FOREWORD BY HIGH REPRESENTATIVE/VICE PRESIDENT JOSEP BORRELL

In November 2021, when I presented the "Strategic Compass", I said that "Europe is in danger". This was before the start of the two deadly wars that are currently unfolding on our borders and dominating the European agenda: Russia's full-scale war of aggression against Ukraine and the war that flared up once again in the Middle East.

Our geopolitical situation has changed profoundly in recent years, and with it, the nature of some of the threats we face.

One of these is Foreign Information Manipulation and Interference (FIMI): Foreign actors, who engage in intentional, strategic and coordinated attempts to manipulate facts, to confuse, sow division, fear and hatred. FIMI is closely connected to both hybrid threats and cyber threats and has become a crucial component of modern-day warfare.

The most obvious example is Russia – using FIMI as a tool in its war of aggression against Ukraine and in efforts to justify its war around the world. However, other actors also engage in the intentional manipulation of public conversations, to achieve their own political and economic goals.

FIMI poses a major threat to liberal democracies, which rely on free and open information. If information is manipulated, our society and the way we engage in public debate cannot work. If information becomes toxic, democracy cannot work. This is a problem we need to address, inside the EU and together with our partners.

This is why, when we created the Strategic Compass, we made countering FIMI one of its goals. Throughout my mandate, I have invested considerably in this area, working closely with all EU institutions, the EU Member States, our international partners and civil society organisations. We have pioneered new approaches and instruments, which culminated in the development of our FIMI Toolbox to effectively address the threat.

This Second EEAS Report on Foreign Information Manipulation and Interference (FIMI) threats sheds light on the current threat landscape, based on 750 investigated FIMI incidents. It raises questions about effective countermeasures and sets out a comprehensive response framework, helping all stakeholders in cooperating more effectively in fighting information manipulation.

The report identifies Ukraine as the primary target of FIMI activities, underscoring the need to intensify countermeasures. It also illustrates the diversity of FIMI's reach, describing attacks on institutions such as the EU or NATO, key media outlets, or individuals, such as politicians and celebrities.

FIMI activities often capitalise on already existing attention around significant events, such as elections. 2024 is a critical year for democracy. All over the world, about two billion people will be asked to cast a vote, including to elect the next European Parliament in June 2024. In light of this, this report also suggests measures and actions to prepare and protect societies against potential information manipulation and interference in elections.

The battle against FIMI is a matter of European security. It is one of the battles of our times. And with the tools we are developing, it is a battle that can be won.

Josep Borrell Fontelles

4 ADDRESSING FIMI DURING ELECTORAL PROCESSES

While Chapter 3 is a conceptual outline of the Response Framework, Chapter 4 will focus on the practical question of how it can be used. The Response Framework will be applied to the analysis of election-related FIMI incidents and outlines a possible workflow to address FIMI and disinformation during elections.

The issue of external interference in elections, both within and outside the EU, remains a key concern as Member States prepare themselves for the European Elections in 2024. However, it will not only be a key year for the EU, but many other national elections are taking place, including in Belgium, the US, Ukraine and India among many others. Interference in elections can take different shapes and the actors involved in it may not always be recognisable; however, their common trait is the use of cost-effective and varied methods aimed at instigating instability and division within societies.

Considering numerous instances of electoral interference documented in prior studies[60], it is prudent to prepare for possible interference also during the upcoming 2024 European Elections. The complexity of the European Parliament election, comprising 27 individual processes across the EU Member States with different electoral traditions, could be a target of manipulative activity. However, while acknowledging the ongoing threats and past well-known cases of election interference**, it is important to avoid inflating the threat while ensuring elections' integrity both in the EU Member States and around the world.** An EEAS cross-case analysis of FIMI incidents in recent elections **underlines the importance of closely addressing FIMI and disinformation through a risk-based perspective in order to differentiate perceived risks from actual risks**.

This chapter will first present a cross-case analysis of 33 FIMI incidents in election contexts, which will then lead to considerations on when and how FIMI actors mobilise to interfere in elections. This section will conclude by combining the results obtained from the analysis with the Response Framework to FIMI Threats described in Chapter 3 and therefore attempt to establish an example of a reactive response strategy that can be used in preparation for this year's elections.

CROSS-CASE PATTERNS

The sample of cases chosen for this report consists of a total of 33 analysed FIMI incidents concerning elections in the following countries: United States (Midterm Elections 2022), Italy (General Elections 2022), Kosovo (Local Elections 2023), Montenegro (Parliamentary Election 2023), Spain (General Election 2023), Liberia (General Elections 2023), Poland (Parliamentary Election 2023), Netherlands (Parliamentary Election 2023) and Democratic Republic of the Congo (Presidential Election 2023). Although the main cases are a product of EEAS internal analysis, the findings have been complemented and checked against the results of previous reports on FIMI cases produced by civil society, specifically on the French Presidential elections (2017)[61], US Presidential elections (2020)[62] and German Federal elections (2021)[63].

Details of the analytical methodology applied can be found in the EEAS' 1st Report on Foreign Information Manipulation and Interference Threats[64]. The type of standardised methodology used in this report relies on systematic application of standardised analytical frameworks, taxonomies and standards to describe FIMI threats, such as the ABCDE framework[65], DISARM Red Framework[66] and the Structured Threat Information Expression Language (STIX)[67]. The use of this standardised methodology provides evidence-based analysis and is a key element to support the application of better-informed responses.

A cross-case analysis of the collected incidents reveals patterns of manipulative behaviour, preferences in choosing targets of the incidents and other motivations behind attacks. The incidents can be divided in five macro-categories that are characterised by the type of threats posed to the elections. **Threats are defined according to the target of the attack, the presumed objectives of the attacker and the methods** (Tactics, Techniques and Procedures - TTPs) **used. Each section contains a reflection on the possible risks generated by the described threats**.

Threat 1: Targeting Information Consumption

- **Objectives:** Threat actors want to **control the information flow** and set the agenda on certain key topics during the electoral period.

- **Methods:** Many of the cases detected in this category coincide with the **preparation phase** of the incidents[68] where threat actors prepare their infrastructure and try to establish their legitimacy by occupying the information space and engaging with audiences that in the future may receive targeted incidents. Some examples of incidents in this phase include the set-up of dedicated channels and social media accounts to distribute targeted messaging and organise coordinated distribution of content. Proxy media and channels were promoted through already established channels to ensure the delivery of FIMI content. Narratives **discrediting traditional or mainstream media** are also common among these incidents.

- **Risks:** General distrust in official sources and mainstream communication channels used to disseminate information on elections or used by democratically elected officials, thereby fuelling reliance on fringe or unverified sources.

Threat 2: Targeting Citizens' Ability to Vote

- **Objectives:** Threat actors seek to lower representativeness of election results.

- **Methods:** The main ways to affect citizens' ability to vote are, on the one hand, to **encourage abstention** and, on the other hand, to **promote invalid votes.** Both methods could cause voluntary or involuntary reaction by voters targeted by FIMI messages.

  In the case of the **promotion of abstention**, both physical disruption of the vote and confusion regarding the terms and requirements to vote can generate an **involuntary reaction**, whereby citizens want to participate in the democratic process, but their capacity is lowered. Examples of this can be false security alerts near polling stations, which generate a sense of insecurity (e.g. terrorism or health risks), or generating confusion about the terms and requirements to vote (e.g. dates, documentation, procedures). At the same time, a **voluntary** abstention from the vote can be caused by discouraging citizens from voting for any political party or persuading them to use abstention as a gesture of protest.

  The **promotion of invalid votes** is recurrent across multiple elections analysed. In this case, citizens can be involuntarily brought to cast invalid votes, for instance by misleading them into using fake ballots. Incidents also promote the idea of non- or invalid voting as an expression of protest, thus convincing voters to voluntarily cast an invalid ballot.

- **Risks:** Parts of society will not accept elections results as legitimate, which can even lead to violent reactions, protests and unrest.

Threat 3: Targeting Candidates and Political Parties

- **Objectives:** Threat actors carry out FIMI incidents affecting parties or individual candidates with the aim of **polarising citizens** by supporting or attacking specific political positions or **promoting a specific political option**. In certain cases this entails **undermining political adversaries** or, in a more granular way, specific minorities, political projects or political views.

- **Methods:** The analysis of the selected incidents shows that techniques used to affect parties rely mainly on undermining specific candidates, often through **direct, personal attacks** in order to affect both electoral campaigns and political aspirations (e.g. allegations of corruption; reputation scandals; use of gender, sexual orientation or race…) or **dispute the independence** of political parties (e.g. allegations of interference). One prominent example in which FIMI actors at least amplified attacks is the case of the gender-based disinformation attacks against German Foreign Minister Annalena Baerbock when she ran as a candidate in the German Federal Elections in 2021[69].

  Other polarisation methods often **leverage existing narratives**, such as conspiracy ideologies, or **use breaking news** events or active crises to favour or disfavour ideological groups (e.g. using topics such as migration, COVID-19, the Russian invasion of Ukraine…), thereby **directing attention** to certain specific political topics. One example is the MacronLeaks[70], which affected President Macron during the French Presidential election in 2017 by releasing personal emails, previously obtained in a hack, just two days before the vote.

- **Risks:** Discouraging candidates to run for election or to be vocal about certain issues constitutes a risk. The repercussions can be both personal and public for the candidate and could possibly undermine their political career and their ability to represent voters' interests.

Threat 4: Targeting Trust in Democracy

- **Objectives:** In the analysed incidents, threat actors aimed to undermine democracy as a political system, and citizens' support for it. Their goals can be geopolitical, economic, political or simply aimed at sowing confusion.

- **Methods:** The electoral system is portrayed as weak and open to manipulation, for example by spreading content on false fraud allegations, pre-agreed election results, alleged irregularities during the vote, non-reliable vote-counting systems. Examples include the organisation of protests or alleged hack and leak operations undermining the integrity of individuals or entities. Some other cases leverage the narrative that voting does not yield political change, a narrative that also can be found in the threats promoting abstention. This kind of content usually increases as the election approaches and reaches a peak on election days.

- **Risks:** Abstention, protest votes and invalid votes, low turnout, sustained protests, and an overall impression that elections are not democratic.

Threat 5: Targeting Election-Related Infrastructure

Cyber-enabled operations can be used both to attack physical infrastructure and to reinforce threat actors' operations. In the context of FIMI attacks, cyberattacks can be followed by an information manipulation component, as it is the case for some of the analysed incidents, thereby constituting a form of hybrid attack.

- **Objectives:** Disrupt physical infrastructure and sow doubts regarding the legitimacy of the voting process, as well as generating an overall sense of distrust and insecurity regarding the technical infrastructures used by election authorities. Such incidents aim to portray the system as insecure and open to manipulation.

- **Methods:** Cyberattacks targeting key voting infrastructures can prevent citizens from voting and interrupt the normal course of the voting system. Such operations could also be costly for the attacker, who often opts for a cheaper type of attack that hijacks the public perception on the security of the elections. For instance, cyber-enabled operations like DDoS attacks against non-key infrastructure or online impersonation of relevant entities are mostly a symbolic way for threat actors to show that they could potentially interfere and create uncertainty.

  While cyber-enabled FIMI incidents against non-key infrastructure have been recorded in the context of this report, disruptive incidents involving cyberattacks on key infrastructures have not. However, it is relevant to mention them for the overall understanding of potential threats against elections[71].

- **Risks:** Real risks caused by cyberattacks could undermine actual key election infrastructures, thereby invalidating or interfering in the results. Perceived risks can create a sense of insecurity and the impression that elections are not secure, even if the attack had no actual impact.

INSIGHTS ON EXPECTED THREAT PROGRESSION DURING ELECTIONS

Determining if, when and how elections might be targeted is an estimate than needs to take into account many variables, which can never be established with full certainty. A closer analysis of the five categories of threat identified above,

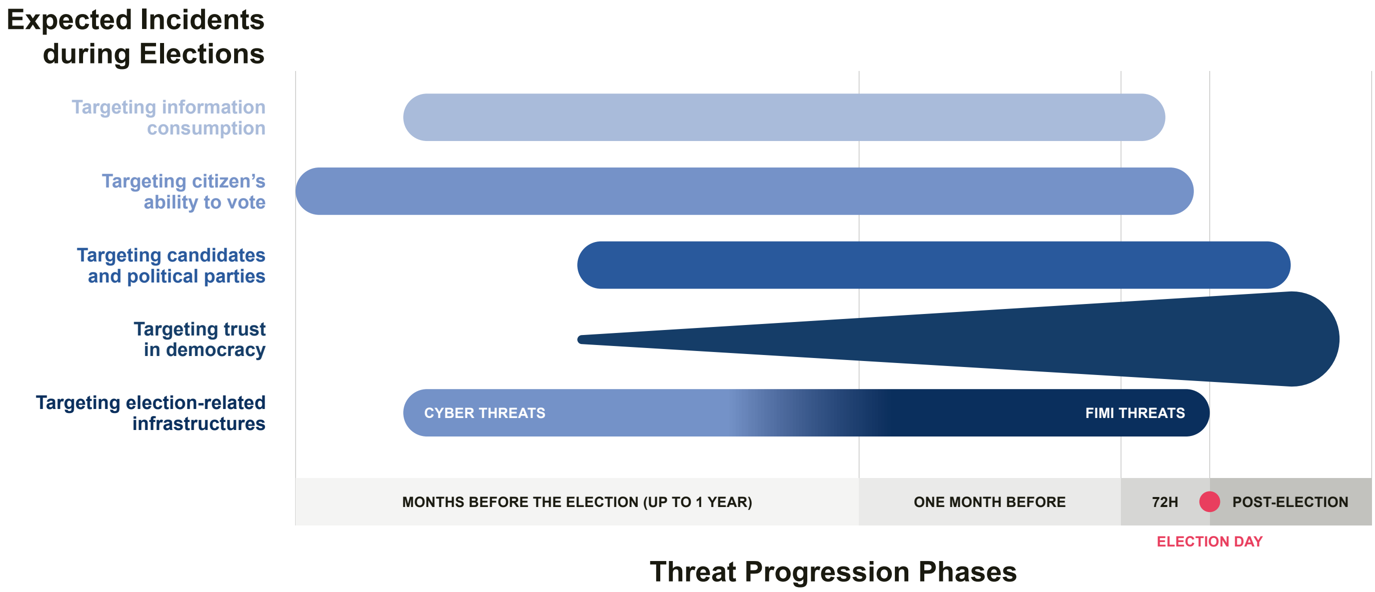


Figure 8: The graph shows the five types of threats to elections on a timeline involving four threat progression phases across the electoral process. The length of the bars shows the distribution of the analysed incidents across the timeline.

according to a chronological perspective, reveals four different time periods where attacks are more likely to take place. In the pre-election period, **months before the vote**, threat actors strategically establish infrastructure, engaging in FIMI campaigns and preparing FIMI campaigns based on cyber intrusions. As the election period approaches, FIMI incidents intensify from **one month** before the elections, and even more so during the last **72 hours** of the pre-electoral period, and manipulative techniques become more diverse. **Election Day and post-election** activities can become critical too, potentially triggering calls for action to delegitimise and question results. Throughout, threats are strategically linked, with prior phases influencing subsequent ones. False or exaggerated narratives spread before the elections, for example, can be used after the elections to question their legitimacy. The following paragraphs outline what incidents might be expected during the four threat progression phases.

Phase 1: Months Before the Elections

This initial phase can start several months before the elections, which, in the incidents analysed, consists of a period extending up to one year prior to them. This phase corresponds also to the preparation of future incidents.

Notably, during this phase, threat actors engage in creating and organising infrastructure and assets to influence information consumption in the lead-up to elections. These channels are launched well in advance and promoted through influential channels within the attributed FIMI ecosystem, such as diplomatic accounts and state-controlled media belonging to the threat actor. Over the course of months leading to the election, these actors "recruit" and interact with their target audiences, which in the cases analysed involved using clickbait, exploiting breaking news events or using information-laundering techniques, establishing legitimacy for subsequent phases (2, 3, and 4).

Incidents targeting candidates and political parties can start in this period as well and they leverage critical or divisive narratives and try to polarise citizens on key political issues (e.g. migration, Russia's war against Ukraine or any local political topics receiving attention). In the analysed incidents, threat actors engage in undermining trust in electoral integrity by recycling or reframing old videos/images, promoting conspiracy narratives related to controversial topics, and employing fake experts to present decontextualised statements or produce fabricated videos.

The preparation for hybrid incidents involving threats to election-related technologies and infrastructures can also be carried out during this phase. Hacking activities such as operations to access or compromise internal information systems, to facilitate FIMI attacks closer to the day of the vote, could be expected during these early times ahead of the vote.

Phase 2: Election Month

This phase covers the last month before the elections, representing the culmination of electoral campaigns. It is worth noting that the official duration of the electoral period differs from country to country. During this month, public discourse intensifies, focusing prominently on electoral information.

In this phase, FIMI activity increases, with threat actors adopting a more varied modus operandi and seizing heightened collective attention towards the topic of elections.

Analysed incidents show that efforts to **legitimise and promote previously established channels** persist during this period as a continuation of the activity from Phase 1.

In this phase, the networks created can be activated to launch attacks aimed at undermining the reputation of candidates and political parties. The cases analysed show the dissemination of fabricated content, such as videos or images, stories about alleged pre-election arrangements between candidates and other organisations (*i.e. the EU and the US, inter alia*), thereby creating false allegations of alleged interference.

Preparation for attacks against online infrastructures can happen during this period too. A notable example involved the registration of online domains through typosquatting techniques (imitating legitimate websites), which remained dormant until activation, in the last 72 hours before the vote. Backup versions of these domains were also prepared, indicating the preparation phase for later hybrid FIMI incidents in Phase 3.

Closer to the week of the vote, networks of political cyber-activist groups, such as Pro-Russian hacktivist groups (e.g. NoName, Anonymous Russia or Killnet), intensified their activity. They publicly organised and communicated alleged or real attacks against non-key infrastructure in countries holding elections through their social media channels. These attacks, such as DDoS attacks or alleged hack and leak operations, aim to generate distrust regarding the integrity of elections rather than causing real damage.

More sophisticated attacks targeting election-related technologies may also be deployed to undermine the reputation of candidates and political parties. Existing material, obtained through prior hacks, can be repurposed to leak private information. For example, after a hacking operation in Poland, information on candidates was exposed through CIB (Coordinated Inauthentic Behaviour) networks that subsequently amplified the content (see examples below). With much less investment, threat actors can also claim a hack and leak operation took place, exploiting heightened awareness or expectations about cyber intrusions, and release allegedly real information harming candidates or parties.

Threat actors may **amplify existing stories, narratives and allegations about the elections**. Recycling, reusing and inflating fringe or anecdotal content published before this or even earlier elections is used to shift attention away from policy debates and to increase negative perceptions about candidates, parties and the electoral process. These campaigns prepare the landscape for more serious incidents in the last hours before the vote (Phase 3) or the post-election phase, including calls for action and the organisation of offline events, such as demonstrations.

Phase 3: Last 72 Hours before the Vote on Election Day

This phase starts in the final 72 hours leading up to voting day and lasts until the closing of the polling stations. During this period, threat actors exploit the last moments to potentially influence citizens' willingness to vote or the direction of their vote. Incidents occurring in this timeframe are particularly crucial, given the limited time available to react, defend, or respond to any potential threat. Additionally, certain incidents during this period may involve physical or offline components, like **calls for actions or alerts**, such as alleged terrorist threats or orchestrated pro-abstention **demonstrations**.

The atmosphere generated during these 72 hours as a result of FIMI incidents can increase the success of subsequent incidents in Phase 4. Notable examples from the analysed incidents involve campaigns discouraging civic participation, by promoting both involuntary and voluntary abstentionism. As explained in the paragraph "Threat 2: Targeting Citizens' Ability to Vote", the involuntary abstentionism can be induced by falsely alerting citizens about potential physical dangers around the polling stations. Threat actors may also employ fabricated evidence or misuse past existing evidence, presented as "breaking news". Other FIMI incidents aim to cause voluntary abstention or proactive actions from citizens, such as protest votes or the use of invalid votes.

During this period, in addition to advocating for low levels of participation, threat actors intensify their operations to sow distrust in the electoral process. Other FIMI incidents attempt to **expose alleged breaches** in the integrity of the electoral process and results. Fabricated or out-of-context repurposed content, such as videos, can be generated and disseminated by the FIMI infosphere to cast doubts on the legitimacy of the vote counting process or make allegations of potential foreign interference during the electoral process. Notably, the hacktivist groups mentioned may pose threats to election-related technologies, announcing further Distributed Denial of Service (DDoS) and claiming hack-and-leak operations to underscore the supposed insecurity of the infrastructure.

Allegations concerning future manipulated results, false predictions, and accusations of interference are likely to give rise to incidents in Phase 4, with a clear connection to the feelings of insecurity and doubt instigated during Phase 3.

Phase 4: Post-Elections

This phase begins at the closure of the polling stations and encompasses post-election activities, including the processing of votes, the publication of first results, and the certification of official results. Incidents occurring in this period can be of critical importance as they have the potential to trigger calls for action and violent events aimed at delegitimising the election results.

The success and impact of incidents during this phase are dependent on the atmosphere created by events in the preceding phases. If there are existing allegations of fraud or widespread doubts about the integrity of the electoral process, these can fuel post-election FIMI action. Threat actors strategically exploit post-election uncertainty as an opportunity to launch attacks.

The incidents documented in this phase leveraged allegations of fraud, interference, and manipulation of results to challenge the electoral will of citizens. Threat actors employ various tactics, including the creation of hashtags, conspiracy narratives and online campaigns or inciting existing groups to organise calls for action or demonstrations. These demonstrations have the potential to escalate into violent incidents, posing a threat to public security.

Furthermore, FIMI incidents in this phase may have a broader target, seeking to undermine democracies from within and attack their core principles. These incidents may be linked to long-term attacks aimed at achieving (geo)political goals. Examples among the analysed incidents promote narratives on the futility of elections by portraying them as a mere "parody" of democracy with predetermined outcomes, often with the implication that secretive outside forces predetermined the results.

Examples: Interconnection of threats across phases

Two case studies from a few incidents collected in the Spanish and Polish elections in 2023 show well how threats can be interconnected and identified across different phases, based on proximity to the Election Day.

SPANISH ELECTIONS 2023

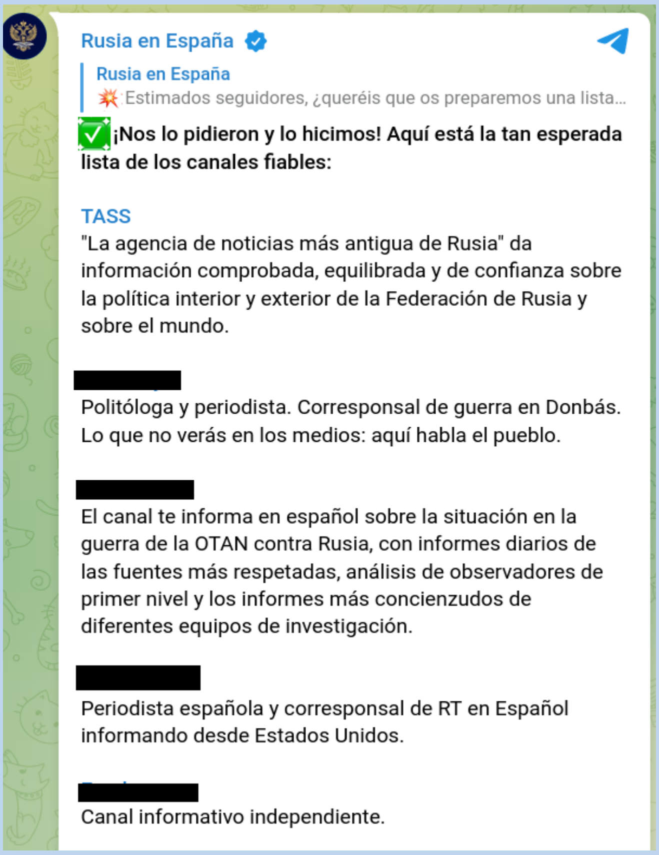
Phases 1 and 2: Months before the Spanish elections took place, an official Telegram account of the Russian government suggested to its audience to follow a long list of Telegram channels as a source of information. Sometime later, channels linked to the Russian FIMI infosphere further promoted this 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***).



Rusia en España

Rusia en España
💥 Estimados seguidores, ¿queréis que os preparemos una lista...

✅ ¡Nos lo pidieron y lo hicimos! Aquí está la tan esperada lista de los canales fiables:

TASS
"La agencia de noticias más antigua de Rusia" da información comprobada, equilibrada y de confianza sobre la política interior y exterior de la Federación de Rusia y sobre el mundo.

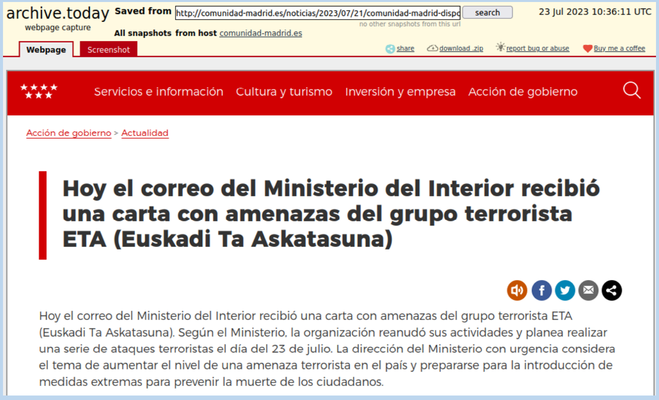
[redacted]
Politóloga y periodista. Corresponsal de guerra en Donbás. Lo que no verás en los medios: aquí habla el pueblo.

[redacted]
El canal te informa en español sobre la situación en la guerra de la OTAN contra Rusia, con informes diarios de las fuentes más respetadas, análisis de observadores de primer nivel y los informes más concienzudos de diferentes equipos de investigación.

[redacted]
Periodista española y corresponsal de RT en Español informando desde Estados Unidos.

[redacted]
Canal informativo independiente.

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



Hoy el correo del Ministerio del Interior recibió una carta con amenazas del grupo terrorista ETA (Euskadi Ta Askatasuna)

Hoy el correo del Ministerio del Interior recibió una carta con amenazas del grupo terrorista ETA (Euskadi Ta Askatasuna). Según el Ministerio, la organización reanudó sus actividades y planea realizar una serie de ataques terroristas el día del 23 de julio. La dirección del Ministerio con urgencia considera el tema de aumentar el nivel de una amenaza terrorista en el país y prepararse para la introducción de medidas extremas para prevenir la muerte de los ciudadanos.

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

POLISH ELECTIONS 2023

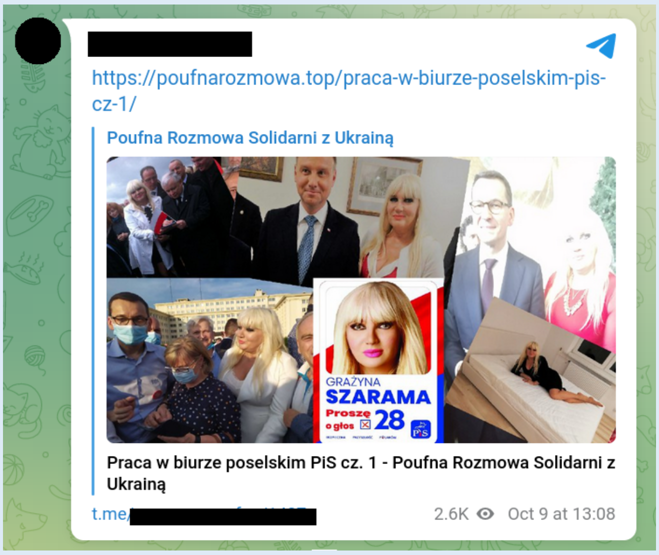
Phase 1: Months before the Polish elections, Belarusian state-affiliated media created Polish-language channels on social media targeting audiences in Poland with daily content. Such channels were used to spread Belarusian and Russian FIMI content in Polish throughout all the period leading up to the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



[redacted] [redacted]

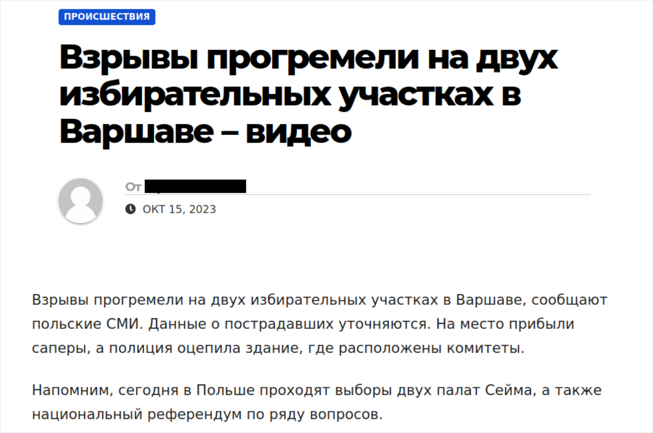
https://poufnarozmowa.top/praca-w-biurze-poselskim-pis-cz-1/

Poufna Rozmowa Solidarni z Ukrainą

Praca w biurze poselskim PiS cz. 1 - Poufna Rozmowa Solidarni z Ukrainą

t.me/[redacted] 2.6K Oct 9 at 13:08

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



ПРОИСШЕСТВИЯ

Взрывы прогремели на двух избирательных участках в Варшаве – видео

От [redacted]

ОКТ 15, 2023

Взрывы прогремели на двух избирательных участках в Варшаве, сообщают польские СМИ. Данные о пострадавших уточняются. На место прибыли саперы, а полиция оцепила здание, где расположены комитеты.

Напомним, сегодня в Польше проходят выборы двух палат Сейма, а также национальный референдум по ряду вопросов.

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

CRAFTING POSSIBLE RESPONSES TO ELECTION-RELATED FIMI

Considering the analysis of FIMI incidents related to elections from both a temporal and a threat-based perspective, how can the FIMI defender community be resilient and prepare for potential FIMI activities targeting upcoming elections?

The Response Framework to FIMI threats proposed in Chapter 3 of this report is a tool that can help to design protective and responsive strategies to guard elections against FIMI. The model suggests that preparation needs to happen long before the elections in order to have enough time to plan and put in place defence mechanisms that might be activated when an incident occurs. Adapting the workflow of the Response Framework to elections helps to identify different actions happening across the different phases of the Threat Analysis Cycle and the Response Cycle. The workflow below is indicative but if applied to the different phases of the electoral process, it can guide defender teams in monitoring and responding to election-related FIMI.

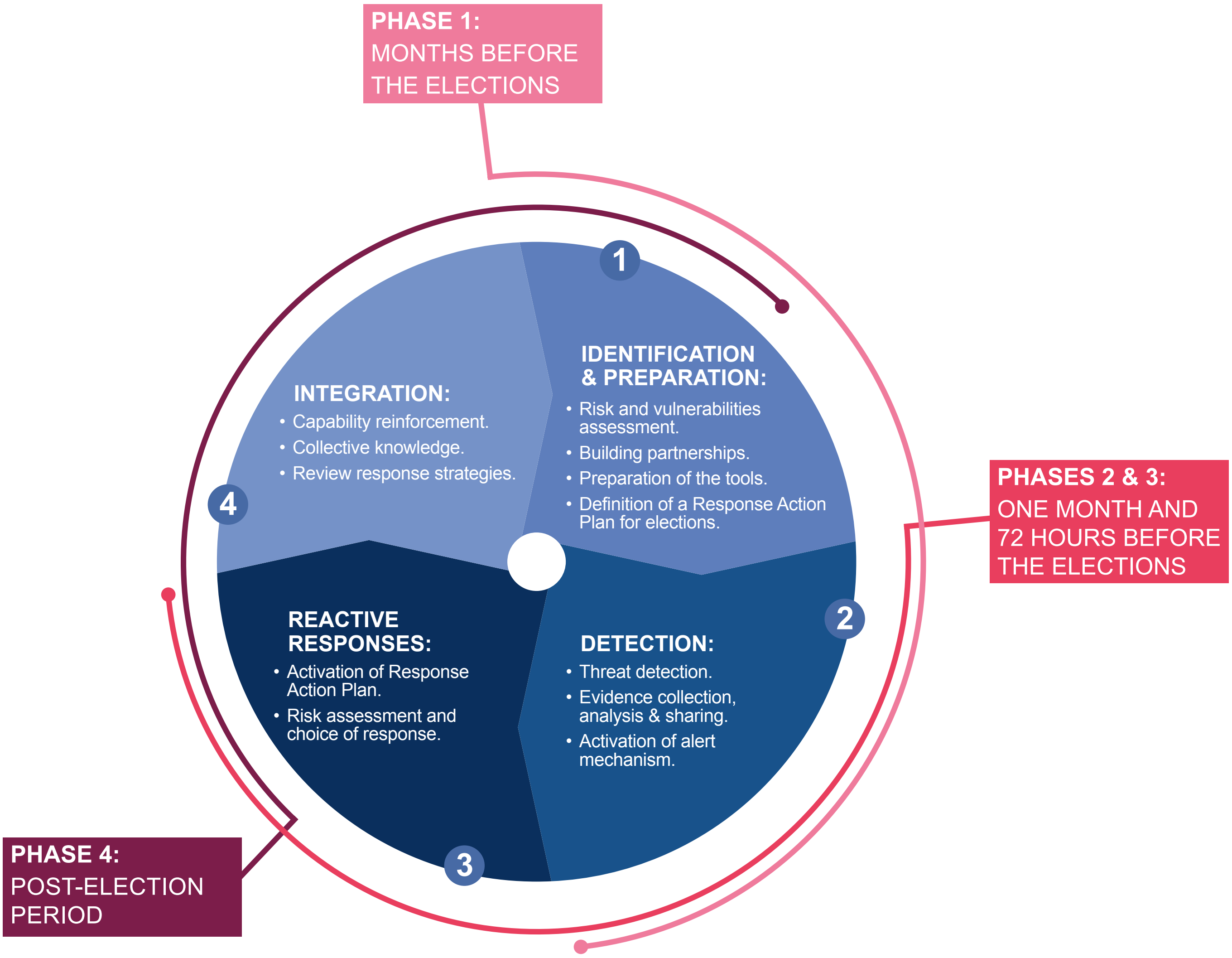

PHASE 1:
MONTHS BEFORE THE ELECTIONS
PHASES 2 & 3:
ONE MONTH AND 72 HOURS BEFORE THE ELECTIONS
PHASE 4:
POST-ELECTION PERIOD
1
IDENTIFICATION & PREPARATION:
• Risk and vulnerabilities assessment.
• Building partnerships.
• Preparation of the tools.
• Definition of a Response Action Plan for elections.
2
DETECTION:
• Threat detection.
• Evidence collection, analysis & sharing.
• Activation of alert mechanism.
3
REACTIVE RESPONSES:
• Activation of Response Action Plan.
• Risk assessment and choice of response.
4
INTEGRATION:
• Capability reinforcement.
• Collective knowledge.
• Review response strategies.

Figure 13: The graph shows a Response Framework applied to elections. The inner cycle shows the different phases of the Framework, which includes elements of both the Threat Analysis Cycle and the Response Cycle (as per Chapter Three). The outer arches represent the threat progression phases of election-related incidents identified in this report. These phases show indicatively when the actions included in the four steps of the inner cycle are expected to happen. The arches overlap when actions are supposed to take place in parallel.

The following paragraphs give the details on the four phases of the Response Framework for elections.

Identification & Preparation:

This step encompasses Phase 1, which starts well before the elections and prepares the ground for the period around Election Day. It may coincide with the period in which threat actors also prepare their infrastructures and assets to influence media consumption and prime audiences with their narratives in the lead-up to elections.

- **Risk and Vulnerabilities Assessment:** Organisations and entities need to conduct a comprehensive evaluation of vulnerabilities and risks according to their specific role in the elections. For example, institutional communication departments would have different risk assessment criteria than an electoral commission or political parties. This is also the basis for the establishment of individual threat levels, which later guide the activation of responses.

- **Building Partnerships and Escalation Channels:** It is important to develop internal and external communication and escalation channels within tailored partnerships on elections. Relevant partners for the escalation of possible FIMI incidents are, among others, election authorities, parliaments and national governments, communication departments managing voting campaigns, civil society organisations involved in election-related topics, political parties, and social media platforms. Establishing points of contact and mechanisms for sharing information on FIMI incidents contributes to overall resilience against election-related threats.

- **Prepare Tools and Sources to Monitor:** Map out the media and social media landscape relevant to elections, identify key players, influential actors, and potential sources of election-related FIMI and disinformation. Equip analytical teams with tools for real-time monitoring, focussing on recognising both general and country-specific election-related FIMI threats.

- **Define a Response Action Plan for Elections & Integrate Previous Lessons Learned:** Build a Response Action Plan upon a reflection on the organisational capacities and needs to respond to threats during elections. This plan needs to be organisation-specific, and outline responsibilities and procedures, ideally minimising decision-making time during critical moments. Incorporate lessons from past election cycles, analysing previous attacks on election integrity, responses used, and their outcomes. Responses would need to be tailored to the nature and severity of the FIMI threat.

- **Activate Preventive Countermeasures:** In this phase, preventive activity often translates into pre-bunking election-related disinformation, preparing and launching communication campaigns to promote accurate and easily accessible information. Other types of preventive measure include starting the collection of information on incidents to build preparedness if the threats intensify. Chapter 3 outlines different types of proactive action in more detail.

Detection:

The detection phase is based on the previous identification and preparation phase. It needs to start well before the elections and continue throughout until the post-election phase.

- **Threat Detection:** Analytical teams, trained during the previous phase, start with the detection of incidents based on TTPs commonly employed by actors spreading FIMI during elections and understand how threat actors behave in the context of elections. This proactive approach contributes to building resilience and preparedness.

- **Evidence Collection and Analysis:** Conduct online investigations and collect evidence using the tools and sources prepared during the previous step. Organise information according to the ABCDE framework and encode data using taxonomies and Structured Threat Information Expression (STIX) to be able to share situational awareness and exchange data with partners.

- **Activation of Alert Mechanism:** Utilise previously identified partnerships and escalation channels to proactively alert partners about incidents before and during the electoral process.

Reactive Response:

This type of response is aimed at providing a timely reaction to an ongoing incident. It is normally activated at critical times, for example when FIMI threats start intensifying as the day of the vote approaches.

- **Risk Assessment and Choice of Response:** Assess risks of an ongoing incident targeting the election and tailor reactive responses to the perceived or real risk that could arise in a specific context.

- **Activate Reactive Responses:** Initiate the reactive responses from the pre-defined "Response Action Plan", which was defined in the identification and preparation step. Upon detection of election-related threats, set in motion responses aimed at minimising, containing or redirecting the spread of election-related FIMI. You may also opt to not react if responses would be more harmful than the attack.

Integration:

This step is normally conducted in the post-election phase, once enough data has been collected and analysed.

- **Capability Reinforcement:** Conduct a comprehensive evaluation of the detection and response efforts enacted before, during and after the elections. Perform a post-mortem analysis, identifying lessons learned, successful strategies, and areas for improvement in the context of elections. Incorporate new analytical insights into updated strategies in preparation for the next elections.

- **Collective Knowledge:** Engage in knowledge exchange with partners and with the public, contributing to a collective understanding of emerging threats specific to elections. Collaboratively enhance overall situational awareness on FIMI during elections through data sharing.

- **Review Response Strategies:** Refine response strategies based on the outcomes of the responses produced during the entire election cycle.

Reacting to Election-Related FIMI

In the context of combating FIMI targeting elections, a wide array of **preventive measures** are available to all defenders. Building on these efforts, the defender community needs to tackle the challenge of formulating effective and timely responses while incidents unfold. How to choose the appropriate approach, and which reactive measures can be employed when confronted with FIMI incidents in real-time? Expanding and understanding which reactive responses are at the disposal of the defender community is key. As described in Chapter Three, the main aims of **reactive responses** are to **contain** the incident from spreading further, **minimise** the spread of the attack, and **redirect** audiences towards verified information, or, decide to **ignore** in order to avoid escalating an incident.

The following paragraph showcases some reactive responses available to different categories of election-related threats identified earlier in this chapter.

	REACTIVE RESPONSES			
THREAT	**Ignore**	**Contain**	**Minimise**	**Redirect**
1) Targeting information consumption	During the election period, the defender community needs to carefully strike a balance between responding to threats and ignoring them. Some considerations to be taken into account when choosing to ignore: - Certain incidents need to be monitored, but not forcibly addressed as long as they do not pose a threat - It is in many cases it is not worth addressing a story that has not gained traction online or offline - Think about whether responding will only amplify the narrative or instil fear in the audience by exposing a particular incident - Sometimes it is better to leave it to someone else to develop a response to an incident. Passing the information to the relevant stakeholders and asking for their support is a good reflex in this case. - Not responding immediately to an incident does not mean inaction. Keep cataloguing the evidence found until it can be used for a response.	- Inform platforms pre-emptively of the build-up of networks or about an unfolding incident. They can take action faster if the activity violates their Terms of Service. - Seek assistance from other organisations in coordinating action to limit the spread of FIMI - Mute or block accounts or channels - Request platforms to have expedited review for content related to elections - Share publicly evidence of channels exclusively or significantly involved in FIMI - Invest sufficiently in online community management on owned channels - Identify and act upon the misuse of your brand, content or communication channels - Early exposure of the creation of networks of channels used by malign actors	- Indicate any breach of Terms of Service to hosting platforms, including harmful and illegal content - Fast debunking and fact checking. Consideration of fact checks in algorithmic amplification processes - Competent authorities can issue removal orders to hosting service providers in order to request the closure or transfer of maliciously used assets - Warnings, strikes and temporary or permanent closure of channels engaging repeatedly in election-related FIMI - Mobilise law enforcement when public safety is in danger (i.e. threats to the individual and society) - Issue legal notices against perpetrators of harassment campaigns against candidates	- Sustained campaign to promote accurate and reliable sources together with correcting false information in relation to elections
2) Targeting citizens' ability to vote				- Launch or support campaigns that promote the act of voting and the participation in democratic processes - Provide, and regularly remind of, accurate information on correct voting modalities across all the available channels
3) Targeting candidates and political parties				- Attribute actors orchestrating campaigns against political parties and candidates - Debunk and provide accurate information - Support other FIMI defenders and targets of FIMI campaigns
4) Targeting trust in democracy				- Engage in campaigns that promote the correct voting modalities, election integrity and participation in democracy - Transparent reporting and coverage of electoral process
5) Targeting election-related infrastructures (hybrid incidents)			- Liaise with election authorities and/or law enforcement if you spot incidents involving real-life threats - Impersonations of real election-related or governmental websites: request relevant national authorities to block/take down the website. Further anti-copyright infringement measures can be taken by relevant bodies.	- In case of cyberattacks or reporting thereof, follow transparent disclosure protocols and do not inflate the impact it had on the elections - Hack & leak operations or information breaches, especially when published close to election date, should be treated with absolute caution.