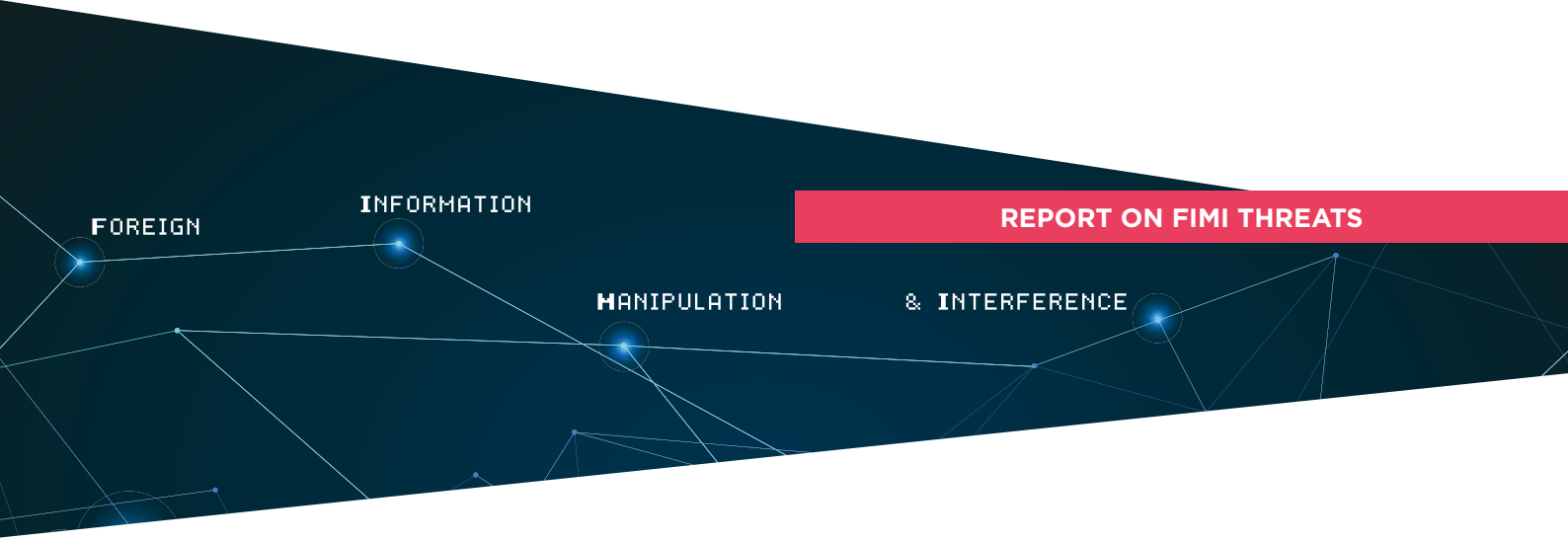


REPORT ON FIMI THREATS

2nd EEAS Report on Foreign Information Manipulation and Interference Threats

A Framework for Networked Defence

January 2024

European Union
EXTERNAL ACTION

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

TABLE OF CONTENTS

GLOSSARY

Term	Explanation
FIMI	Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.[1]
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.
STIX	The Structured Threat Information Expression (STIX™) language is a data format used to encode and exchange cyber threat intelligence (CTI). It can also be used to share information on FIMI incidents, by breaking them down into their different constitutive elements.[2]
Response Framework to FIMI Threats	This framework is a systematic way of organising and conceptualising the analysis and response processes to FIMI. It merges two workflows: an analytical one providing information on the threat and a response one facilitating the decision-making process on countermeasures. The Response Framework relies on the assessment of potential risks and vulnerabilities extracted from the aggregated knowledge of past investigations. Each organisation should adapt its strategy and organise preventive and reactive activities before, while and after an incident occurs.
Threat Analysis Cycle	It provides one core analytical workflow that delivers on the both short- and long-term objective of systematically analysing and disrupting FIMI and disinformation by providing insights for quick and timely responses. The functioning of the Threat Analysis Cycle has been outlined in the 1st EEAS report on FIMI threats.
Response Cycle	It provides one core response workflow to define evidence-based countermeasures to FIMI and disinformation. This Cycle is composed of a series of steps outlining the process to make informed decisions based also on the information obtained through the Threat Analysis Cycle.
Kill Chain	The term "kill chain" describes an end-to-end process, or the entire chain of events, that is required to perform a successful attack. Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases.[3]
Risk Assessment Matrix	To avoid relying on subjective assessment, this system helps to measure the level of risk of an incident based on different indicators such as spread, severity, TTPs or potential consequences. The threat level scored by the matrix indicates the level of adequate action needed. Each organisation can design its own matrix based on internal capabilities and needs.
FIMI Toolbox	The Strategic Compass, adopted in March 2022 by the EU, sets out a plan of action for strengthening the EU's security and defence policy by 2030. One of the aspects covered in terms of security policy is the development of a Toolbox to counter Foreign Information Manipulation and Interference.[4] The toolbox is a catalogue of instruments, many of which are in constant implementation, to tackle and respond to FIMI operations.
FIMI-ISAC	Information Sharing and Analysis Centres (ISAC) are platforms of various kinds that facilitate sharing of information between different actors about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. Specifically, the FIMI-ISAC promotes the use of standardised frameworks, taxonomies, and data standards, enabling members to build upon shared threat models and information to better address emerging threats[5].

EXECUTIVE SUMMARY

This first edition Since the release of the 1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats in February 2023, foreign actors have continued their intentional, strategic and coordinated attempts to manipulate facts, to confuse, and to sow division, fear and hatred. The most obvious example is Russia – trying to justify its war of aggression against Ukraine. However, other actors, such as China, also engage in the intentional manipulation of public conversations. They do so in an attempt to achieve their own political and economic goals by undermining the credibility of democratic institutions, and encouraging division and polarisation within European societies and beyond.

This 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats builds on the 1st Report and completes the work towards a common framework for networked defence against FIMI. This edition is based on **750 investigated FIMI incidents** between 1 December 2022 and 30 November 2023. These cases have been collected by the EEAS in line with its mandate and thoroughly analysed following the methodology outlined in the 1st Report on FIMI Threats. They cannot, however, be considered the only incidents in the information environment.

Based on these insights and on previous findings, as well as the continuous work of the EEAS, the report proposes a "**FIMI Response Framework**" with the aim of linking analysis and insights even more effectively to timely responses, highlighting the importance of cooperation between all the stakeholders that hold key instruments to respond to the intentional manipulation of the information environment.

2024 will be a "super election" year, with at least 83 individual elections all around the world, including the European Parliament Elections for the 27 EU Member states. This report therefore presents a **case study that applies the response framework to FIMI incidents investigated in past elections,** to showcase how its application can further enhance the community's efforts to close the space for manipulation. While the potential threat should not be inflated, the report suggests a number of measures and actions to prepare and protect against potential information manipulation and interference in an electoral context.

The **main findings** of this report, based on the samples used, are:

- **Ukraine remains the country that is targeted most** across the investigated incidents. The European Union has sanctioned key, Kremlin-controlled outlets for their involvement in supporting the Russian war of aggression against Ukraine; however, these findings show that continued and further efforts are necessary to address the ongoing use of FIMI to undermine the country's stability and security, as well as to erode support for Ukraine.

- **FIMI targeting is diverse and also affects non-political individuals.** In the sample used, 149 different organisations were targeted – most frequently the EU and its Member States, as well as NATO, but also various media organisations like Euronews, Reuters, Deutsche Welle and the New York Times. The EEAS also investigated specifically FIMI targeting the LGBTIQ+ community in a dedicated report, highlighting the targeting of individual societal groups. The sample investigated also showed targeting of 59 different individuals ranging from Ukrainian President Volodymyr Zelenskyy and Ukrainian First Lady Olena Zelenska, to the High Representative of the Union for Foreign Affairs and Security Policy/Vice President of the European Commission Josep Borrell or French President Emmanuel Macron. However, venturing beyond the political realm, personalities like the movie actors Nicolas Cage and Margot Robbie and many others saw their voices, statements and faces maliciously used in FIMI incidents with the obvious intention to reach wider and new audiences.

- **Events are important catalysts for FIMI activity**. In 21.3% of the analysed incidents, FIMI activity seized on the already existing attention around events such as political summits, elections, emergencies, official visits and others. The vast variety of events suggest that FIMI actors closely follow institutional and media activity. They strategically and opportunistically make use of the attention created by certain events to pursue their interests.

- **Cross-platform coordination is the default modus operandi in FIMI incidents**. More than 4 000 channels were active 9 800 times across the 750 investigated incidents in this report. Channels can be websites or social media profiles, groups and pages. The platforms most often involved were Telegram and X (formerly Twitter). FIMI activity, however, was observed on virtually all other big, new and niche platforms.

- **AI usage in FIMI is minimal but attention-grabbing**. AI usage in FIMI operations, as observed in this report, constituted an evolution rather than a revolution in conducting FIMI attacks with existing response approaches remaining applicable. Exploiting the high attention on AI risks may be the objective of attacks to distribute FIMI. Responsible experimentation with generative AI tools may hold more benefits for defenders than attackers.

- **Protecting elections from FIMI starts months before and must continue after Election Day**. FIMI actors begin to prepare their operations to target elections well in advance and gradually intensify their attacks. They prepare an alternative information environment, targeting voters, political parties and candidates as well as trust in democracy. Early FIMI activity is also used to sow division after an election has taken place. In the context of elections, while raising our defences is a necessary prerequisite, **defending our societies against FIMI means first and foremost safeguarding the common public space in which ideas can be freely formed and fairly debated.**

Stakeholders from government, international organisations, civil society and private industry have continued to invest in tackling FIMI, sometimes while themselves being targeted by FIMI activity. Despite all existing investments and efforts in the defender community, the threat persists, adapts and evolves. Threat actors are not using FIMI as a sporadic opportunity to interfere, but as a strategic instrument of their foreign policy.

FIMI activity relies on an ecosystem – consisting of the connection between different actors, their proxies and assets – to implement sustained manipulation. Responses to this networked threat need to be equally well connected across the defender community when implementing them. **FIMI is considered a security threat, as well as a threat to society and democracy**, and the response repertoire against FIMI needs to mirror this complexity.

The past has shown that everyone in the defender community is a crucial partner, providing unique insights and implementing specific responses that are available to them. The FIMI Response Framework aims to unlock the power that these individual responders could wield in a more networked and connected, collective response.

Disclaimer: The empirical data mentioned in this report is based on the strategic FIMI monitoring efforts of the EEAS. It reflects patterns seen in known outlets related to overt Foreign Information Manipulation and Interference (FIMI) or independently attributed operations by selected actors and on priority issues of the EEAS. The evidence presented in this report serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity. Conclusions made in this report are meant to complement other types of analysis on different aspects of foreign electoral interference.

1 INTRODUCTION

2024 will see citizens all around the world called upon to exercise their right to vote in at least 83 individual elections, including the European Parliament Elections for the 27 EU Member states[6]**.**

Foreign Information Manipulation and Interference (FIMI) is a global challenge – one that knows no geographical or thematic borders. Anyone can be the target of information manipulation. Cooperation across countries, communities and stakeholders is crucial. Therefore, the EEAS presented a proposal for a common analytical framework and methodology in its 1st EEAS Report on Foreign Information Manipulation and Interference Threats in 2023. Its aim was to bring experts closer together to systematically detect, analyse, document and ultimately understand FIMI activities. This provides a strong basis for operationalising these insights into responses. Building on and complementing this methodology, this 2nd report on FIMI threats outlines how to collectively activate threat-informed countermeasures in a network of FIMI defenders. To connect thorough analysis to effective action, it proposes an **evidence-informed and risk-based framework of responses – the FIMI Response Framework –** which enables the activation of adaptive instruments. For the European Union, these are comprised in the FIMI Toolbox[7].

In 2023, the defender community made significant progress towards a more standardised, collective understanding of the threat and more effective cooperation in tackling FIMI. Advancements in the creation and adoption of standardised analytical frameworks, such as ABCDE[8], DISARM[9] or the Online Operations Kill Chain[10] are just some examples. Convened by the European Fact-Checking Standards Network Project (EFCSN), a European Union (EU) funded project, civil society organisations have cooperated to establish voluntary guidelines for investigators conducting public-facing Open-Source Intelligence (OSINT) work.[11] In November 2023, the Organization for the Advancement of Structured Information Standards (OASIS) launched the Defending Against Disinformation-Common Data Model (DAD-CDM) project, "*a [global] open source initiative to develop data exchange standards for normalising and sharing*" FIMI threat information based on the well-established Structured Threat Information Expression (STIX)[12] standard.

2023 also saw significant progress on agreements to express and – where possible – share threat information between FIMI defenders. In the context of the EU-US Trade and Technology Council[13], the EU and the United States agreed on a shared standard for structured threat information exchange on FIMI, reflecting the shared recognition of FIMI as a key challenge, as well as the need to continue fostering the transatlantic partnership as outlined during the 2023 EU-US Summit[14]. In parallel, the first civil society organisations agreed on the need for a common analytical methodology and formed the first Information Sharing and Analysis Center for FIMI, the FIMI-ISAC[15], as proposed in the Strategic Compass for Security and Defence. Practical sharing of structured threat information has also seen pioneering developments with France's agency for vigilance and protection against foreign digital interference (VIGINUM)[16] and Meta (Facebook)[17], making their research findings on FIMI openly available for researchers and analysts via the developer platform Github.

Threat intelligence has been defined as "*evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard*."[18] That is, analysis and decision making to counter threats need to go hand in hand.

In the presentation of the first Report on FIMI Threats, **HRVP Josep Borrell** laid out the path ahead: **"*Only when we will have clarity on the nature of the problem, can we try to define and implement proper responses*."**[19]

With the common understanding of the FIMI challenge having advanced significantly, this report will describe a framework for **turning collective insights into collective action**. FIMI targets all aspects of our societies; even though many individual FIMI incidents remain limited in their impact, the constant, daily manipulative behaviour attempting to undermine our societies, trust in democracy and the international, rules-based order can have a long-term corrosive effect. Foreign actors deploy information manipulation and interference as a systematic tool of their foreign policy, targeting in particular vulnerable groups and attacking journalists and civil society, as well as undermining trust in democratic processes. As it has been seen through Russia's use of information manipulation to prepare and support its war of aggression against Ukraine, FIMI is also a considerable security threat.

This report first briefly looks at the EEAS findings on FIMI throughout 2023 in Chapter Two. It then presents the **FIMI Response Framework** in Chapter Three. This framework outlines how analysis and adequate responses to FIMI can be more closely connected – from the importance of preventive action to responses that can be made while an incident occurs, as well as in the aftermath of it. Importantly, it also describes how learning from past incidents can feed back into the analysis cycle and increase our resilience against future attacks. Chapter Four applies the FIMI Response Framework to the **protection of elections** from FIMI, indicating expected incidents and how to further increase our collective preparedness.

Defending our societies against FIMI means safeguarding the common public space in which ideas can be freely debated and formed. In the context of elections, while FIMI has to be taken into account, the primary focus must be on providing timely, accurate and transparent election information and discussing ideas.

2 FIMI TRENDS AND FINDINGS IN 2023

This chapter aims to give a brief overview of the main observations on FIMI activity the EEAS has monitored and investigated over the past year. The continuous monitoring and investigation of FIMI incidents is key to ensuring situational awareness. It enables a better understanding of the tactics, techniques and procedures as well as the content used by FIMI actors – these insights are a key requirement for effectively tailoring responses.

The EEAS detected, investigated and encoded 750 cases of detected Foreign Information Manipulation and Interference incidents between 1 December 2022 and 30 November 2023. The number of cases analysed signifies an almost doubling of cases and capacity for detection and analysis compared to the year prior. This is largely due to the commitment to, and implementation of, the common framework and methodology to systematically collect evidence on FIMI activity as outlined in the first threat report, which enabled more targeted detection based on high-risk TTPs and focused OSINT investigations.

The **targets of FIMI attacks** are truly global. In 49% of the cases analysed according to the common framework, countries or their official representatives across the world were directly targeted 480 times. The country most often targeted was Ukraine, with 160 cases recorded. The United States of America were targeted by 58 of these cases, followed by Poland (33), Germany (31), France (25) and Serbia (23). In total, FIMI activity directly observed by the EEAS targeted 53 different countries. Further reports also show FIMI activity in Australia[20] and Latin America[21] during this time, highlighting that FIMI is a global threat.

FIMI not only targets countries, it is also directed at organisations, groups and individuals. **30% of all cases targeted 149 different organisations 318 times**. The organisations most frequently subject to FIMI attacks were the EU (19% of cases targeting organisations, excl. attacks against individual EU institutions), NATO (15%), the armed forces of Ukraine (14%), the UN (3%) as well as various media organisations like Euronews (3%), Reuters (2%), Deutsche Welle (2%) or the New York Times (2%). While public organisations are directly attacked, media organisations and their brand are much more likely to be misused in FIMI attacks through impersonation, in order to lend credibility to manipulated content.

In 18% of all cases, State-driven FIMI activity also targeted 59 different individuals, 171 times. Individuals targeted were mostly heads of states and governments as well as international organisations. Most targeted was Ukrainian President Volodymyr Zelenskyy (40% of cases targeting

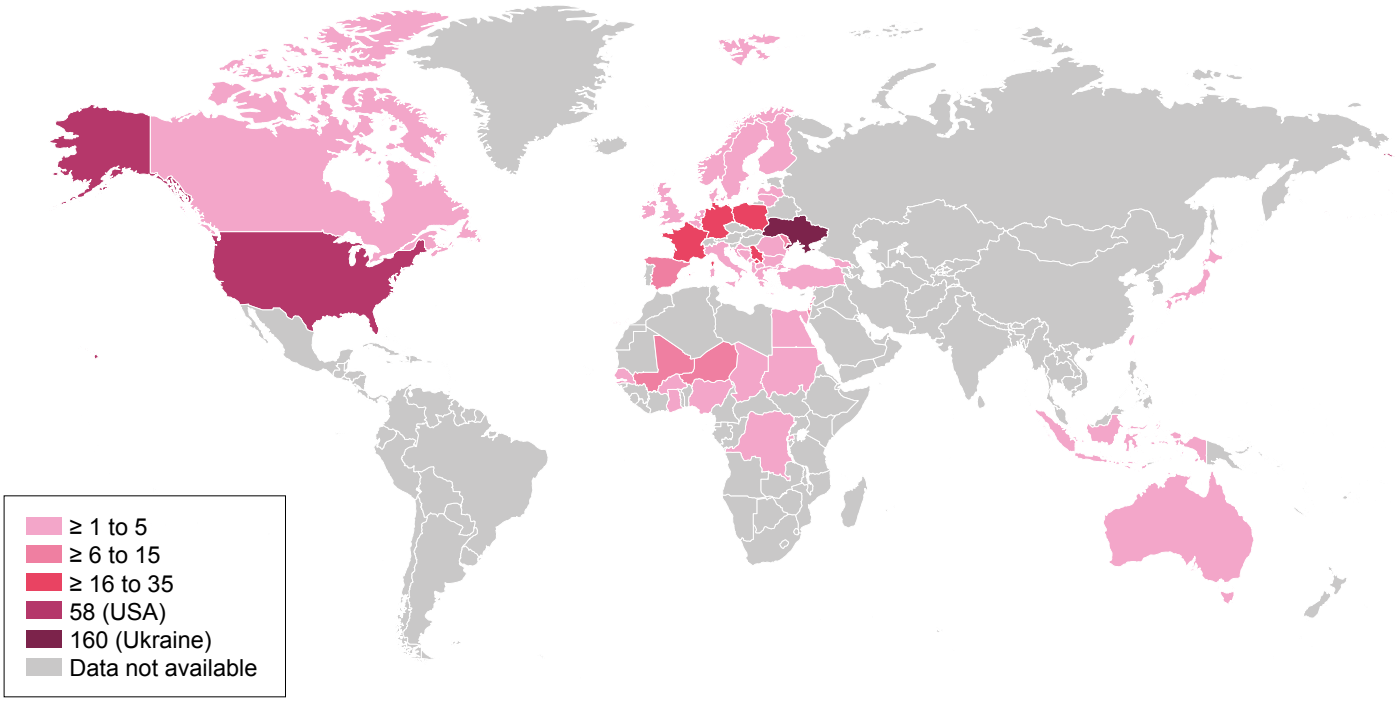


Figure 1: Countries targeted by FIMI incidents observed by the EEAS in 2023.

individuals), the High Representative of the Union for Foreign Affairs and Security Policy/Vice President of the European Commission Josep Borrell (20%), European Commission President Ursula von der Leyen (9%) and French President Emmanuel Macron (4%). Ukrainian First Lady Olena Zelenska has been the victim of at least two FIMI cases recorded by the EEAS. Our analysis in 2023 has also recorded multiple FIMI incidents that used statements by celebrities without their knowledge to conduct FIMI attacks. Personalities like the movie actors Elijah Wood, Nicolas Cage, Margot Robbie, or the author Stephen King and many others saw their voices, statements and faces maliciously used in FIMI incidents with the obvious intention of getting these incidents to reach wider and new audiences and to achieve higher levels of credibility, as was also recently reported by third party sources[22].

Gender-based and anti-LGBTIQ+ FIMI attacks were also recorded during this past year and show a worrying trend that has been also documented in the latest EEAS report "FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity"[23].

In 2023, the EEAS began to systematically encode if **FIMI incidents were conducted in the context of specific events**.

Events can be important motivators triggering FIMI activity, either in anticipation of these events, and with the intention of influencing them and perceptions of them, or as a reaction to events that provide an opportunity to reiterate pre-existing narratives.

Out of the 750 cases within the scope of this 2nd Report, 160 FIMI cases were judged likely to be linked to 94 individual events. Events that may trigger FIMI activity span a wide range of types:

- **Communication and statements by public figures**. This can include speeches by politicians or interviews, but also publications on various platforms.
- **Political summits** (e.g. the 2023 NATO summit in Vilnius or meetings of the G7 and European Council)
- **Diplomatic negotiations** (e.g. peace or trade talks)
- **Electoral events** (e.g. elections or referenda)
- Natural or man-made **emergencies**, **crises and disasters** (e.g. shootings, the Turkey-Syria earthquake in February 2023 or the massacre in Bucha, Ukraine)
- **Military or security incidents** (e.g. the Hamas attack against Israel in October 2023 or the coup in Niger in July 2023)
- **Observances** (e.g. Ukraine's independence day on 24 August)
- **Official visits** (e.g. Volodymyr Zelenskyy's visit to the Canadian Parliament in September 2023)
- **Public policy output** (for instance, various formal products from public bodies, including legislation, recommendations, reports or conclusions).

The events that triggered the most FIMI cases in the sample included the 7 October 2023 Hamas attack on Israel, the 26 July 2023 coup d'état in Niger and HRVP Borrell's speech at the 7 February 2023 "Beyond Disinformation" conference, where the 1st EEAS Report on FIMI Threats was presented.

The vast variety of targeted events suggests that FIMI actors closely follow institutional and media activity and, strategically as well as opportunistically, hijack the attention created by certain events to reach wider audiences and shift the narrative surrounding the event. Therefore, any organisation and political institution can expect adversarial FIMI activity at its own events during moments of high visibility.

Online FIMI content is distributed via coordinated channels. Channels can be websites or social media profiles, groups and pages. To create a FIMI case, threat actors seed, share and amplify content across a variety of channels, inter alia to create the illusion of authentic discussion and interest or to obfuscate the origins of FIMI content. Cross-platform coordination is the default. For (a simplified) example: a forged document is first uploaded to an unknown, newly created website, then linked to by inauthentic accounts on various social media. These posts are then re-shared on known aggregator accounts and this "discussion" ultimately reported on by more established sites.[24]

In deconstructing the chain of amplification steps across the sample cases, around 4 000 different channels were identified. Most channels only occurred once or twice across all cases while others, particularly channels on Telegram, have been observed to be involved in dozens of cases (up to 84), facilitating the seeding, amplification and dissemination of FIMI content. The identified channels were active 9 800 times across the 750 cases. The most often used platforms were Telegram (496 times) and X (formerly Twitter, 452 times) but channel activity was

also observed on Facebook, VKontakte (VK), Youtube, Odnoklassniki (OK), TikTok, alternative, smaller video-focused platforms, Reddit and others.

Artificial Intelligence is not (yet) the biggest threat. The advancements in generative artificial intelligence capabilities and public availability have fuelled intense discussions, including as to their potential misuse for FIMI and disinformation purposes[25]. FIMI actors were quick to experiment with these newly available capabilities to produce synthetic media[26] in 2022[27] and continued testing the use of AI throughout 2023. As for example in November 2023, when a synthetically altered video tried to convince Ukrainians to launch a coup[28]. Or in late December 2023, when an AI-generated video of Moldovan President Maia Sandu was shared by newly created accounts pretending to be authentic channels of the Moldovan government.[29] Cases of AI-generated audio imitating the voices of politicians have been reported in the UK[30] and Slovakia[31] – in the latter case just two days before the elections.

While there have been FIMI cases using AI-generated media within the 750 cases observed by the EEAS, they constitute a minority of less than 20. Usage of AI in FIMI currently focuses on enhancing two stages of the FIMI kill chain in particular: "creating content" and "establishing legitimacy". The vast majority of the techniques used to "create content" in non-AI cases remains the repurposing of existing content in the form of images, such as memes, photos or screenshots, as well as edited video clips or articles. These techniques already constitute low-cost elements in FIMI attacks and the objective for FIMI actors remains to make the content believable and to make its distribution appear organic. While AI-generated content could increase the credibility of FIMI content, its inauthentic distribution patterns remain. Overall**, AI usage in FIMI operations, as observed in 2023, constituted an evolution rather than a revolution,** with existing response approaches remaining applicable – such as the use of anti-spam measures.[32]

A more plausible scenario than automated AI information manipulation, in the short term, is the exploitation of the heightened attention to the threat posed by AI. Generating coverage of otherwise low-visibility or contained FIMI attacks that feature AI-generated elements may be the objective of threat actors, in order to gain access to a wide audience and inflate the real threat posed.

The explosive growth and availability of **AI tools may even hold more benefits for defenders than attackers**. Custom training, tutoring and assistance can democratise access to fields relevant for FIMI research, like public interest and ethical OSINT, programming or technical writing. Or it can make existing research more accessible. "Responsible experimentation with generative AI tools"[33] will keep the FIMI defender community informed of the real risks posed by AI as well as help identify where it can enhance defender capabilities.

As this chapter shows, the threat and the ways in which information is being manipulated are constantly evolving. It is therefore crucial that the responses to the threat are adaptive enough to account for new tactics, techniques and procedures used by threat actors, and enacted in a timely fashion. To support this further, the next chapter will outline a proposal for a "FIMI Response Framework".

3 FROM ANALYSIS TO ACTION: A RESPONSE FRAMEWORK TO FIMI THREATS

The EEAS has been leading the way in advancing the conceptualisation and practical implementation of methods to analyse and systematically understand Foreign Information Manipulation and Interference (FIMI). Delivering on the commitments made under the **Strategic Compass**[34]**,** as well as in line with objectives of the **European Democracy Action Plan**[35], the 1st and the present 2nd report on FIMI threats respond to the following main needs:

1. A **common terminology of Foreign Information Manipulation and Interference (FIMI)** to establish a common understanding of the threat as a challenge of manipulative behaviour and to facilitate whole-of-society collaboration
2. A **common framework** to optimise knowledge generation, exchange and activation based on open-source and collaborative standards
3. An **EU Toolbox of joint responses (FIMI Toolbox)** to inform effective and proportional counter-FIMI measures.

The first edition of the EEAS Report on FIMI Threats outlined an analytical methodology for systematically detecting, analysing and documenting FIMI activities. Building on this methodology, this second report makes the connection between that analysis and threat-informed, adaptive countermeasures. To connect analysis to action, this report proposes an **evidence- and risk-based framework of responses to FIMI ("Response Framework to FIMI Threats")** that enables the activation of adaptive instruments. Each organisation and entity can develop its own Response Framework. In the case of the European Union, the Response Framework can complement the EU FIMI Toolbox, which comprises the instruments that are available to the EU to enact these responses.

The proposed Response Framework is a way to structure the thinking on how to prevent, deter and respond to FIMI. It aims to further our collective ability to tackle this issue and to enable the diverse defender community to develop their own response plans, inviting them to **complement and adapt**.

The Framework highlights the **need for the early implementation of long-term preventive strategies** that are established well before an attack happens. While prevention is key, various types of responses can be implemented at any stage in the lifecycle of a FIMI incident. Different types of responses should be combined as part of an effective response strategy. **Integrating collective analytical insights and response capabilities will continuously improve our collective preparedness**. The key point of the model is that the **successful implementation of responses demands a whole-of-society collaboration**. No one in the defender community can counter the threat alone.

This third chapter will outline:

1. Why FIMI needs to be understood as a complex threat, endangering areas from national and global security to democracy, social cohesion and human rights. This will include an explanation of the FIMI Toolbox.
2. How to methodologically develop a Response Framework to FIMI threats and how this is interconnected with the analysis of FIMI incidents.
3. How to practically implement the framework to prevent, prepare for, respond to and recover from FIMI attacks.

Chapter Four will apply the Response Framework outlined in this section to the specific case of FIMI during elections.

MULTIPLE THREATS, MULTILEVEL RESPONSES

The threats to the information environment are cross-cutting and cannot be limited – neither do they stop at borders, nor do they stop from focussing on any topic that could be useful to sow division. Likewise, such threats cut across different fields: **disinformation**, that is the intentional sharing of false and/or misleading content**, has been described as a threat to democratic processes and institutions, as well as to social cohesion**[36]**.** The same applies to Foreign Information Manipulation and Interference – foreign actors seeking to exacerbate societal divisions, undermine the credibility of governments and institutions, target the integrity of elections and increase control over the information environment at home and abroad. In fact, the goal is not only to shape the global narratives, but also to suppress and silence dissenting voices. FIMI activity has also been shown to have a harmful impact on individuals or groups. This includes journalists, dissidents or civil society organisations who are targeted by suppression tactics, such as bullying, harassment or threats. It can also target groups of people due to their identity, such as FIMI activity targeting LGBTIQ+ people[37].

Therefore, FIMI also **poses a threat to the individual's human rights**.

The Russian full-scale invasion of Ukraine has shed more light on how FIMI has been used as a strategic and coordinated policy and tool in the preparation and execution of the military aggression against Ukraine. This has highlighted that the harm of FIMI activities goes beyond the impact on democracy and society – it can also be used as an instrument of war. In this context, **FIMI and disinformation can have a negative impact on national and global security**[38] **that needs to be addressed with proportional responses.**

Threat actors are not using FIMI as a sporadic opportunity to interfere, but as a strategic instrument of their foreign policy. FIMI is considered a security threat, as well as a threat to society and democracy, and the response repertoire against FIMI needs to mirror this complexity. Therefore, there is not just one single solution for addressing the threat, not just one response that will mitigate all the risks and threats.

In order to tackle such multi-faceted and multi-level threats, the EU has developed the FIMI Toolbox:

Figure 2: Visualisation of the FIMI Toolbox: Situational Awareness, Resilience Building, Disruption and Regulation and EU External Action.

EXPANDING THE SCOPE OF RESPONSE TO FIMI – THE FIMI TOOLBOX

In recent years, the European Union has established many instruments that enable Institutions and Member States to address FIMI, while fully respecting fundamental rights and freedoms. The FIMI Toolbox outlines different areas and instruments that together constitute a robust and comprehensive framework for tackling FIMI. The toolbox includes short-, medium- and long-term measures – from prevention to reaction – and it is a dynamic system in order to account for the constant evolution of the threat. Existing instruments can be complemented, where appropriate, by new instruments. Figure 2 should also not be regarded as an exhaustive list of instruments, but aims to give an overview over the diversity of them across the four different areas. It is also important to note that many of these instruments help to support and enable the EU's civilian and military missions and operations (CSDP[39] missions and operations) to tackle FIMI in their geographical theatres, as set out in the Strategic Compass on Security and Defence.

The FIMI Toolbox should also be seen as complementary to other Toolboxes, in particular the EU's Hybrid Toolbox. Cooperation across the domains is crucial to use them to their full potential. Moreover, in order to tackle FIMI, it is essential to cooperate with other players in the defender community – following the "whole-of-society" approach.

The instruments can be grouped into four dimensions:

1. **Situational Awareness:** A thorough understanding of the threat is a key prerequisite, to inform which responses and which responder are most appropriate.
2. **Resilience Building:** Examples include strategic communications, the cooperation in the EU's Rapid Alert System or efforts to inform and raise awareness, which are ongoing on a permanent basis.
3. **Disruption and Regulation:** Efforts to further trust, transparency and safety in the information environment, such as the Digital Services Act, are permanent instruments that shape the environment in which responses to FIMI are taken.
4. **Measures related to EU external action, including CFSP[40] and diplomatic responses:** This dimension opens up instruments in the area of foreign and security policy, such as international cooperation, the G7 Rapid Response Mechanism or the sanctions on Kremlin-controlled outlets like RT and Sputnik.

This report aims to highlight how the FIMI Toolbox and the Response Framework are two sides of the same coin and mutually reinforcing. The FIMI Toolbox is the structural framework in which the EU continues to develop its instruments to prevent, deter and respond to FIMI, which dovetails with the Response Framework for operational responses.

In order to be successful, responses to FIMI need to take place at different levels and be adapted to the type of attack. The first edition of the EEAS report on FIMI Threats detailed the steps and Open Source frameworks for a standardised methodology to understand and share threat information between members of the defender community and to identify the type of threat encountered.[41] This methodology outlined the analysis of behavioural patterns – categorised in Tactics, Techniques and Procedures (TTPs). Inspired by defence models from cybersecurity, the **Kill Chain perspective**[42] **applied to FIMI gives us the possibility to understand which manipulative techniques have been used in each stage of an incident** – TTPs used in the planning, preparation and the execution phases of an attack. **The current report expands the analysis to match responses and upgrade the repertoire of countermeasures**.

While progress has been made in the analytical and policy areas, the **functional and coordinated activation of responses remains a challenge.** The practical implementation of countermeasures needs to be conceptualised in a Response Framework that helps practitioners to better connect analysis to responses and activate them in a network of responders. The Response Framework to FIMI Threats will help answer the questions: Which adequate responses should be activated? When should they be activated? Who can activate and implement them? And how can they be activated?

PROTECT AND REACT: ELEMENTS OF A FRAMEWORK FOR RESPONSES TO FIMI

The Response Framework is a guide to how defenders can prevent, prepare for, respond to and recover from FIMI attacks while continuously improving their security in future attacks. The framework can be used by different types of organisation and offers the possibility of being tailored to individual resources and capabilities. The model incorporates elements of risk assessment and management, crisis management and cyber defence[43]. The Framework is composed of three main elements:

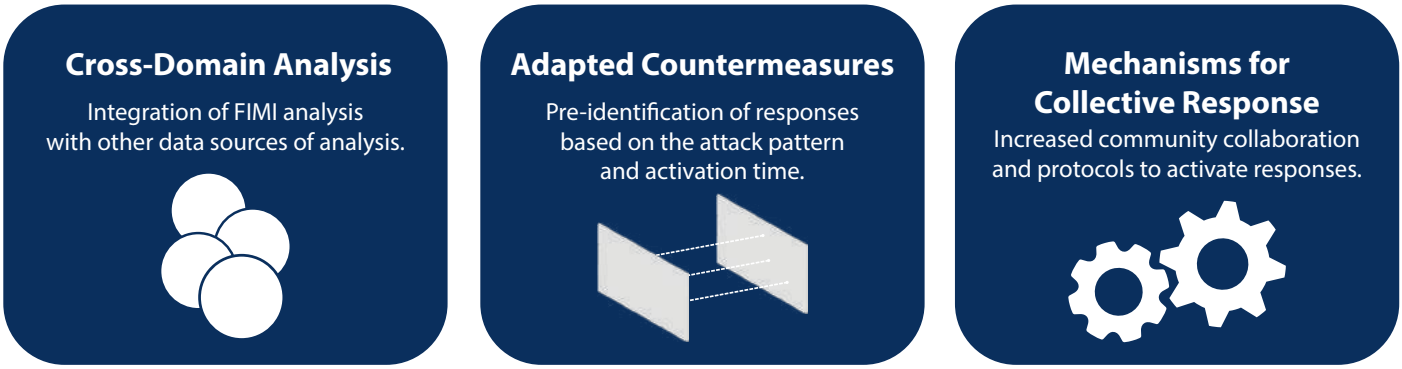


Figure 3: Elements of the Response Framework to FIMI Threats.

Cross-Domain Analysis: An Approach to Understand the Bigger Picture

The tactical analysis of FIMI described in the first EEAS report on FIMI threats proposed a methodological model to extract findings based on Open Source information. Open Source data can show solid behavioural, contextual and technical[44] indicators. However, the results exclusively based on Open Source information cover only a part of the picture and analysts can face limitations in attributing operations. For example, Open Source evidence can demonstrate publication patterns in a network of coordinated websites. However, in order to connect this network to an infrastructure or to a threat actor, analysts may need to complement with other types of data from different domains, like cybersecurity.

In this framework, **the cross-domain dimension of FIMI analysis refers to the need to complement the results of FIMI investigations – based on Open Source information – with other types of data**[45], such as proprietary or classified information[46]. Merging insights from FIMI analysis, cybersecurity[47], Information Environment Assessment[48], Public Opinion Research, Human Factor Analysis and others will help to generate a more holistic understanding of FIMI and related threats. Achieving interoperability between these various information types remains a priority to quickly understand the bigger picture.

No Silver Bullet Against FIMI: Repository of Adaptive Countermeasures

The second element of the Response Framework is a catalogue of pre-identified responses mapped to the types of attack. Based on the detection and analysis of the attack patterns, this Defense Arsenal will help to activate short- and long-term responses. **A logical connection between detection, analysis and responses optimises the strategy and the activation of countermeasures.**

The cybersecurity-inspired kill chain approach applied to information manipulation helps to break down and structure how to analyse and disrupt FIMI activities[49]. However, while cybersecurity has been a source of inspiration to conceptualise the work on FIMI, there are distinctions between the two domains that require expanding the scope of countermeasures. **Compared to cyber, FIMI has a stronger socio-cognitive component that also plays a role in the analysis and the design of responses beyond the technical dimension.**

Creating the Response Arsenal of possible and suitable countermeasures requires the same cooperative mapping and collection effort as for the Attack Arsenal that collects and structures observed manipulative tactics, techniques and procedures (TTPs). Mapping observed countermeasures and linking them to the types of attacks used will aid decision-making, especially in case of crises.

In the FIMI domain, the technical analysis of TTPs is a key element that allows us to understand how a threat actor conducts their attack across different stages of an incident (from planning to preparation and execution phases). This focus on identifying TTPs also enables

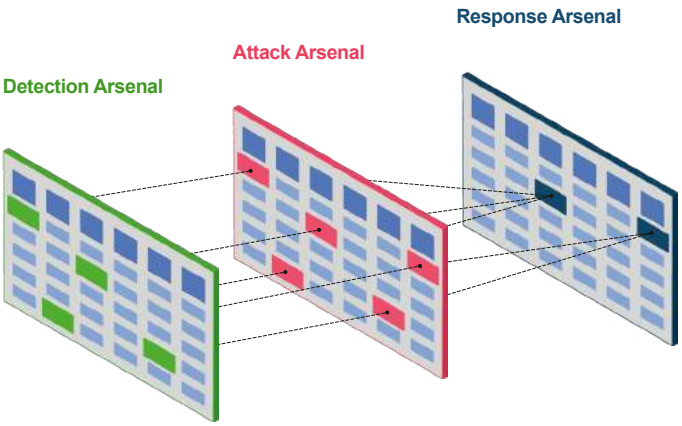


Figure 4: Matrix visualisation of the FIMI Detection, Attack and Response Arsenals inspired by MITRE's offensive and defensive technique relationships (ATT&CK and D3FEND)[50]

the collective creation of the **Detection Arsenal for the defender community,** which provides good case practices and solutions for identifying the presence of certain TTPs.

In FIMI, the behavioural analysis of TTPs is complemented with other non-technical indicators described in the ABCDE Framework (such as narratives, nature of the threat actor, triggering events or types of targets). Therefore, **it is the combination of both – TTPs and contextual indicators – that is used to inform this Response Arsenal** Over time, a better understanding of the Attack Arsenal can lead to pre-identification of specific responses that proved effective in mitigating certain types of attacks.

Defenders should expand their counter-activities to include periods outside a moment of crisis. **Preventing, deterring and responding to FIMI is a long-term process that combines preventive and long-term activities with specific reactive measures in critical moments**. The Response Arsenal should be composed by countermeasures that are activated before, during and after an incident. These activities can be combined and used complementarily.

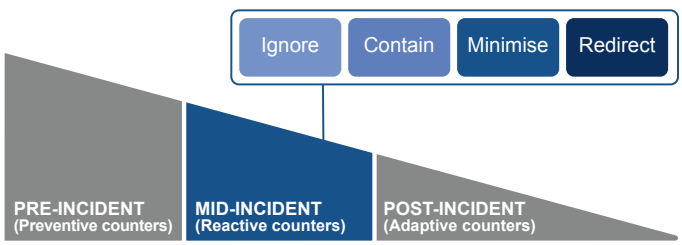


Figure 5: Types of response by activation time and quantity of available countermeasures

Pre-incident Countermeasures

Prevention plays a significant role in countering FIMI and its importance lies in its ability to address FIMI at its root rather than dealing with its consequences. The defender community can establish proactive countermeasures in anticipation of FIMI incidents before they gain traction or escalate. During this period, more types of counter-activities are available and can be activated. **The pre-incident activities have long-term objectives to build societal resilience and aim at reducing the attack surface for FIMI**. Some examples are building engaging online communities with a purpose, exercising good community management, identifying and closing data voids[51] or enhancing media literacy.

Moreover, **pre-incident countermeasures increase the capacity of the defender community to defend against and identify threats and prepare for future crises**. Preventive countermeasures established in this period help to better plan and prepare future decision-making processes and anticipate problems. These measures may include fostering collaboration between stakeholders or developing policy and mechanisms available for times of crisis.

EXAMPLES OF PRE-INCIDENT COUNTERMEASURES[52]

- Creation of common Analytical Frameworks and Methodology
- Implementation of programmes of Media and Information Literacy, support for Independent Media, support to Civil Society and support to Fact Checking initiatives
- Use of Strategic Communication activities to build resilience and trust
- Investment in Capacity Building to enable members of the defender community
- Creation of policy instruments (like the AI Act, Code of Practice on Disinformation or the Digital Services Act)

Mid-incident Countermeasures

In the event of an incident, it is too late to trigger preventive mechanisms. Instead, it is time to activate reactive countermeasures from the Response Arsenal, specifically adapted to the type of attack. **The primary goals of reactive responses are to contain the incident from spreading further, minimise the impact of the attack, and recover from the potential harm.**

On the one hand, the analysis of TTPs can lead us to find effective technical responses to disrupt the distribution chain of an incident. On the other hand, each incident has contextual or regional specificities that need to be considered in order to assess the suitability of a counter. Therefore, **defenders will need a Risk Assessment Matrix to prioritise threats according to their severity and likelihood. Being able to assess the risk level of an incident helps to select proportionate countermeasures.** The risk indicators would be oganisation-specific and tailored to the information environment in question[53].

To effectively deploy reactive responses during a FIMI incident, four distinct sets of countermeasures are available, depending on the objective of our actions:

- **Ignore:** While it may be tempting to directly confront manipulated information, doing so can inadvertently increase the damage. **The evaluation of the likely risk and impact of the response can lead to the conclusion that any reactive response should be avoided.** This non-reactive strategy should be complemented by other proactive measures that help to improve situational awareness and build resilience.

- **Contain:** In case of an incident, **containment strategies primarily aim to prevent the spread of an incident by hindering its further development as anticipated by the kill chain**. The objective is that the FIMI incident does not gain traction or escalate further. This type of intervention is predominantly applicable when the detection mechanisms identify incidents in their initial phases.
  This strategy does neither try to tackle the steps already taken by the attacker nor try to reduce the footprint of the attack. Instead, **the actions focus on the next predictable steps in the distribution chain, to prevent the FIMI incident from progressing to the next tactical step of the attack and potentially reaches new audiences.**

EXAMPLES OF CONTAINMENT COUNTERMEASURES

- Pre-bunk a story before it strikes
- Early exposure of a network
- Rapidly inform stakeholders of your findings to active contingency plans
- Restrict amplification of manipulated content
- Prompt audiences when they engage with a manipulated content

- **Minimise**: In the event of a FIMI incident, **defenders can reduce or disable the visibility of FIMI content already distributed.** Content moderation mechanisms are enabled when the content violates transparent policies or guidelines. Therefore, **these actions will considerably depend on existing regulations or mechanisms put in place during the pre-incident phase**. Limiting the reach of an incident needs to be proportionate and applicable in cases where there are strong behavioural indicators of manipulation, such as the use of coordinated, inauthentic behaviour (CIB) or the use of illegal content.

EXAMPLES OF MINIMISING COUNTERMEASURES

- Remove content violating pre-existing community guidelines: coordinated and inauthentic behaviour, impersonations, malicious false content, non-transparent paid ads.
- Remove or transfer websites, channels or accounts involved in FIMI activities
- Issue legal notices

- **Redirect**: In cases where minimisation techniques cannot be deployed anymore, or in complementarity, other types of response can be implemented to readdress and redefine the situation while mitigating the potential effects of a FIMI attack. Whilst FIMI incidents give visibility to specific topics, **defenders can use moments of crisis as an opportunity to redirect the focus of attention and take ownership of the situation**. These activities target new and old audiences already exposed to the FIMI activity.

EXAMPLES OF REDIRECTING COUNTERMEASURES

- Expose and debunk the incident, manipulation techniques and threat actor objectives
- Provide suitable, easily accessible, reliable information
- Update and adapt misused content to redirect audiences to verified content
- Use humour-based responses[54]
- Label false and misleading content with warnings or debunks by third-party organisations
- Give visibility to reliable content

Post-incident Countermeasures

After an incident has passed, defenders still have countermeasures at their disposal. **Countermeasures happening in the aftermath of an incident aim at recovery and deterrence of future attacks.** Moreover, measures in this period are carefully designed not only to address the immediate consequences of an incident but also **to facilitate long-term learning and enhance preparedness for future incidents**.

EXAMPLES OF POST-INCIDENT COUNTERMEASURES

- Information sharing with relevant stakeholders to reinforce situational awareness
- Capacity building among the defender community, based on insights gained from previous incidents
- Identify and limit financial incentives for FIMI activities
- Activate diplomatic responses
- Deploy legal responses, including sanctions
- Monitor and respond to evasion tactics circumventing legal responses
- Reinforce and adapt response instruments based on lessons learnt

Shared Problem, Shared Solution. Network of Responders and Responses

No matter at which stage responses are to be taken – be it before, in the middle of or following a FIMI incident – it may be that a certain response option is not within the realm of a specific stakeholder or that other stakeholders would be more effective in implementing them. Therefore, in light of the response framework, it needs to be considered who is best placed to enact the response and which processes are needed to activate them. Depending on the context of the attack, **the opportunities to respond to FIMI are distributed between stakeholders with different competences**. In this context, **it is essential to establish collaborative networks of stakeholders that get active, depending on the circumstances of each attack**[55].

The diverse defender community is composed of a wide range of actors (governments, private sector, civil society, independent media, academia etc.) each equipped with different resources, mandates and capabilities. By bringing in this unique set of knowledge and analytical insights, depending on the situation, the defender community strengthens its collective resilience and ability to effectively tackle FIMI.

Below is an example of collaboration in the defender community to address the specific issue of FIMI targeting LGBTIQ+ communities.

FIMI TARGETING LGBTIQ+ PEOPLE: WELL-INFORMED ANALYSIS TO PROTECT HUMAN RIGHTS AND DIVERSITY

In 2023, EEAS Stratcom carried out a project to understand how FIMI activities target LGBTIQ+ communities and how stakeholder collaboration could contribute to countering this divisive threat. Besides the empirical analysis of documented cases of FIMI targeting LGBTIQ+ identities, the project brought together for the first time a wide number of stakeholders to discuss and design specific collaborative responses to the threat. More than 100 stakeholders (from civil society, platforms, government and academia) from different regions of the world participated in two events organised in Brussels. The report "FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity"[56] brings together the conclusions of the discussions between different members of the defender community in a format of recommendations to overcome the lack of coordination, cooperation and communication among different stakeholders. The project is a key example of stakeholder collaboration in order to design mechanisms for collective response specific to FIMI activities targeting LGBTIQ+ communities.

Figure 6: Picture of the conference held in Brussels on the 23rd of October 2023 and the cover of the report.

The members of the network should be prepared and well equipped to collaborate, share knowledge and coordinate efforts at different stages. The design of collective processes and protocols to activate responses should aim at preventing future attacks. **The mechanisms for collective response outline the steps that need to be taken when an incident occurs, ensuring that all relevant stakeholders are informed and ready to act swiftly and in a coordinated manner.** These systems provide a structured approach by establishing procedures that guide stakeholders to report, receive and respond to FIMI incidents. Moreover, in case of attacks that put in danger the physical integrity of people and operations, protocols should include real life security elements[57].

Examples of stakeholders	Examples of mechanisms for collective response
▪ Governments ▪ Government Agencies ▪ National Security Agencies ▪ Diplomatic Corps ▪ Law Enforcement Agencies and Media Regulations ▪ International Organisations and Networks ▪ Media Organisations ▪ Tech Companies ▪ Social Media Platforms ▪ Hosting Service Providers ▪ Civil Society ▪ Advocacy Groups ▪ Think Tanks ▪ Academia/Research Institutions ▪ Users/Citizens ▪ Cybersecurity Experts ▪ Ethical Hackers	▪ **Create internal dedicated response teams** specialised in translating analytical insights into responses and launch coordination mechanisms with relevant stakeholders. ▪ **Create dedicated forums or bodies** to exchange information and coordinate responses (such as ISACs, task forces or working groups). ▪ **Establish internal and external communication protocols, escalation channels and alerting systems** to promptly notify. ▪ **Implement internal and external protocols to initiate specific actions** after an incident has been identified. ▪ **Build protocols with relevant stakeholders** to ensure that information is understood and acted upon. ▪ **Coordinate public communication strategies** with other stakeholders.

While at first glance it might seem that the list of stakeholders is very long, the connections and ties within this network require continuous nurturing and development. The Response Framework aims to help make the links between those partners who can enact responses, to build the links within the network in a more systematic manner and to ensure that the community can use its instruments in a collective way.

TWO GEARS, ONE ENGINE: PRACTICAL IMPLEMENTATION OF THE RESPONSE FRAMEWORK TO FIMI THREATS

At an operational level, it is of course important that the Analysis Cycle and the Response Cycle are not operating in silos. They need to be integrated into one process, so that the analysis can feed the responses, and the insights from the responses can then again be taken into account in the analysis. **The Threat Analysis Cycle, such as the one described in the first EEAS report on FIMI Threats, is interconnected with the response workflow**. The response workflow also includes the assessment of threats, the design and activation of countermeasures and the evaluation of counteractivities' effects.

The Response Framework to FIMI Threats introduces a systematic way of organising and conceptualising the analysis and response processes. This system requires continuous information-sharing between both processes. Moreover, its successful implementation is subject to a constant evaluation of the system in order to apply lessons learnt to update and adapt the Response Arsenal.

The workflow of the Response Framework coordinates actions in the different phases of the Threat Analysis Cycle and the Response Cycle. The process starts with a preventive phase - before an incident occurs - that includes a Risk Assessment evaluation of potential threats and vulnerabilities followed by the design of a Response Strategy. After that, the results of the Risk Assessment inform the Threat Analysis Cycle to set the Strategic Monitoring priorities. The application of the EEAS common framework and methodology[58], outlined in the 1st EEAS report on FIMI threats, will lead to a systematic detection and investigation of threats.

When a threat is detected, the whole workflow enters into action. First, with the activation of alerting mechanisms. Second, with the evaluation and selection of adequate countermeasures according to the results of the analysis and the designed Response Strategy. And third, with the activation of the mechanisms for collective response to mobilise relevant stakeholders. The Response Framework is designed to be self-reinforcing. That is, after an incident concluded, the insights generated during the analysis and counter steps improve the next iteration of both Cycles. **Evidence-informed remediation strategies will make future attacks more difficult.**

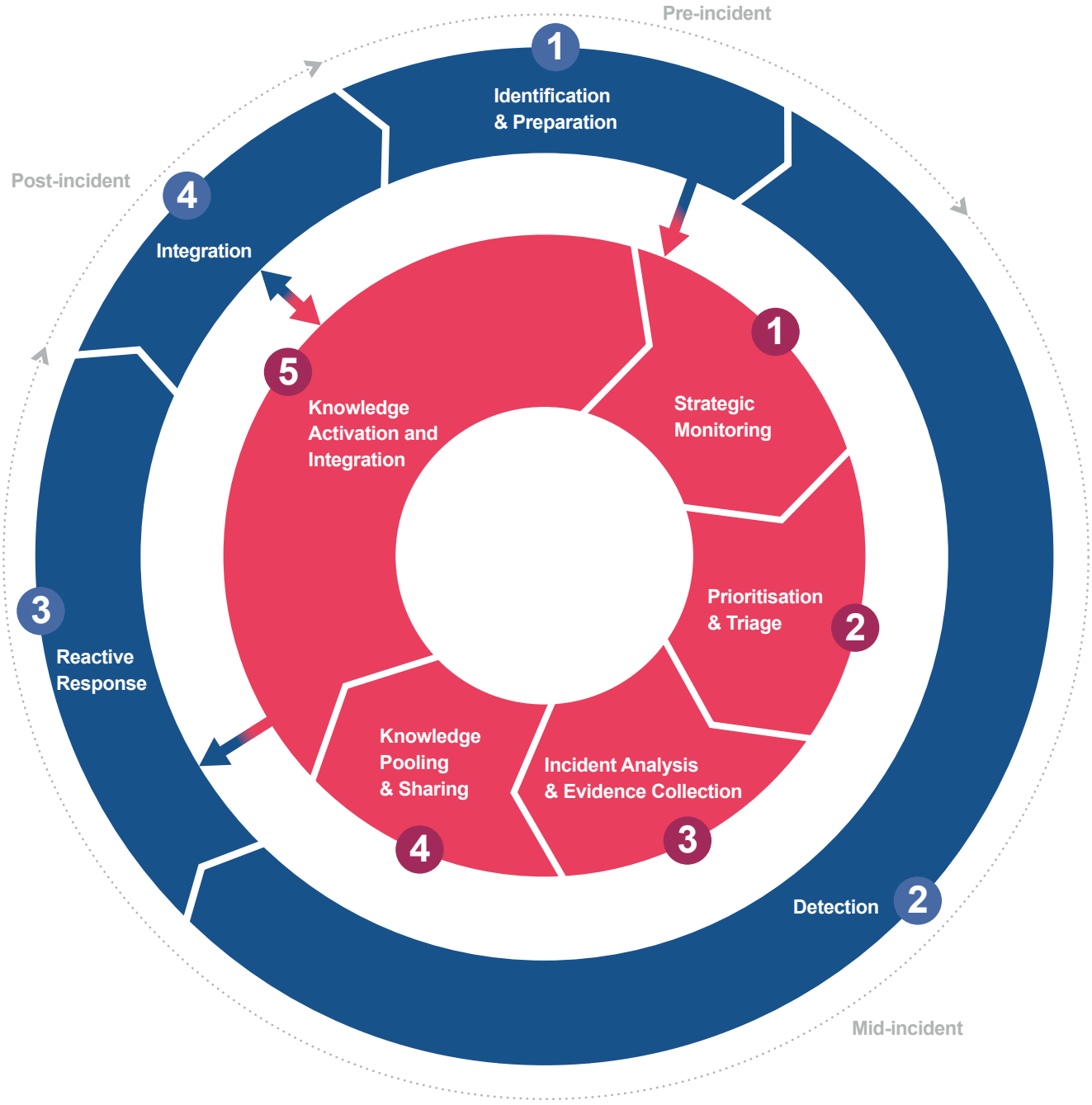
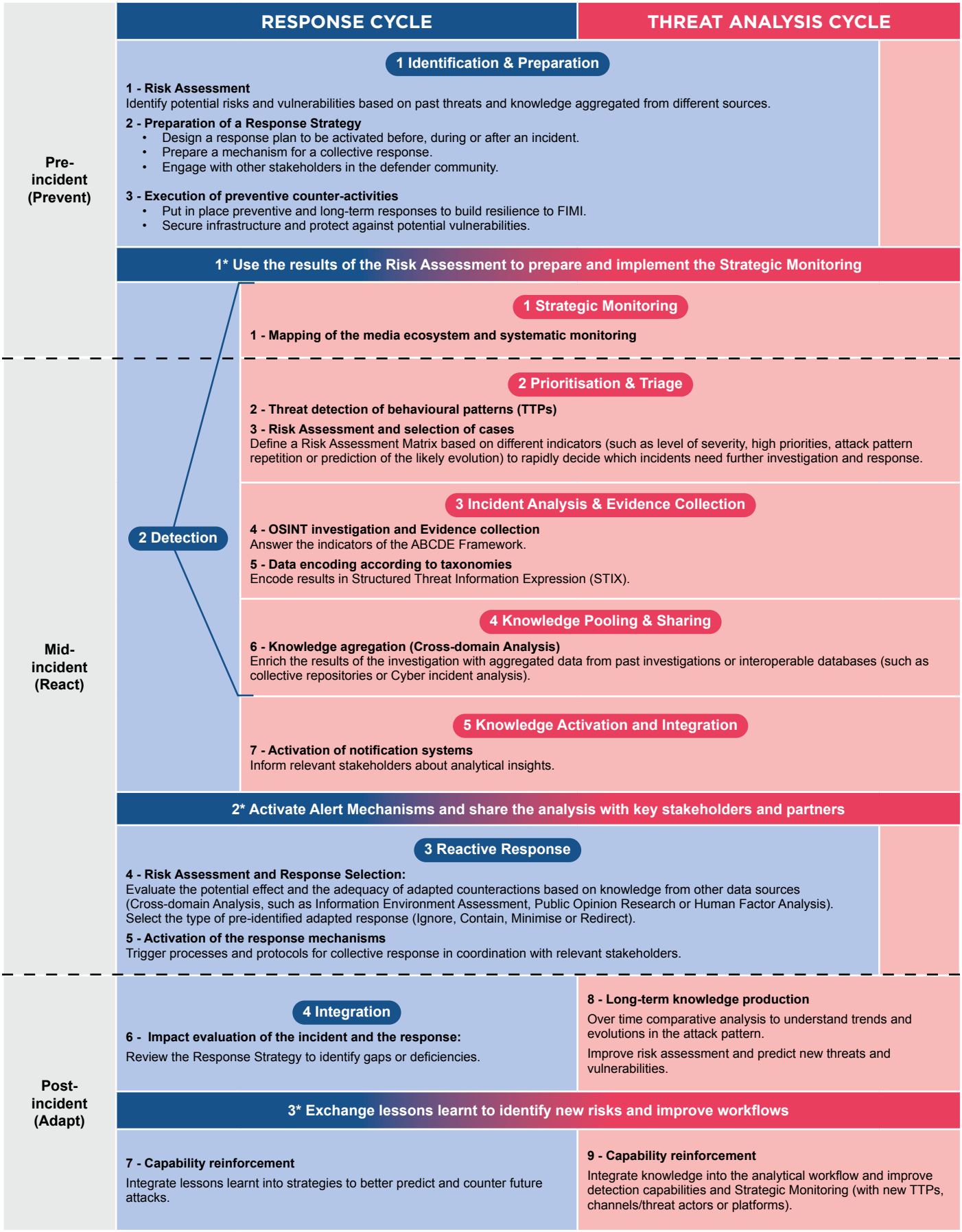


Figure 7: Interconnection between the Threat Analysis and the Response Cycles.

The following table describes in detail the different steps and interconnections between the Threat Analysis and the Response Cycles.



TOWARDS NETWORKED DEFENCE: STRONGER TOGETHER

In summary, **the Response Framework provides a structured approach for responding to short- and long-term FIMI threats by establishing interconnected workflows that guide stakeholders through necessary steps to activate effective and proportionate countermeasures.** Whilst the framework is conceptual in nature, its design guides the practical implementation of response plans for a wide range of stakeholders.

With the common framework and methodology to systematically collect evidence of FIMI having made significant progress, the community's focus can now evolve to strengthen the common approach to responses. Similarly to the use of common frameworks to collect, map and exchange information on manipulative TTPs, collective standards can be used to create, map and exchange information on responses. The STIX standard already enables the encoding of responses taken against FIMI via the "Course of Action" STIX object[59]. By encoding threat information together with the countermeasures deployed, not only it is possible to map out the landscape of countermeasures and who is best placed to deploy them, but also to assess the effectiveness of responses.

Defence against FIMI must be thought as a networked task. **All members of the defender community must assess which role they do and can play in the activation of responses.** As outlined in this chapter, the successful implementation of responses depends on a collaborative approach sustained by processes and protocols that build bridges across members of the defender community.

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,

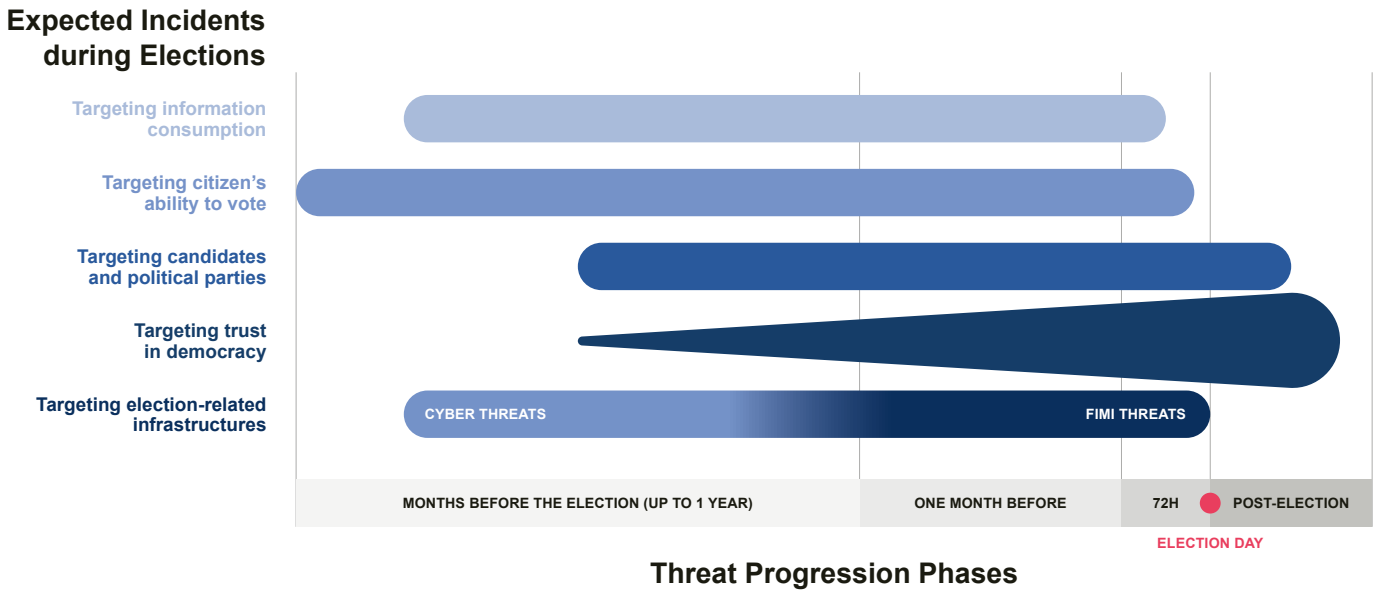


Figure 8: The graph shows the five types of threats to elections on a timeline involving four threat progression phases across the electoral process. The length of the bars shows the distribution of the analysed incidents across the timeline.

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***).

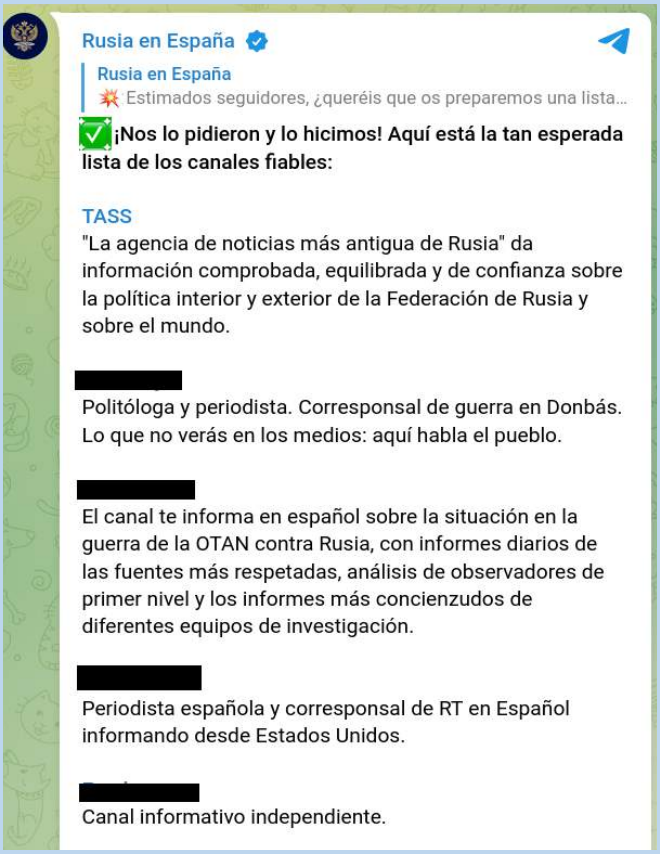


Figure 9: Screenshot of a post from the Telegram account of @EmbajadaRusaEs suggesting a list of sources to follow

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

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***).

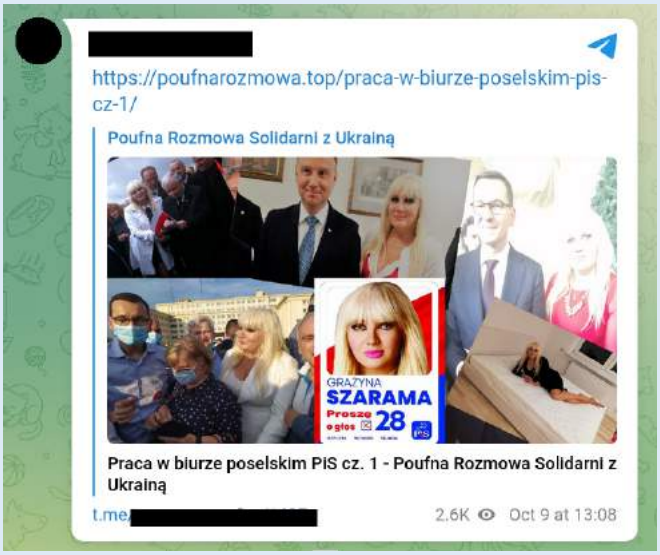


Figure 11: Amplification on Telegram of the leaked files of a candidate running in the Polish elections 2023.

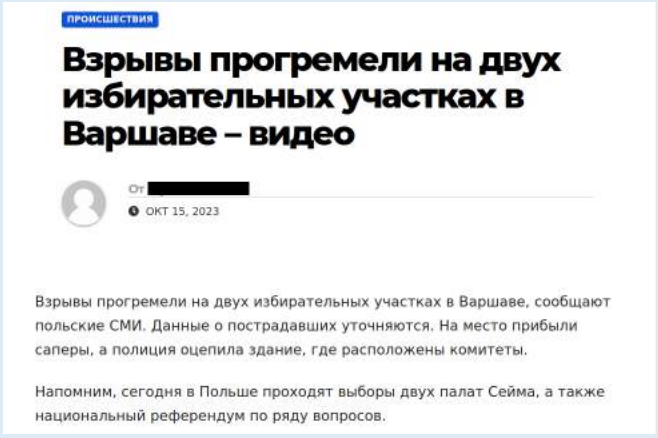


Figure 12: Screenshot from a Russian media outlet. Translation of the title: “Explosions occurred in two polling stations in Warsaw – video”

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.

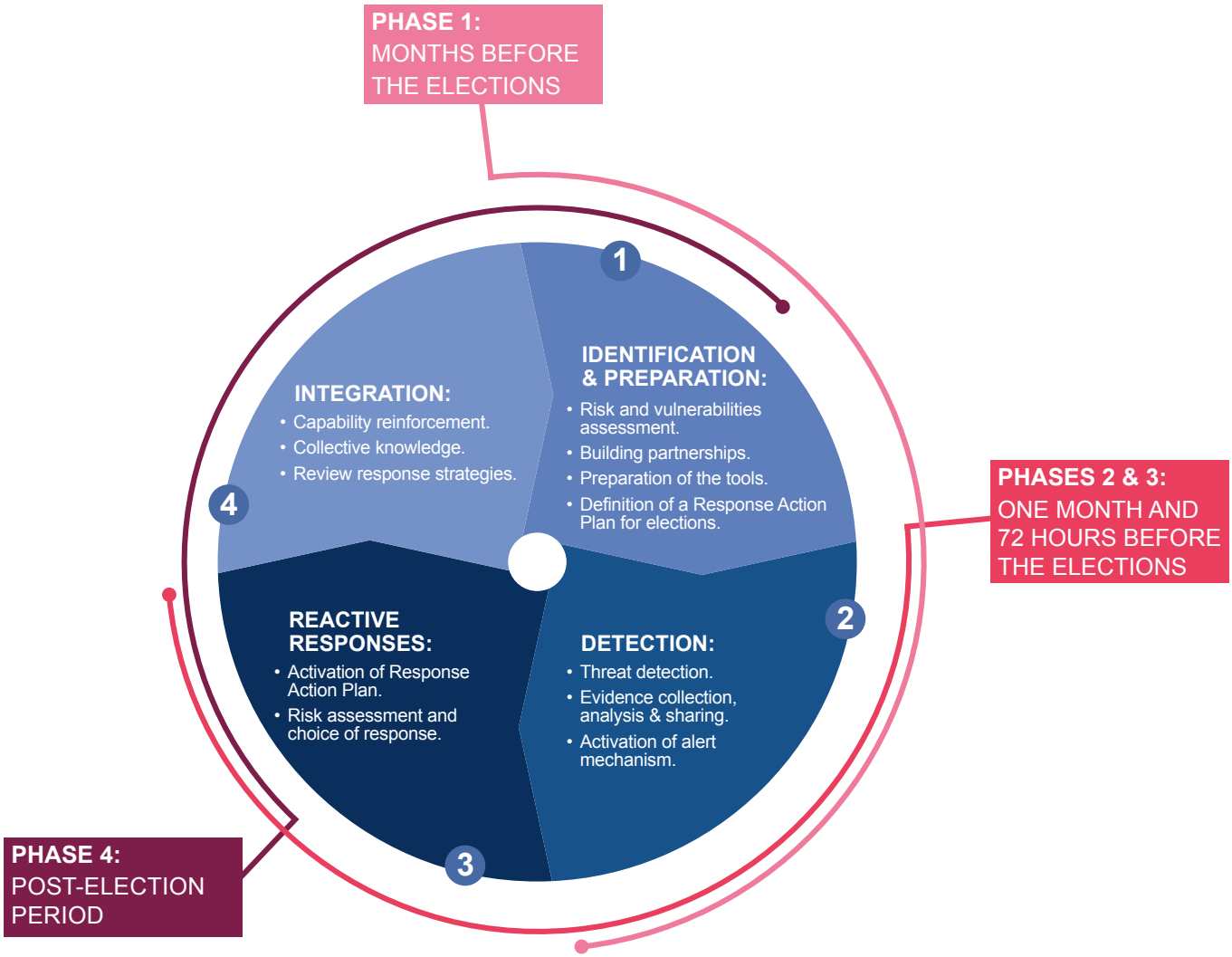


Figure 13: The graph shows a Response Framework applied to elections. The inner cycle shows the different phases of the Framework, which includes elements of both the Threat Analysis Cycle and the Response Cycle (as per Chapter Three). The outer arches represent the threat progression phases of election-related 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.

5 CONCLUSIONS

Ensuring that analysis feeds into timely and effective responses against FIMI is a continuous effort. In a diverse FIMI defender community, everyone contributes to the collective understanding and countering of the threat. The crux lies in effectively linking what we know to what we can do. Therefore, this 2nd Report on FIMI Threats has presented the FIMI Response Framework. Based on a thorough understanding of the threat, the framework aims to help stakeholders link the collective analysis work more directly with the collective response efforts, enabling the activation of effective and proportionate countermeasures to FIMI in a continuously developing threat environment. To further support this networked approach to defending against FIMI, the framework is based on commonly shared, open and collaborative standards.

Threat actors capitalise on the repetitiveness of their action: individual incidents might not achieve wide visibility or be directly impactful, but leaving them unchallenged over time may compound their impact. Any unsuccessful FIMI attack provides a learning opportunity, for attackers but also defenders. Re-running FIMI attacks later or in another country with slight variations may lead to low-impact attacks turning harmful. By exchanging information on observed FIMI attacks, defences and their impact, the defender community can be one step ahead.

In addition to acknowledging the threat that FIMI poses and the need to prevent, deter and respond to it, it is crucial to have a holistic view of the information environment. The concept of information integrity, which has recently gained traction with the work of the United Nations on a Global Code of Conduct for Information Integrity on Digital Platforms[72] and the Global Declaration on Information Integrity Online[73], might offer guiding inspiration.

The term "information integrity" is defined in this Declaration as an information ecosystem that produces accurate, trustworthy, and reliable information, meaning that people can rely on the accuracy of the information they access while being exposed to a variety of ideas. [The] term "information integrity," [can] offer a positive vision of a broader information ecosystem that respects human rights and supports open, safe, secure, prosperous and democratic societies.[74]

Good communication on, and defence against, FIMI in elections starts well in advance. The European Elections will take place between 6 and 9 June 2024. The European Parliament already launched the website elections.europa.eu in 2023 to provide all EU citizens with authoritative information on the elections in all EU languages. To start preparing against FIMI in advance by building communities of purpose is the best means to minimise risk and to be ready for a potential intensification of threat activity around key election moments and beyond.

REFERENCES

1 European External Action Service (EEAS) (October 2021) *Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report.* https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis-division_en

2 *Introduction to STIX™*. https://oasis-open.github.io/cti-documentation/stix/intro

3 Pols, P. (February 2023) *The Unified Kill Chain: Raising Resilience Against Advanced Cyber Attacks.* White Paper. https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

4 European External Action Service (EEAS) (2022) *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security.* https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

5 *About FIMI-ISAC* https://fimi-isac.org/

6 (9 January 2024). New York Times. https://www.nytimes.com/2024/01/09/business/media/election-disinformation-2024.html

7 Council of the European Union (July 2022) *Council conclusions on Foreign Information Manipulation and Interference (FIMI).* https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf

8 Pamment, J. (September 2020) *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework*. Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

9 DISARM Foundation. *DISARM Framework.* created by SJ Terp and Dr. Pablo Breuer. https://www.disarm.foundation/framework

10 Nimmo, B. and Hutchins, E. (March 2023) *Phase-based Tactical Analysis of Online Operations*. Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/2023/03/16/phase-based-tactical-analysis-of-online-operations-pub-89275

11 ObSINT. *Guidelines for public interest OSINT investigations.* https://obsint.eu/

12 OASIS OPEN (16 November 2023) *OASIS Mobilizes Open Source Community to Combat the Spread of Disinformation and Online Harms from Foreign State Actors.* https://www.oasis-open.org/2023/11/16/oasis-defending-against-disinformation-dad-cdm/

13 European Commission (31 May 2023) *Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden.* https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992
European External Action Service (31 May 2023) *Trade and Technology Council Fourth Ministerial – Annex on Foreign information manipulation and interference in third countries.* https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

14 European Council (20 October 2023) *EU-US summit, 20 October 2023.* https://www.consilium.europa.eu/en/meetings/international-summit/2023/10/20/

15 *About FIMI-ISAC* https://fimi-isac.org/

16 VIGINUM (23 August 2023) *RRN: a complex and persistent information manipulation campaign* https://github.com/VIGINUM-FR/Rapports-Techniques

17 Meta. Meta Threat Research Indicator Repository, a dedicated resource for the sharing of Indicators of Compromise (IOCs) and other threat indicators with the external research community. https://github.com/facebook/threat-research

18 Gartner Inc. (16 May 2013) *Definition: Threat Intelligence.* https://www.gartner.com/en/documents/2487216

19 European External Action Service (EEAS) (February 2023) *Opening speech by HRVP Josep Borrell at the EEAS Conference on Foreign Information Manipulation and Interference.* https://www.eeas.europa.eueeas/disinformation-opening-speech-high-representativevice-president-josep-borrell-eeas-conference_en

20 Johnson, B. and Dunne, J. (7 March 2023) *Seeking to undermine democracy and partnerships.* Australian Strategic Policy Institute (ASPI) https://www.aspi.org.au/index.php/report/seeking-undermine-democracy-and-partnerships

21 US State Dept. (7 November 2023) *The Kremlin's Efforts to Covertly Spread Disinformation in Latin America.* https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/
Chequeado (February 2023) *Ucrania: la desinformación alrededor de la guerra.* https://chequeado.com/wp-content/uploads/2023/04/Informe-Ucrania-la-desinformacion-alrededor-de-la-guerra-FINAL.pdf

22 Watts, C. Microsoft (7 December 2023) *Russian influence and cyber operations adapt for long haul and exploit war fatigue.* https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

23 European External Action Service (EEAS) (October 2023) *FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity* https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-LGBTQ-Report-03-Digital%201.pdf

24 EUvsDISINFO (8 July 2019) *Operation Secondary Infektion: The DFRLab Exposes a New Russian Influence Campaign.* https://euvsdisinfo.eu/operation-secondary-infektion-the-dfrlab-exposes-new-russian-influence-campaign/

25 For example:
- Atlantic Council (2023) *Scaling Trust on the Web.* https://www.atlanticcouncil.org/wp-content/uploads/2023/06/scaling-trust-on-the-web_comprehensive-report.pdf; -World Economic Forum (20 January 2024. *Global Risks Report 2024.* https://www.weforum.org/publications/global-risks-report-2024/in-full/

26 "Synthetic media (also known as AI-generated media, generative media, and personalized media) refers to any media created or modified by algorithmic means, especially through the use of artificial intelligence algorithms." https://www.w3.org/community/synthetic-media/wiki/Main_Page

27 Evon, D. (16 March 2022) *Bad Deepfake of Zelenskyy Shared on Ukraine News Site in Reported Hack.* Snopes.
https://www.snopes.com/news/2022/03/16/zelenskyy-deepfake-shared/

28 StopFake (11 August 2023) *Fake: Ukrainian Commander-in-Chief Zaluzhny Is Preparing a Military Coup.*
https://www.stopfake.org/en/fake-ukrainian-commander-in-chief-zaluzhny-is-preparing-a-military-coup/

29 Președinția Republicii Moldova (29 December 2023) *Instituția prezidențială îndeamnă cetățenii să fie atenți față de informațiile false care apar în spațiul public, însoțite de imaginea Președintei Maia Sandu.* https://presedinte.md/rom/presa/institutia-prezidentiala-indeamna-cetatenii-sa-fie-atenti-fata-de-informatiile-false-care-apar-in-spatiul-public-insotite-de-imaginea-presedintei-maia-sandu

30 Full Fact (11 October 2023) *No evidence that audio clip of Keir Starmer supposedly swearing at his staff is genuine.*
https://fullfact.org/news/keir-starmer-audio-swearing/

31 Wired (3 October 2023) *Slovakia's Election Deepfakes Show AI is a Danger to Democracy.* https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/

32 Keast, J. (2023) *Shadow Play.* Australian Strategic Policy Unit (ASPU). https://www.aspi.org.au/report/shadow-play

33 Harvard University (15 November 2023). *Ideas for experimenting with Generative AI: Use cases and things to keep in mind.* https://huit.harvard.edu/news/ai-use-cases

34 European External Action Service (EEAS) (2022) *A Strategic Compass for Security and Defence.* https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

35 European Commission (2020) *A European Democracy Action Plan.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

36 Boyle, J. (May 2022) *European Voices for Healthier Democracies: Combatting Disinformation, Misinformation & Fake News.* Friends of Europe. https://www.friendsofeurope.org/wp/wp-content/uploads/2022/06/DE-Focus-group-report.pdf

37 European External Action Service (EEAS) (October 2023) *FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity* https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-LGBTQ-Report-03-Digital%201.pdf

38 Jeangène Vilmer, J-B Escorcia, A. Guillaume, M. Herrera J. (August 2018) I*nformation Manipulation: A Challenge for Our Democracies.* Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the French Ministry for the Armed Forces. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

39 CSDP (Common Security and Defence Policy)

40 CFSP (Common Foreign and Security Policy)

41 European External Action Service (EEAS) (February 2023) *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence* https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

42 Schneier, B. (24 April 2019) *Toward an Information Operations Kill Chain.* Lawfare Blog. https://www.lawfareblog.com/towardinformation-operations-kill-chain

Bergh, A. (2020) *Understanding Influence Operations in Social Media: A Cyber Kill Chain Approach.* Journal of Information Warfare, Vol. 19, No. 4, pp. 110-131. https://www.jstor.org/stable/27033648

Nimmo, B. and Hutchins, E. (10 November 2022) *Presentation on Overarching Online Operations Kill Chain.* Cyberwarcon Conference. https://www.csoonline.com/article/3680149/meta-s-newkill-chain-model-tackles-online-threats.html

43 US Cybersecurity and Infrastructure Security Agency (November 2021) *Cybersecurity Incident & Vulnerability Response Playbooks.* https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

44 Pamment, J. and Smith, V. (19 July 2022). *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online.* Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifyingthose-responsible-for-malicious-behaviour-online/244

45 Schwille, M. Atler, A. Welch, J. Paul, C. Richard, C.B. (2020) *Intelligence Support for Operations in the Information Environment*. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3161/RAND_RR3161.pdf

46 Pamment, J. and Smith, V. (19 July 2022). *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online.* Report by NATO Strategic Communications Centre of Excellence and the European Centre of Excellence for Countering Hybrid Threats. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifyingthose-responsible-for-malicious-behaviour-online/244

47 ENISA and EEAS (8 December 2022) *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape.* https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

48 For more on Information Environment Assesment: NATO Allied Command Transformation (3 April 2023) *Information Environment Assessment Capability Programme Plan Initiated.* https://www.act.nato.int/article/information-environment-assessment-capability-programme-plan-initiated/

49 ENISA and EEAS (8 December 2022) *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape.* https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

50 More on MITRE ATT&CK and DEF3ND frameworks: https://d3fend.mitre.org/about/

51 Golebiewski, M. and Boyd, D. (2019) *Data Voids – Where missing data can easily be exploited.* Data & Society. https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf

52 This list is not exhaustive and it is just for example purposes.

53 The Response Framework can be compatible with any Risk Assessment Matrix for information manipulation such as the ones proposed by:

- the Early Warning System of the expert forum of the Spanish Department of National Security - Spanish Department of National Security (2023). *Foro contra las campañas de desinformación en el ámbito de la seguridad nacional. Trabajos 2023.* Chapter 6. https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf

- the New Risk Perspective - Lindbom, H. (1 April 2022) *Capability Assessment for Stratcom using the new risk perspective to inform the development of effective response capability assessment for countering information influence operations.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240

- the RESIST2 Impact Analysis – UK Government Communication Service (2021) *RESIST2. Counter-disinformation Toolkit.* https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf

- the Breakout Scale – Nimmo, B. (September 2020) *The Breakout Scale: Measuring the impact of influence operations.* Working Paper of the Brookings Institution. https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/

54 Giles, K. (November 2023) *Humour in online information warfare: Case study on Russia's war on Ukraine.* Hybrid CoE Working Papers. https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231106-Hybrid-CoE-Working-Paper-26-Humor-to-combat-disinformation-WEB.pdf

55 Van der Staak, S.and Wolf, P. (2019) *Cybersecurity in Elections. Models of Interagency Collaboration.* International Institute for Democracy and Electoral Assistance. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

56 European External Action Service (EEAS) (October 2023) *FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human*

rights and diversity https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-LGBTQ-Report-03-Digital%201.pdf

57 Siman, B. (21 September 2023). *Countering FIMI: A Critical Imperative for Mission Safety.* EGMONT Royal Institute for International Relations." https://www.egmontinstitute.be/countering-fimi-a-critical-imperative-for-mission-safety/

58 European External Action Service (EEAS). February 2023. *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence.* https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

59 STIX Project. *STIX CourseofAction Type.* https://stixproject.github.io/data-model/1.2/coa/CourseOfActionType/

60 Authority for European Political Parties and European Political Foundations (November 2023) *Foreign Electoral Interference Affecting EU Democratic Processes.* https://www.appf.europa.eu/cmsdata/277388/Foreign%20electoral%20interference%20affecting%20EU%20democratic%20processes.pdf

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

62 National Intelligence Council (US) (10 March 2021). *Foreign Threats to the 2020 US Federal Elections.* https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

63 Kovalčíková, N. and Weiser, M. (30 August 2021) *Targeting Baerbock: Gendered Disinformation in Germany's 2021 Federal Election.* GMF Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/targeting-baerbock-gendered-disinformation-in-germanys-2021-federal-election/

64 European External Action Service (EEAS) (February 2023) *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence.* https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

65 Pamment, J. (September 2020) *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework*. Working Paper of the Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

66 DISARM Foundation. *DISARM Framework* created by SJ Terp and Dr. Pablo Breuer. https://www.disarm.foundation/framework

67 Structured Threat Information Expression (STIX™) *Introduction to STIX.* https://oasis-open.github.io/cti-documentation/stix/intro

68 DISARM Killchain phase "Preparation".

69 Kovalčíková, N. and Weiser, M. (30 August 2021) *Targeting Baerbock: Gendered Disinformation in Germany's 2021 Federal Election.* GMF Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/targeting-baerbock-gendered-disinformation-in-germanys-2021-federal-election/

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

71 O'Connor, S. Hanson, F. Currey, E. Beattie, T. (October 2020) *Cyber-enabled foreign interference in elections and referendums.* International Cyber Policy Centre of the Australian Strategic Policy Institute. https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

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

73 Government of the Netherlands (September 2023) *Global Declaration on Information Integrity Online.* Diplomatic Statement. https://www.government.nl/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online

74 Ibid.

75 ECD Confidencial Digital (July 2023) *Una web que suplanta a la Comunidad de Madrid se inventa que ETA amenaza con atentados este 23 de julio.* https://www.elconfidencialdigital.com/articulo/seguridad/web-que-suplanta-comunidad-madrid-inventa-que-eta-amenaza-atentados-23-julio/20230723143844613758.html

76 EUvsDisinfo. December 2023. *Elections in Poland through the prism of Lukashenka regime's propaganda.* https://euvsdisinfo.eu/elections-in-poland-through-the-prism-of-lukashenka-regimes-propaganda/

77 Gielewska, A. Dauksza, J. Szczygieł. (15 March 2022). *Behind the hack-and-leak scandal in Poland.* https://frontstory.pl/afera-mailowa-dworczyk-obajtek-rosja-zhakowany/?tztc=1 and https://vsquare.org/behind-the-hack-and-leak-scandal-in-poland/

78 Polska Agencja Prasowa (20 July 2022) *Russian services are behind the attack on politicians' accounts* (translation from Polish) https://www.pap.pl/aktualnosci/news%2C1377585%2Czaryn-za-atakiem-na-konta-politykow-stoja-rosyjskie-sluzby.html

79 Post on X from Polish media outlet Onet @OnetWiadomosci. https://archive.ph/OQsSt


European Union
EXTERNAL ACTION