keenly sensitive to any extra-regional entities attempting to influence unrest and poll interference" (Petek, 2025).

The first notable case of foreign digital interference within the borders of EU member states can be linked to the final round of the 2017 Presidential elections in France. The operation aimed at Presidential candidate Emmanuel Macron resulted in the so-called "Macron Leaks", where a large-scale of stolen internal campaign data, combined with real and altered emails and documents of Macron's team, were released online (Conley and Jeangène Vilmer, 2018). French scholar Jean-Baptiste Jeangène Vilmer in his detailed report claims that the operation had three distinct dimensions, notably, the disinformation campaign, the hack, and the leak, where no single actor was behind. However, the two main sources of the anti-Macron propaganda were attributed to the Kremlin media (Russia Today and Sputnik) and the American alt-right (Jeangène Vilmer, 2019). The aftermath of the incident led to the adoption of the EU initiatives,

such as the Action Plan against Disinformation in 2018, which addressed concerns for the upcoming 2019 European Parliament elections, and called for response actions to strengthen resilience towards disinformation. (EEAS, 2018).

Despite the efforts to combat the threat, instances of foreign digital interference continued to occur. One of the most recent cases involved the Romanian 2024-2025 Presidential elections, which resulted in the annulment of the first round of elections due to accusations of flawed electoral processes. The pro-Russian candidate, Călin Georgescu, became a frontrunner in the votes "due to a complex strategy of information manipulation" (Stanescu, 2024). Later revealed by the Supreme Court of National Defense (CSAT), vote rigging and sophisticated illegal media campaigns were backed by Russian financial support to foster societal division. (Stanescu, 2024).

The latest EEAS report of 2025 exposed elements of long-term operations, such as Doppelgänger, Portal Kombat, False Façade, and the African Initiative, which altogether constitute a part of a vast and sophisticated FIMI ecosystem. The campaigns are primarily attributed to Russia, where each is aimed at expanding the Russian narrative, discrediting Ukraine, interfering in Western politics, and undermining democracy, using tactics such as impersonation and paid influencer promotion. (EEAS, 2025).

2.3. Evolution of FIMI behaviors and techniques

This section will explore the evolution of FIMI based on the annual reports published by the EEAS. Prior to deeper examination, it is first important to clarify the term of Tactics, Techniques and Procedures, as specifically articulated by the EEAS:

> *TTP(s) In the context of FIMI, "Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. "Tactics" are the operational goals that threat actors are trying to accomplish. "Techniques" are actions through which they try to accomplish them. "Procedures" are the specific combination of*

techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.

(EEAS, 2023)

The distinction between illegal cyber attacks and malicious FIMI activities will become clearer as we delve into exploring the exact techniques and procedures involved.

TTPs Category	2023 EEAS Report	2024 EEAS Report	2025 EEAS Report
Impersonation	Mimicking trusted media outlets	Sophisticated impersonation of individuals and organizations	Fake news ecosystems with 124 incidents recorded
Bot networks	No mention	No mention	Often disposable botnets across 38,000+ channels
Coordinated Inauthentic Behavior (CIB)	Cross-posting among inauthentic accounts	Systematic cross-platform campaigns	Systematic cross-platform campaigns
Localization	30 languages used	Still present, but was not explicitly discussed	349 incidents of tailored messages via local references
Artificial Intelligence	Image/video manipulation	Deepfakes	41 cases of deepfakes and other AI manipulations
Election interference	No mention	Infrastructure preparation, information laundering, CIB (Spain, Poland, 2023 elections)	42 cases detected during 2024 European Elections
Content formats	Images, videos, memes, infographics, and articles	Video campaigns, manipulated speeches	AI audio, deepfake video, and fake websites
Evasion	Use of diplomatic channels and limited encryption	Use of encrypted messaging apps (Telegram)	Disposable CIB accounts
Notable examples (see Annex)	Impersonated media outlets, such as, the French Charlie Hebdo, German Titanic and Spanish El Jueves	Polish and Spanish election interferences	FIMI operations such as the Doppelgänger, Portal Kombat and other campaigns targeting key events in 2024

Table 3. Tactics, Techniques, and Procedures (TTPs) trends by category in EEAS reports.
Prepared by the authors based on EEAS reports.

Table 2 shows that in the EEAS's debut report on FIMI, it was identified that the most prevalent content formats were image/video-based, with minimal use of articles on impersonated media outlets (EEAS, 2023). To deliver fabricated content, actors relied on cross-posting content on different social media platforms. Markedly, Russia frequently employed official communication channels (76 channels out of 207) such as diplomatic service accounts (EEAS, 2023). This tendency could be attributed to the sanctioning of popular state-controlled channels within the EU. Moreover, since the end of 2022, FIMI actors have been mindful of localizing

content, with the first report revealing the use of 30 languages across 100 incidents (EEAS, 2023). These outlined two primary objectives of TTPs are to distract and distort, especially when covering topics of “Russian invasion of Ukraine” and “Energy crisis” (EEAS, 2023).

In the following report, there is a traced trend of increased FIMI attacks directed at different European and international organizations, along with non-political individuals. Media organizations were likely to be targeted through sophisticated impersonation techniques that add credibility to inauthentic content. There is also one predominant technique that was given a name in this report. The Coordinated Inauthentic Behavior (CIB) describes the use of networks of accounts to spread particular messages across various platforms while concealing their true nature (EEAS, 2025). Although this term was introduced in the glossary of the last third report, this technique has been consistent across all three reports. The application of enhanced AI tools was noticed in several FIMI cases, particularly Deepfake technology, which is usually employed to create manipulated videos for the impersonation of some individuals. However, the EEAS claims that the use of AI in 2023 showcases an evolution rather than a revolution (EEAS, 2024).

The latest report has outlined the significant trend in enhanced localization techniques, with recorded 349 occurrences in 2024. This technique of maliciously tailoring content to align with the target audience's habits and context builds up credibility. Tailoring information manipulation to specific historical and cultural contexts has now been integrated into the existing toolkit that was previously predominantly utilizing local languages. This shift was also accompanied with lessened Western support for Ukraine (EEAS, 2025). Additionally, there has been an increase in the use of disposable botnets, with CIB accounting for 73% of all recorded channels. This can be confidently stated that CIB has become a prominent aspect of FIMI activities, continuously evolving to be more and more systemic. While AI usage is gradually

rising, it still constitutes a relatively small part of all FIMI activity and is usually applied for the creation of Deepfake audio and video content (EEAS, 2025).

Cross-platform coordination, a simultaneous use of different platforms, is found to be a recurring technique, with the first explicit identification of it in the second report as the "default modus operandi" (EEAS, 2024). This character has been persistent in the last report, illustrating the distribution of channels across various social media platforms (EEAS, 2025). Certain platforms are often utilized due to the possibility to easily create disposable accounts or, depending on the target audience's preferences, particular platforms can dominate in specific FIMI incidents, as evidenced by the predominant use of Facebook in targeting African countries (EEAS, 2025). This also points to another significant characteristic that has evolved over time: content adaptability and formatting. These advancements may imply a progression in the strategic planning of FIMI, increasing sophistication, thereby increasing the perceived trustworthiness.

Overall, the foundation of the TTPs remains consistent, and the rise in usage of AI has enabled actors to scale their activities significantly. However, as it has been noted by the EEAS, AI has also a potential to benefit the defender community as well as the attackers (EEAS, 2024). The general pace of evolution is rapid, with increased reach of FIMI attacks onto other states such as the Middle East, Asia, and African countries. This gradual yet progressive sophistication helps actors to achieve their objectives more effectively, necessitating an enhancement in defence mechanisms.

2.4. Key actors: Russia and China

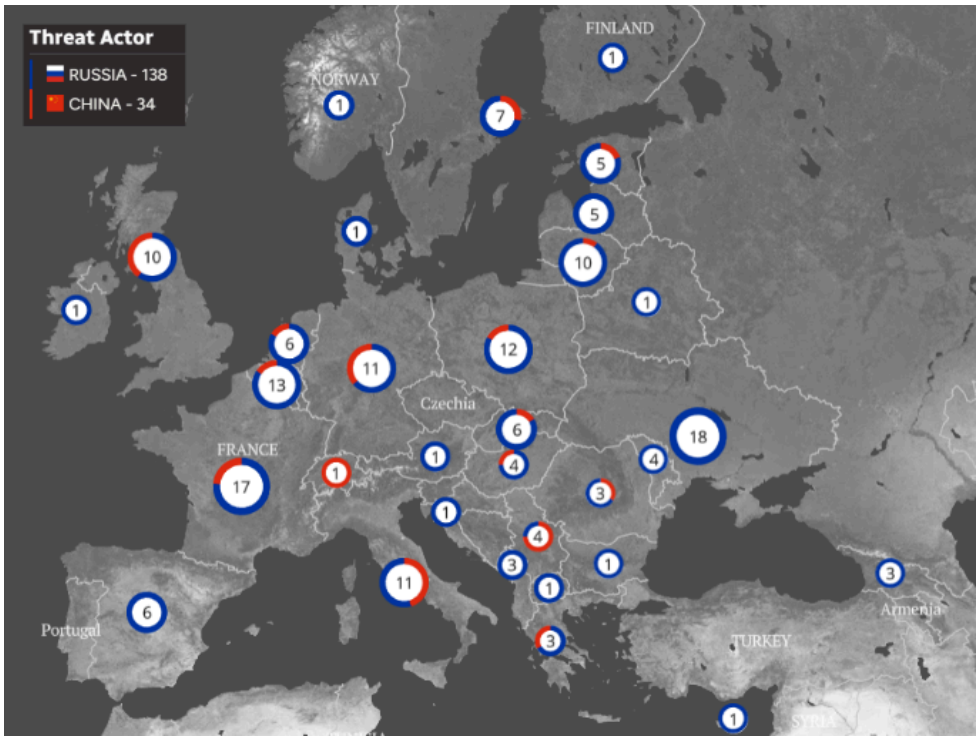


Figure 1. The number of foreign information manipulation incidents in Europe from 2014 to 2025

Source: *Authoritarian Interference Tracker; The Alliance for Securing Democracy.*

As mentioned earlier, the EEAS reports underscore that the origin of foreign digital interference primarily comes from two state actors - Russia and China, with the first being more frequent. Figure 1 below illustrates the distribution and intensity of foreign information manipulation across the European mainland between 2014 and 2025, with a total number of 172 incidents, 138 of which are attributed to Russia and 34 to China, based on the data provided by the Authoritarian Interference Tracker.

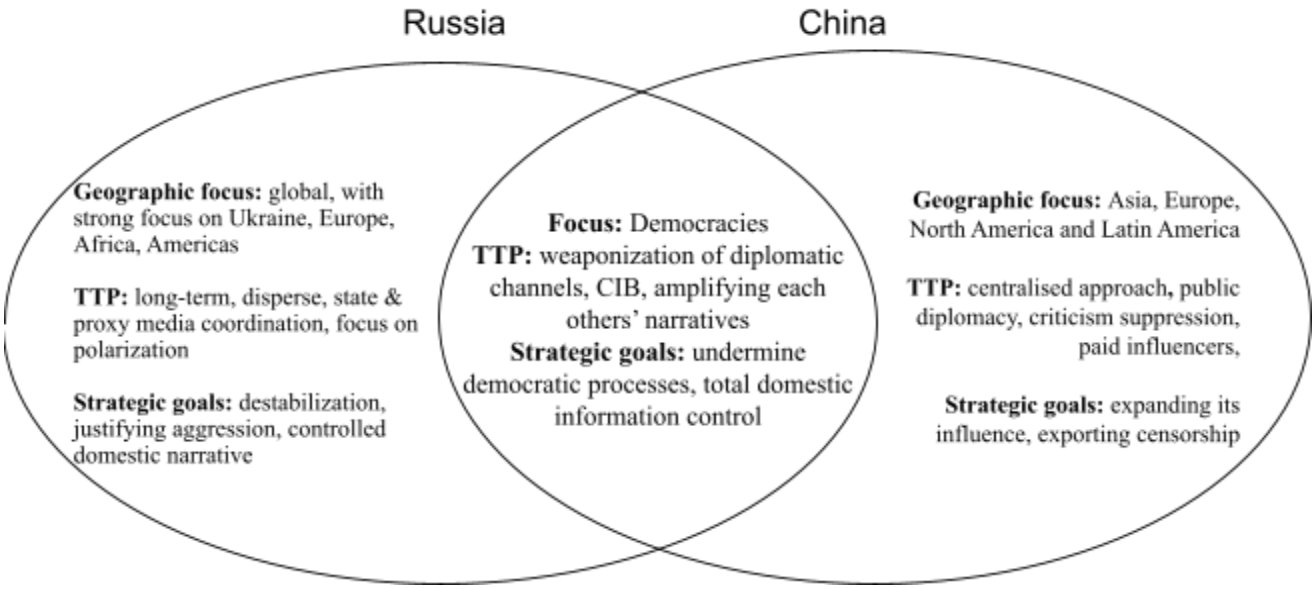


Figure 2. Comparison of key FIMI actors
Prepared by the authors based on EEAS reports.

The third report has also indicated Russia to be the most frequent FIMI actor, specifically within the EU member states. Russian attributed infrastructures, which include all channels where connections to the actor are not concealed, account for 20% of total FIMI activity, while China encompasses 3.5% (EEAS, 2025).

While these two actors have aligned some of their FIMI campaigns and exhibit some common patterns of action and strategic goals, their coordination primarily remained opportunistic across all three reports. As illustrated in Figure 2, differences exist in their tactics and approach to FIMI. China is characterized by its centralized and synchronized infrastructure that targets defined objectives and topics, whereas Russia adopts more of a polycentric method, simultaneously addressing various countries and topics (EEAS, 2025). The general stance of China on foreign information manipulation is centered around specific and highly sensitive topics, namely dealing with conflicted regions like the South China Sea, Xinjiang, Tibet, and

Hong Kong (EEAS,2025). The main objective of these efforts is to reshape global perceptions and expand its political and economic influence.

Russia, on the other hand, tends to take advantage of every opportunity presented by important events, such as elections or some statements of high profile individuals. Such events often trigger Russia's swift efforts to distract or distort the targeted audience's perceptions, allowing it to destabilize political processes or justify its ongoing war in Ukraine. Hence, its strategy includes a wide range of misinformation, specifically tailored and adapted to various scenarios, with their bigger scope focused on polarizing opinions in targeted regions rather than merely expanding its influence (EEAS, 2025).

Nonetheless, there are some notable amplification and mutual coordination efforts between these two actors, particularly when reinforcing anti-Western narratives. They both portray the West usually as weak and unstable, with NATO being blamed for the conflict escalation following the 1000 days since the start of the invasion of Ukraine (EEAS, 2025). Despite the above mentioned differences in tactics and approaches, their overarching core goals often closely align.

There are similar tactics employed by these two actors, as both utilize channels that could serve different roles depending on the levels that they operate: high influence hubs, boosters, and bridges between clusters. The high influence hubs are usually state controlled media outlets that generate large volumes of content, which are then spreaded by boosters across all channels, and further amplified by bridgers, that enlarge its global reach by sharing content in the languages of the targeted audiences (e.g., Sputnik Afrique, Pravda in English)(EEAS, 2025)

3. EU mechanisms and instruments to counter FIMI

To understand the emergence of the EU's countermeasures landscape, it is necessary to outline its diplomatic service body, the European External Action Service. This body addresses a wide variety of issues ranging from public diplomacy and crisis responses, with one of their focuses being tackling disinformation and FIMI. Development of response capabilities to disinformation primarily began in 2015 (Information Integrity and Countering FIMI, 2025). As previously mentioned, it has established a variety of mechanisms to define, detect, coordinate and respond to disinformation.

Earlier actions include the Rapid Alert System (RAS), launched in March 2019. This real time information sharing and monitoring system enables EU member states to share FIMI instances, which then raises awareness and provides coordinated responses across the union (Factsheet: Rapid Alert System, 2019). The system's benefits extend as a valuable data collection tool for researchers to analyse, track, and develop further response measures (see Annex).

In spring 2023, the creation of the Information Sharing and Analysis Centre (FIMI-ISAC) further strengthened the overall toolkit of the EU (see Annex). This initiative is a collaboration among like minded organizations that are interested in detecting, identifying malicious information manipulation behaviors (FIMI-ISAC, 2023). This promotes and coordinates cohesive defence measures through the knowledge exchange and joint efforts by FIMI experts.

Tool	Purpose	Developed by	When	Response Measures	Application in EEAS / EU
Kill Chain	Model describing sequential stages to detect and disrupt	US military doctrine, Lockheed Martin (cyber)	Military-pre-2010s Cyber-2011 FIMI-2020s	Early detection and disruption at each stage	Understand FIMI campaign lifecycle; guides timing and targeting of countermeasures
DISARM	Framework for cataloguing, analyzing, and coordinating responses	DISARM Foundation and partners	~2022	Structured incident analysis, shared taxonomy, data exchange (STIX)	Adopted by EEAS, NATO, US; supports Rapid Alert System and ISAC
FIMI Toolbox	Comprehensive catalogue of instruments to prevent, detect, and respond	EEAS, EU institutions	Developed post-2022 (Strategic Compass)	Four pillars: Situational Awareness, Resilience Building, Disruption & Regulation, External Action.	Central operational framework for EU. Integrates short, medium, and long-term measures
FIMI Exposure Matrix	Analytical tool to systematically classify/attribute FIMI infrastructure	EEAS (Strategic Communications Division)	2025 (3rd EEAS FIMI Report)	Mapping infrastructure network analysis, enhanced attribution, targeted disruption	Supports identification and attribution of FIMI actors

Table 4. Overview of EEAS recommended responses. *Prepared by the authors based on EEAS reports*

The main focus of our study, the annual EEAS reports on FIMI, can be seen as a response mechanism itself, formulating response measures and recommendations. The first two reports particularly address the need for common definitions and terminology related to FIMI, introducing a framework for knowledge generation and information sharing. The pioneering report has introduced several response measures aimed at better understanding, detecting and disrupting FIMI activities, namely through the Kill Chain model. Originally utilized in the military and cybersecurity sphere, this very model can ideally be integrated to the FIMI landscape by allowing for a clear examination of each incident in sequential stages: planning, preparing, and executing to assessing (EEAS, 2023). This model offers the most optimal taxonomy for the Disinformation Analysis and Risk Management (DISARM) framework introduced in the report, which is an open source framework for cataloging and analysing FIMI

(EEAS, 2023). Along with this, the second report developed a crucial EU toolbox of joint responses that integrates analytical and response cycles to ensure more proportional and effective responses to counter FIMI. These initial reports served as foundational elements for the further punitive and specific response measures; they laid the baseline for tools that can refine and enhance counter mechanisms.

The initial efforts to construct the necessary framework were exemplified by the second report's contribution. It built upon the first report's FIMI framework that began with the Threat Analysis cycle, by subsequently expanding to include the Response cycle in the following report (EEAS, 2024). This workflow includes assessing threats, creating and developing countermeasures, and evaluating their effectiveness. The authors highlight the importance of continuous information sharing between the two workflows to create a systemic organization of the response arsenal (EEAS, 2024). The framework proposed in the second report consists of several important pillars: Cross-Domain Analysis, Adapted Countermeasures, and Mechanisms for Collective Response (EEAS, 2024). The first one emphasises information gathering that goes beyond technological aspects due to the socio-cognitive component of FIMI. Meaning, both types of data–the behavioral analysis of TTPs and the non-technical contextual indicators-inform the overall response strategy (EEAS, 2024). Meanwhile, the adapted countermeasures meet the need for preventive and long-term responses by developing a list of counter-activities for each stage: pre-incident, mid-incident, and post-incident (EEAS, 2024).

As noted in earlier sections, the latest report offers stricter and more punitive measures to the defender community through the systematic analytical tool known as the FIMI Exposure Matrix. The matrix incorporates sophisticated attribution methodologies that consider both behavioral indicators (posting times, language use, TTPs) and technical (IP addresses, hosting

data). This tool enables the defender community to recognize the complexities around linking FIMI activities to threat actors, since there is a high risk of falling for over-attribution because some narratives could explicitly benefit particular actors (EEAS, 2025). Hence, the criterias for attribution proposed by the matrix entail a thorough comparison of indicators with previously detected profiles of adversaries, aiming to identify specific 'signatures' linked to them. Despite the strong analytical and evidence-based approach, the public attribution remains a political decision (EEAS, 2025). Acknowledging the potential diplomatic consequences, it is crucial to further advance attribution methodologies and to enhance the available knowledge of threat actors, while remaining open to the possibilities of unexpected parties getting involved.

These efforts, combined, underscore the importance of EEAS's role within the FIMI landscape by offering insights that could be then transferred to other targeted states.

4. Critical perspectives on the EU approach

This subsection engages with several critical perspectives which stem from the EU's approach to counter foreign digital interference, as highlighted in scholarly literature. The report by SG Strat (2024), for instance, offers an overview of the EU's efforts by focusing on activities done by EEAS in 2023. Another comprehensive report for 2024 by Gehringer (2024) explores in greater detail several measures that include: the Digital Services Act (DSA), the Code of Practice on Disinformation (CoPD), and initiatives such as EUvsDisinfo and the European Digital Media Observatory (EDMO).

Colliver (2020) introduces an empirical examination of the primary pioneering document focusing on the 2019 European Parliament elections. The author highlights the need for enhancing transparency by adopting one model that will enable research and the expert community to freely observe the online environment. According to the author, the self-regulatory

nature of the document is not enough; from their perspective, the code was rather a preliminary effort to build common grounds with Big Tech companies. With the subsequent strengthening of the CoPD in 2022, a study was implemented to compare the two versions and their effect, with no significant improvement in the misinformation ecosystem observed (Papadogiannakis et al., 2024). Authors also note the limitation caused by relatively few signatories adopting the CoPD; however, rather than criticizing it, they view it as a reflection of a desire for a misinformation-free online space.

Following this, Shattock (2021) provides additional analytical perspectives to look at the CoPD alongside other policy measures. The author argues that the era of self-regulatory measures in the misinformation landscape has come to an end, especially with the introduction of a binding legal framework - DSA. However, Shattock formulates several criticisms regarding the EU policy approach. In particular, he outlines several details that DSA overlooked, namely the issue of "harmful but lawful" content, which presents challenges in balancing legal regulation with freedom of expression. Conjointly, the literature outlines the limitations of these policies with Shattock (2021) labeling it a 'piecemeal' approach, while other authors echo such sentiments, acknowledging the progress.

Discussion and Conclusions

The digital landscape has evolved significantly over the years, capturing shifts from early technical dimensions of cyber attacks, viruses and malware, to what is now taking the form of digital interference and information manipulation. It has become easier for state and non-state actors to take advantage of the gray zone factor, in which the threat exists. Without resorting to conventional and kinetic acts of conflict, threat actors can conduct attempts of malicious, intended, and coordinated actions to cause potential harm to political systems and societies, and

undermine their core values and principles. Digital threats have become a fixed feature of global politics, where they are no longer occasional or exceptional, but a constant part of international affairs. Operating in a complex non-tangible environment, the problem is causing deep concerns for the global community, both states, international and regional organizations to address it.

Despite the absence of borders in the digital space, as well as the acknowledgment of the threat by the international community and cooperation, states adopt their own countermeasures, which reflects the nuances in how they perceive and address foreign digital interference. The EU is seen emerging as a significant and influential actor, not only in agenda and norms setting, but also in the conceptual shaping of the phenomenon, which can be seen through the institutional leadership of the EEAS.

Observed in the reports rapid evolution of the digital domain and the advancement of manipulation techniques used by the adversaries, from early situational cases of disinformation campaigns and narrative seeding, threat actors have significantly sophisticated their arsenals to whole infrastructures, within a spare of three years, making it challenging to establish clear definitions of what constitutes FIMI and how it should be addressed. Conceptualization of the phenomenon comes with the risk of either being too broad or too narrow, which can be seen through the development process of the EU's articulation.

The EU's efforts, in particular within the EEAS reports spectrum, provide scrutiny for the policymakers and defender communities in addressing the ever-changing global threat. Through its comprehensive and structured analysis of detected FIMI incidents and proposed countermeasures, it offers valuable lessons for other regions as well. The reports depict Russia and China as being the main origins of FIMI actions, targeting democracies in their objective to spread their narratives. In this sense, the importance of this study for Kazakhstan is particularly

highlighted. Given the strategic geopolitical location of Kazakhstan, it is surrounded by two major powers and active actors of FIMI - Russia and China. The relative openness of Kazakhstan in the digital and information space is endangered by the risk of being interfered with, which proves the relevance of the topic for policymakers and academic researchers.

While this research mostly focused on the analysis of the EU's approach to countering foreign digital interference, further studies could explore how its conceptual framework and toolbox can be practically implemented and adopted in the context of Kazakhstan, offering insights upon the effectiveness of such approaches outside the EU.

Bibliography

Official sources:

2022 Strengthened Code of Practice on Disinformation. (2022, June 16). Shaping Europe's digital future; European Commission. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

Canada, G. A. (2025, March 13). *Rapid Response Mechanism Canada: Global Affairs Canada*. GAC. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng#a2

Conley, H., Jeangène Vilmer, J. (2017, June 9). *Successfully countering Russian electoral interference*. Center for Strategic and International Studies. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Colomina, C., Sanchez Margalef, H., Youngs, R., & European Parlament. (2021). *The impact of disinformation on democratic processes and human rights in the world*.

EEAS. (2023, February). *1st EEAS Report on Foreign Information Manipulation and Interference Threats*. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

EEAS. (2024, January). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*.

https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

EEAS. (2025). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. In *EEAS*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

EEAS. (2025) *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European Council. (2015). *European Council meeting (19 and 20 March 2015) – Conclusions* (EUCO 11/15). Council of the European Union. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdfconsilium.europa.eu

European External Action Service. (n.d.). *About EUvsDisinfo*. EUvsDisinfo. https://euvsdisinfo.eu/about/ https://euvsdisinfo.eu/about/

European Commission. (2018a). *A multi-dimensional approach to disinformation: High Level Expert Group on Fake News and Online Disinformation.* *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271*

European Commission. (2018b). *Action Plan against Disinformation* (JOIN(2018) 36 final). https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

Factsheet: Rapid Alert System. (2019, March 5). EEAS. https://www.eeas.europa.eu/eeas/factsheet-rapid-alert-system_en

FIMI-ISAC. (2023, February). FIMI-ISAC. https://fimi-isac.org/

Jeangène Vilmer, J.-B. (2019, June). *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

Ministry for Europe and Foreign Affairs. (2025, February 5). *Foreign digital interference - Publication of the VIGINUM report on information manipulation (5 Feb. 2025)*. France Diplomacy - Ministry for Europe and Foreign Affairs. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/foreign-digital-interference-publication-of-the-viginum-report-on-information?debut_ssra=10&page_courante=2#pagination_ssra

NATO. (2025). *NATO's approach to counter information threats*. NATO. https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en#how

Office of the Director of National Intelligence. (2017, January 6). *Assessing Russian activities and intentions in recent U.S. elections* (ICA 2017-01D). https://www.dni.gov/files/documents/ICA_2017_01.pdf

SG Strat. (2024, May). *EEAS Stratcom's responses to foreign information manipulation and interference (FIMI) in 2023*. EEAS. https://www.eeas.europa.eu/eeas/eeas-stratcom%E2%80%99s-responses-foreign-information-manipulation-and-interference-fimi-2023_en

SGDSN. (2022, November). *Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN*.

https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques#haut-de-page

The United Nations. (2023). Our Common Agenda Policy Brief 8 Information Integrity on Digital Platforms. In *un.org*. United Nations - Civil Society. https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf

United Nations General Assembly. (2023). *The right to privacy in the digital age* (A/RES/78/213). https://docs.un.org/en/A/RES/78/213

Academic sources (books and journal articles):

Alhojailan, M. (2012). *THEMATIC ANALYSIS: A CRITICAL REVIEW OFITS PROCESS. . . - Google Scholar*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0c66700a0f4b4a0626f87a3692d4f34e599c4d0e

Baylis, John, Steve Smith, and Patricia Owens, eds. The globalization of world politics: an introduction to international relations. 4th edition (2008). Oxford University Press.

http://megapro.kazguu.kz/MegaPro/UserEntry?Action=Link_FindDoc&id=41935&idb=0

Clarke, V., & Braun, V. (2016). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Dowling, M. E. (2021). Democracy under siege: foreign interference in a digital era. *Australian Journal of International Affairs*, *75*(4), 383–387. https://doi.org/10.1080/10357718.2021.1909534

Falowo, O. I., Ozer, M., Li, C., & Abdo, J. B. (2024). Evolving Malware and DDoS Attacks: Decadal Longitudinal study. IEEE Access, 12, 39221–39237. https://doi.org/10.1109/access.2024.3376682

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Fridman, O. (2024). Defining Foreign Influence and Interference. *INSS Special Publication*, 1-12.https://kclpure.kcl.ac.uk/portal/en/publications/defining-foreign-influence-and-interference

Georgiana Camelia STANESCU. (2024). Fake News, Bots, and Influencers: The Impact of Social Media on Romania's 2024 Elections. Social Sciences and Education Research Review,. https://doi.org/10.5281/zenodo.15258337

Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). (2025, March 14). EEAS. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

Juhász, K. (2024). European Union defensive democracy's responses to disinformation. *Journal of Contemporary European Studies*, *32*(4), 1075–1094. https://doi.org/10.1080/14782804.2024.2317275

Keohane, R. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy* (REV-Revised). Princeton University Press. https://doi.org/10.2307/j.ctt7sq9s

Kovalchuk, D. (2024). Malware development: From early viruses to modern cyber threats. *Вісник Черкаського Державного Технологічного Університету*, *29*(3), 10–20. https://doi.org/10.62660/bcstu/3.2024.10

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth*. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=8IpfglYAAAAJ&citation_for_view=8IpfglYAAAAJ:u5HHmVD_uO8C

Pamment, J. (2020). *The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework*. Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26180

Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., & Markatos, E. P. (2024). Before & After: The effect of EU's 2022 Code of Practice on Disinformation. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2410.11369

Pollack, M. A. (2005). THEORIZING THE EUROPEAN UNION: international organization, domestic polity, or experiment in new governance? *Annual Review of Political Science*, *8*(1), 357–398. https://doi.org/10.1146/annurev.polisci.8.082103.104858

Petek, B. (2025). *ELECTION INTEGRITY AND FOREIGN INTERFERENCE: THE ROLE OF TECHNOLOGY, POLICY, AND AI IN BUILDING RESILIENT EU FRAMEWORKS*. https://revis.openscience.si/IzpisGradiva.php?lang=eng&id=11448

Rashid, A., Khan, A. Y., & Azim, S. W. (2021). Cyber hegemony and information warfare: A case of Russia. *Liberal Arts and Social Sciences International Journal (LASSIJ)*, *5*(1), 648–666. https://doi.org/10.47264/idea.lassij/5.1.42

Shattock, E. (2021). Self-regulation 2:0? A critical reflection of the European fight against disinformation. *Harvard Kennedy School (HKS) Misinformation Review*. https://doi.org/10.37016/mr-2020-73 Swedberg, R. (2020). Exploratory research. In

Cambridge University Press eBooks (pp. 17–41). https://doi.org/10.1017/9781108762519.002

Van Niekerk, B. (2018). *Information warfare as a continuation of politics: An analysis of cyber incidents* (Vol. 28, pp. 1–6). https://doi.org/10.1109/ictas.2018.8368758

Ördén, H., Pamment, J. (2021, January). What is so foreign about foreign influence operations? *Carnegie Endowment for International Peace* https://carnegieendowment.org/research/2021/01/what-is-so-foreign-about-foreign-influence-operations?lang=en

Media and policy sources:

Bryjka, F. (2024, January 1). *EU Adopts Approach to Countering Foreign Information Manipulation and Interference*. https://www.academia.edu/122468498/EU_Adopts_Approach_to_Countering_Foreign_Information_Manipulation_and_Interference?bulkDownload=true

Berzina, K., Soula, E. (2020). *Conceptualizing foreign interference in Europe*. Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/what-is-foreign-interference-conceptualizing-foreign-interference-in-europe/

Colliver, C. (2020, June 26). *Cracking the Code: An evaluation of the EU Code of Practice on Disinformation - ISD*. ISD. https://www.isdglobal.org/isd-publications/cracking-the-code-an-evaluation-of-the-eu-code-of-practice-on-disinformation/

Gehringer, F. (2024, November 25). *Countering foreign information manipulation and interference*. Foundation Office Canada.

https://www.kas.de/en/web/canada/publications/single-titles/-/content/countering-foreign-information-manipulation-and-interference

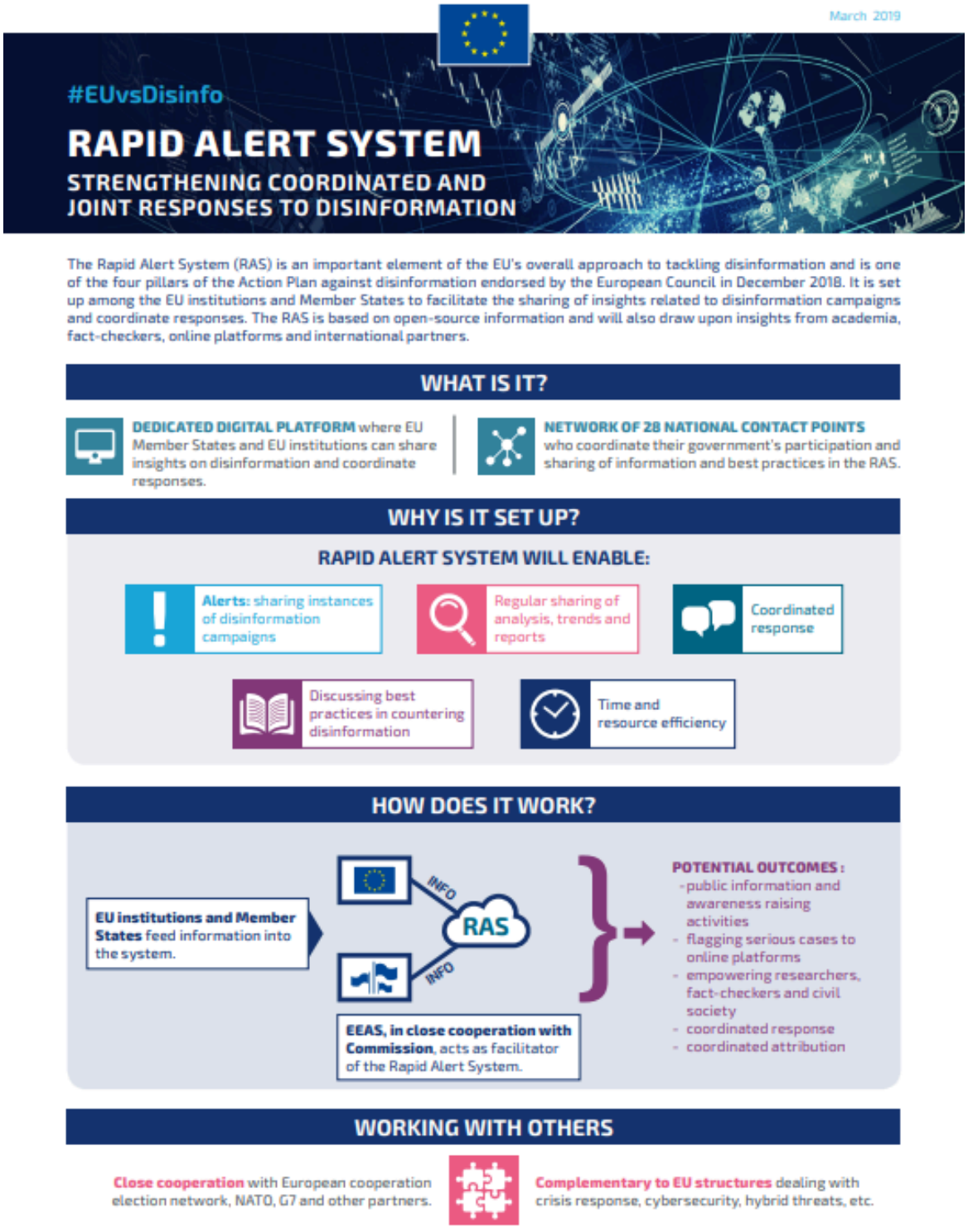
Guo, E. (2025, April 23). US office that counters foreign disinformation is being eliminated. *MIT Technology Review*. https://www.technologyreview.com/2025/04/16/1115256/us-office-that-counters-foreign-disinformation-is-being-eliminated-say-officials/

Annexes

Annex 1. Meta information on EEAS reports

Report	Year	Pages	Incidents	Period	Scope	Special Features
1st	2023	36	100	Oct–Dec 2022	Global, focus on Ukraine	Pilot methodology, Kill Chain approach
2nd	2024	38	750	Dec 2022–Nov 2023	Global, 49% attacks in EU	Risk-based response framework, FIMI Toolbox
3rd	2025	43	505	Nov 2023–Nov 2024	Global, 90 countries targeted	FIMI Exposure Matrix

Annex 2: Rapid Alert System



Annex 3: Impersonation techniques and victims

IMPERSONATION TECHNIQUES AND VICTIMS

A brief look into cases in which Russia impersonated legitimate, trusted entities illustrates that nobody is off limits from seeing their identity or brand misused. Threat actors use impersonation to add legitimacy to their messages and to reach and affect audiences familiar with and trusting the impersonated entities.

Six incidents used cases of impersonation. All of them related to the Russian invasion of Ukraine. **Media outlets were entities most frequently impersonated**. In four incidents, fake cover pages imitating the visual style of European satirical magazines, namely French *Charlie Hebdo*, German *Titanic* and Spanish *El Jueves*, were created to attack Ukraine and Ukrainian President Volodymyr Zelenskyy. Additionally, two videos imitated international media (*Aljazeera* and *Euronews*). The videos falsely claimed that Ukrainian football fans were detained in Doha because of Nazi behaviour during the World Cup, and that a German auction house was going to destroy Russian artworks. All while pretending the message originated from reputable media.

European institutions and politicians were the second most often impersonated entities (two incidents). An animated video listing the alleged disadvantages of Ukraine's accession to NATO, created using an AI-generated voice was presented as an official video by the European Security and Defence College. Moreover, a false account on Facebook used the name and personal information of the former chairman of the Lublin City Council (Poland) to publish a post on the missile blast in Przewodów.

According to preliminary investigations, a Russian attributed channel seemed to be the original publisher of the video impersonating Euronews. The rest of the cases were published by non-attributed channels in the Russian FIMI infosphere. However, the content was rapidly picked-up and amplified by channels attributed to Russian state structures, such as state-linked or state-controlled outlets.

Figure 9 Fabricated covers of EU satirical images

(EEAS, 2023)

Annex 4: Polish elections 2023

POLISH ELECTIONS 2023

Phase 1: Months before the Polish elections, Belarusian state-affiliated media created Polish-language channels on social media targeting audiences in Poland with daily content. Such channels were used to spread Belarusian and Russian FIMI content in Polish throughout all the period leading up to the elections[76].

In this phase, the FIMI infosphere also attacked individual candidates by using old videos reframed in a new context (***Threats 1, 3***).

Phase 2: A few days before the Polish 2023 elections, a website in Polish shared a post, containing leaked photos and videos targeting a candidate in the Polish Parliamentary elections, among other political figures. These were obtained through a previous hacking operation[77].The website was imitating a domain, which was previously blocked for releasing leaked emails from Polish politicians, and which was attributed by independent researchers and Polish services to the Russian and Belarusian security services[78]. The amplification of the content was conducted mostly on X (formerly Twitter), where only 4 accounts were responsible for more than 70% of the activity, indicating inorganic amplification of the content. The aim of this incident was to specifically target certain candidates and to discredit them publicly through anonymous entities (***Threats 3, 5***).

Phase 3: Two days before the elections, Polish media published a video of a police intervention in one of the three polling stations in Poland, where an anonymous bomb threat had been sent before the day of the vote.[79]

Accounts belonging to the Russian FIMI infosphere presented the video in a reframed context, alleging that explosions had already occurred. This misleading framing was amplified by some unattributed pro-Russia accounts on social media. This incident shows an intentional attempt to escalate fears around the alleged bomb threats to the polling stations and thereby dissuade people from going to vote (***Threats 2, 4***).

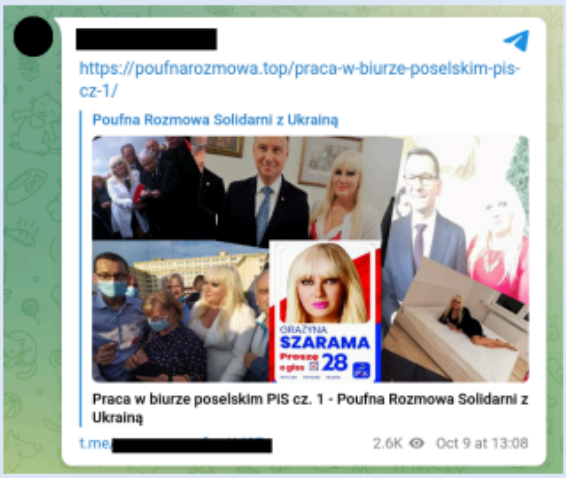


Figure 11: Amplification on Telegram of the leaked files of a candidate running in the Polish elections 2023.

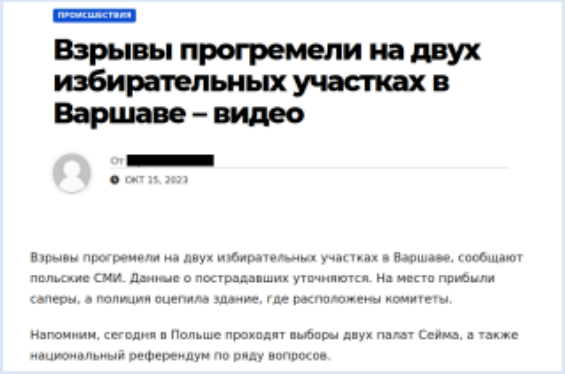


Figure 12: Screenshot from a Russian media outlet. Translation of the title: "Explosions occurred in two polling stations in Warsaw – video"

(EEAS, 2024)

Annex 5: Spanish elections 2023

SPANISH ELECTIONS 2023

Phases 1 and 2: Months before the Spanish elections took place, an official Telegram account of the Russian government suggested to its audience to follow a long list of Telegram channels as a source of information. Sometime later, channels linked to the Russian FIMI infosphere further promoted this initial list through a link allowing subscription to approximately 20 Telegram channels with a single click. These channels were later used to carry out FIMI activities in relation to the Spanish elections. (***Threat 1***)

During **Phase 2**, a pro-Russian hacktivist network claimed to leak information about one Spanish and one European website in Telegram posts containing emails and passwords of the alleged leak. Considering that some information on the alleged leaked accounts were actually included in previous database leaks, this might indicate the creation of inauthentic documents to intimidate opponents and degrade the image of Spain and Europe. Although these incidents did not impact election processes, they could be used to fuel doubts about the integrity of systems. (***Threats 4, 5***)

Phase 3: Some of the accounts mentioned in Phase 1 were involved in a swarming action on different platforms aimed at disseminating fake Spanish electoral ballots containing names of Russian politicians (***Threat 2***).

Additionally, two days before the elections, a domain was registered imitating the official website of the Community of Madrid and its content. The cloned site published an article, warning about a possible attack on polling stations by the former terrorist group ETA on July 23. No amplification was found on open sources, likely indicating that the FIMI operation was possibly carried out on encrypted private channels or chats. According to third-party information, URLs to the domain were received by private Russian Telegram users residing in Spain[75]. (***Threats 1, 2, 4, 5***).

Phase 4: Four days after the Spanish elections, a mirror account of a Spanish RT show on YouTube published a video providing interpretations of the results of the Spanish elections and claimed that regardless of the outcome, Spain would follow the "wishes" of the leaders of the EU and NATO, and of "Washington, London or Brussels". The video content was later cross-posted on various platforms to maximise the reach. The account is most likely used to bypass the sanctions against RT in the EU (***Threat 4***).

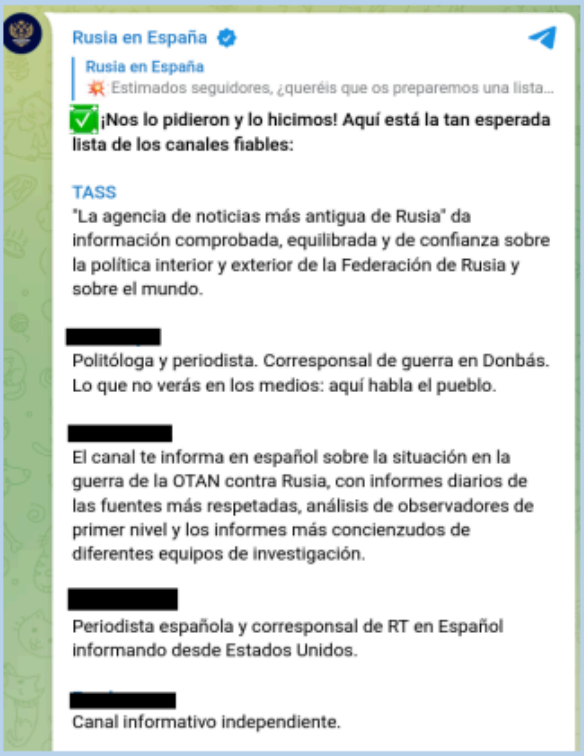


Figure 9: Screenshot of a post from the Telegram account of @EmbajadaRusaEs suggesting a list of sources to follow

Figure 10: Archived version of the now inaccessible website impersonating the official information portal of the Community of Madrid.

(EEAS, 2024)

Annex 6: Covert FIMI operations exploiting events in 2024

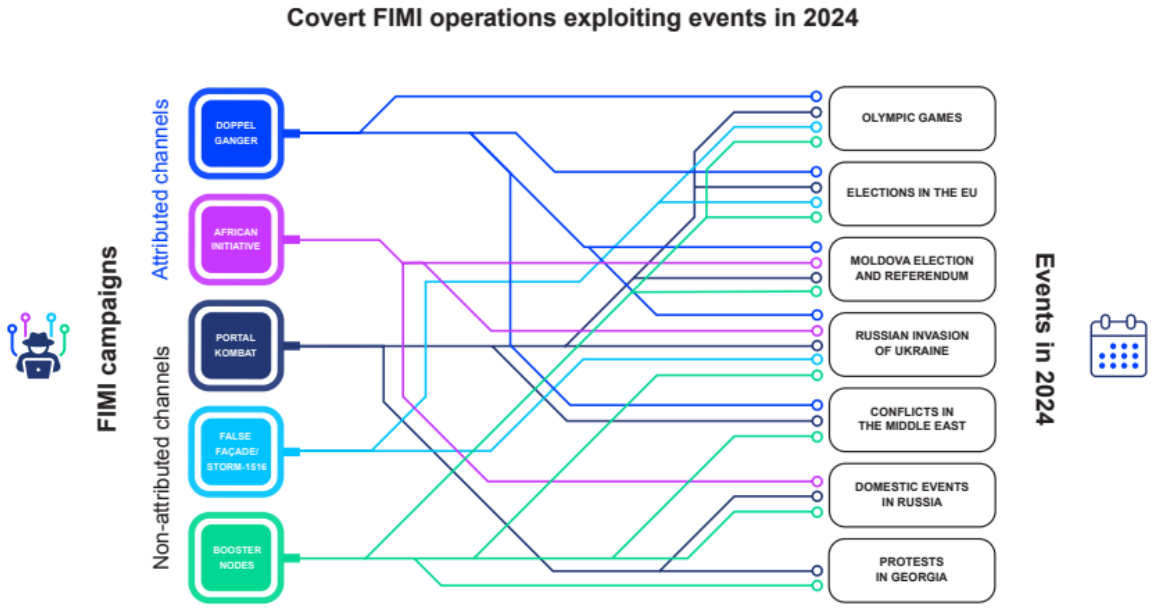


Figure 6: Covert operations and FIMI Booster nodes exploiting events in 2024

(EEAS, 2025)

Annex 7: Portal Kombat

PORTAL KOMBAT

Portal Kombat (also known as the *Pravda network*) was created in 2022 and operates **200 inauthentic media outlets in 35 languages, targeting local and regional audiences across Europe, Africa and Asia**. The network expands through language-specific websites segmented by geography and demographics, including minority groups. Prioritising African influence, it contrasts with False Façade, which focuses on Western audiences. Identified in **73 incidents**, Portal Kombat relies on **high-frequency automated republication of Russian FIMI content**. Initially exposed by VIGINUM, it was **traced to a firm based in Crimea**[46].

Portal Kombat, originally focused on regional audiences in Russia and Ukraine, expanded globally in 2024, registering domains across Europe, Asia and Africa. Following the full-scale invasion of Ukraine, the campaign initially concentrated on shaping narratives around the conflict but later broadened its scope to include other geopolitical issues and local politics.

Rather than creating original content, Portal Kombat relies on automated republication from selected sources, including official Russian government entities, state-affiliated media, Russian Telegram influencers and local anti-establishment outlets. **Despite its low popularity and limited reach, its strategy focuses on saturating local information spaces**. Highly automated systems ensure consistent and low-cost operation. By continuously publishing in local languages, it gradually increases its online presence, often appearing in search engine results at minimal cost.

While initially focusing on websites and social media amplification via platforms like Telegram and VKontakte, **Portal Kombat began making efforts to expand its presence on X in January 2025**.

When coordinating with other covert operations, **Portal Kombat has amplified content from False Façade**, though not in a systematic or consistent manner. In contrast, **it systematically amplifies African Initiative content.**

Annex 8: Doppelganger

DOPPELGÄNGER

Doppelgänger is a FIMI campaign attributed to Russia, active since mid-2022. According to data collected by the EEAS, it **consists of 228 domains and 25,000 CIB networks operating across nine languages**: English, German, French, Spanish, Turkish, Polish, Arabic, Hebrew and Italian. The campaign has a prominent presence within the Russian FIMI infrastructure and has been **linked to 60 documented incidents** in the analysed sample.

Doppelgänger has been widely exposed by international organisations[36] and is **attributed to the firms Struktura and the Social Design Agency (SDA)**. Struktura and SDA are companies directly funded by the Russian state and are involved in interference operations aimed at undermining democracy and eroding international support for Ukraine. Several entities and individuals associated with the campaign have been **sanctioned by the EU**[37], the UK[38] and the US[39].

The main objective of the Doppelgänger campaign is to expand Russian influence globally through audience segmentation and manipulative localised content. Initially focused on impersonating Western news outlets and government websites, **Doppelgänger has evolved into a multi-layered operation**. It deployed networks of thousands of fake domains designed to manipulate platform algorithms, ran sponsored ads on Meta to drive traffic to its deceptive sites, and relied on large-scale CIB networks ensuring widespread distribution. When the amplification occurs in the comment section of accounts belonging to fact-checking organisations, it is known as **Operation Matryoshka**[40].

Over time, the campaign has refined its techniques and has shown **network resilience by adapting to takedowns** by hosting providers and social media platforms. This is achieved through strategies such as re-registering websites under different Top Level Domains (TLDs), migrating to different hosting providers, and using disposable CIB accounts for content amplification. The campaign remains active, **focusing on X and reducing its presence on Telegram and Meta platforms, while extending to new platforms like Bluesky.**

The attribution of Doppelgänger has been made possible through the collection of technical and behavioural indicators, **enabling analysts to identify the systematic repetition of attack patterns**. Proprietary data has confirmed the ownership of the covert operation and its connections to Russian government agencies. **Doppelgänger operates within a closed ecosystem**, functioning as a self-contained cluster with no direct interactions with Russian state official or state-controlled sources. This insular structure suggests a hermetic operational model, reinforcing its autonomy within the broader FIMI landscape.

(EEAS, 2025)