



CEE Digital
Democracy Watch

CSD
CENTER FOR
THE STUDY OF
DEMOCRACY



Prague Security
Studies Institute

DISRUPT Toolkit White Paper

*A Whole-of-Society Approach to
Defending Democracy Against
Influence Operations*

Authors

Saman Nazari Alliance4Europe
Dr. Lumi Sarvela, Alliance4Europe

DISRUPT Toolkit White Paper

A Whole-of-Society Approach to Defending Democracy Against Influence Operations

Authors

Saman Nazari, Alliance4Europe

Dr. Lumi Sarvela, Alliance4Europe

Main Contributors:

Angela Gramada, Association of Experts for Security and Global Affairs ([ESGA](#))

Gloria Trifonova, Center for the Study of Democracy ([CSD](#))

Jakub Szymik, CEE Digital Democracy Watch ([CEEDDW](#))

Julian Neylan, Alliance4Europe ([A4E](#)).

Kristína Šefčíková, Prague Security Studies Institute ([PSSI](#))

Omri Preiss, Alliance4Europe ([A4E](#)).

Ondřej Perušič, Prague Security Studies Institute ([PSSI](#))

Pavel Havlicek, Association for International Affairs ([AMO](#))

Rositsa Dzhekova, Center for the Study of Democracy ([CSD](#))

Stepanka Lukesova, Association for International Affairs ([AMO](#))

Sorin Ionita, Expert Forum ([EFOR](#))

Contributing Organisations:

Pravda.PL

FakeNews.PL

NASK

New Data Academy

OpenMinds

Charles University

IICT

Central European Digital Media Observatory

CeMAS, Centre for the Study of Organized Hate

Demagog

Context

Friedrich Naumann Foundation

Casimir Paulaski Foundation

CBZC

LSEG Risk Intelligence,
FEMBLOC,
Indetrics,
Institute of Public Affairs,
VIGILIA,
ITSP Kybernetes
Bulgarian-Romanian Observatory of Digital Media (BROD) – coordinated by the GATE Institute.

Contributing Individuals:

Wojciech Dzięgiel, Casimir Pulaski Foundation
Wywrót, Centralne Biuro Zwalczenia Cyberprzestępczości
Vojtěch Kupka, CEDMO & Charles University
Dobromiř Wereszczyński, CEE Digital Democracy Watch
Gregor Bauer, CeMAS - Center für Monitoring, Analyse und Strategie
Ammaarah Nilafdeen, Center for the Study of Organized Hate
Natália Sabol Tkáčová, Friedrich Naumann Foundation for Freedom Central Europe
Mateusz Zadroga, Fundacja "Przeciwdziałamy Dezinformacji" - FakeNews.pl
Todor Kiriakov, Idetrics
Devora Kotseva, Idetrics
Yordan Terziev, IICT-BAS
Sonia Horonziak, Institute of Public Affairs
Mariusz Źabiński, Instytut Technologii Społeczno-Politycznych Kybernetes
Zhanna, Kondzirska, London Stock Exchange Group, Risk Intelligence
Michal Marek, NASK
Nicolae Tibrigan, New Data Academy
Yuliia Dukach, OpenMinds
Julia Mikzińska, Stowarzyszenie Pravda

Thank you to all the organisations and individuals who have contributed to the development of the framework and workflows with their insights and feedback and insights. The listed collaborators neither endorse, nor do they assume any liability for the content of the framework.

Table of Contents

Acknowledgement.....	5
Executive Summary.....	6
1. Introduction.....	9
1.1 The Challenge.....	10
1.2 Disruption Toolkit's Objective.....	13
1.3 Why a Framework?.....	13
2. Literature Review.....	15
3. Methodology and Definitions.....	16
4. Disruption Case Studies.....	18
4.1 French Elections Network - Public Pressure.....	18
4.2 Sanction Enforcement - Regulatory Response.....	19
4.3 Doppelganger on Bluesky - Platform Collaboration.....	19
5. DISRUPT - Influence Operation Disruption Framework.....	19
5.1 Object of Framework.....	20
5.2 Framework Phases Overview.....	21
5.3 Phase One: Prepare.....	22
5.4 Phase Two: Disruption.....	24
5.5 Phase Three: Mitigate.....	26
6. General Workflows.....	28
7. Country Localisation.....	29
7.1 The Czech Republic.....	29
7.2 Bulgaria.....	31
7.3 Poland.....	32
7.4 Romania.....	33
7.5 Comparative Analysis of the Countries.....	34
7.5.1 Shared Structural Strengths.....	34
7.5.3 Recurring Operational Gaps.....	34
7.5.4 Coordination Challenge.....	35
7.5.5 Systemic Nature of the Challenge.....	35
7.5.6 Strategic Added Value of a Standardised Framework.....	36
8. Integrating Gender Considerations into the DISRUPT Framework.....	37
9. Structured Cooperation Rather Than Ad Hoc Coordination.....	39
9.1 Establishing Structured Communication Channels.....	39
9.2 Defining Flagging, Escalation, and Delegation Triggers.....	39
9.3. Mapping Countermeasures to Competent Authorities.....	40
9.4. Integrating Civil Society into Advisory Coordination.....	40
10. Whole of Society Approach.....	40

10.1 Roles in a Distributed System.....	41
10.2 Actors.....	41
11. Threat Intelligence Database and Coordination Platform (TRANSCRIPT) - Technical Operationalisation.....	46
12. Recommendations.....	48
12.1 EU Level: Democracy Shield.....	48
12.2 National Level.....	50
12.3 Funding Coordination.....	51
13. Conclusion.....	52

Acknowledgement

The development of the DISRUPT toolkit and its components would not have been possible without the contributions of the over 180 individuals consulted. While Alliance4Europe held the pen, we have tried to channel the collective knowledge provided to us into this toolkit. Thank you for your contribution!

The Disrupt framework builds on and learns from existing works, such as the DISARM Blue and Red Frameworks, Check First's RADAR, Carl Miller's D-RAIL, and CeMAS Integrated FIMI Response Model.

A special thank you to our subgrantees AMO, PSSI, CSD, CEEDDW, Expert Forum, and ESGA for their excellent national knowledge and support in convening. We are also very grateful for the many government agencies that took the time to speak with us and share their insights. Furthermore, thank you to the networks EDMO and CAAD for helping us consult organisations outside our existing circles.

Thank you to NASK, Gate Institute, SWPS and ANCOM for hosting and helping convene workshops.

Finally, thank you to all the members of the CDN with whom we have worked over the past two years on more than 100 cases and numerous successful disruptions of influence operations. This experience has laid the foundation for many of the measures and workflows we have included in the toolkit.

Executive Summary

Influence operations targeting democratic societies have evolved in scale, coordination and strategic sophistication. They constitute a systemic risk to European democratic processes, public trust and societal cohesion, as well as long-term competitiveness and resilience. This threat is increasingly being recognised at both European and national levels, with detection capacity across the Union having significantly improved. **However, no overarching coordinated method had yet been developed to systematically disrupt influence operations.**

This white paper provides a first-of-a-kind operational toolkit to disrupt influence operations. The proposed DISRUPT Toolkit operationalises a whole-of-society approach, providing:

1. A Disruption Framework comprising all the actions a practitioner can take to prepare the evidence needed for disruption, the disruption steps available, and steps to mitigate the effect of an influence operation if disruption fails or takes a long time;
2. Guides and templates for the preparation, disruption, and mitigation measures;
3. Step-by-step workflows to analyse, disrupt and mitigate six different kinds of influence operations, based on the Disruption Framework. These include coordinated inauthentic behaviour, deepfakes and manipulated content, Impersonation, sanctions circumvention, doxing and gendered smear campaigns targeting political candidates.
4. An adaptation of these workflows to the national context of four EU countries;
5. A digital research infrastructure, the Threat Intelligence Database and Coordination Platform (TRANSCRIPT), to enable the operationalisation of the framework, the aggregation of cases and threat actors' assets, and the steps that have been taken to disrupt them.

While the framework was foremost developed to equip non-government actors, it is also a tool to support the work of governments.

The Framework represents the formalisation of the concrete collective experience of the largest counter-disinformation networks in Europe, involving open source intelligence researchers, fact-checkers, policy-makers, journalists, academics, stratcom professionals, cyber security experts, and national authorities across Europe.

The framework introduces a lifecycle-based model structured around three phases:

- **Prepare** - data collection, documentation, attribution and qualification of an influence operation;

- **Disrupt** - who to contact, when and how to disrupt ongoing activities.
- **Mitigate** - mitigating the harm from the operation and building long-term resilience.

This core model can be adapted to different national contexts, in Europe and beyond, by mapping relevant national actors, mandates, capacity, and legal frameworks. The Toolbox presented in this White Paper has already been localised, through a co-creative process, to the Romanian, Bulgarian, Polish and Czech contexts.

Practically, the framework enables the creation of national taskforces who have set workflows on how to detect, disrupt, and mitigate influence operations, in collaboration with government agencies. With shared standards, established frameworks, and common tools, these national taskforces can establish a pan-European decentralised web of responders who continuously disrupt threats towards European democracies, while being able to mobilise against regional or global crises. Additionally, the Framework lays the basis for a digital research infrastructure dedicated to data sharing, knowledge aggregation, a best practice repository, and response monitoring.

The Framework makes the most of what Europe has, because disruption is an immediate need. At the EU level, the framework complements and makes the most of existing legal and resilience instruments, without necessarily requiring further regulatory harmonisation. Improving interoperability across Member States. It makes use of existing capabilities by providing the operational sequencing layer required for coordinated incident management under the emerging **European Democracy Shield** architecture. Embedding the framework logic within cross-border coordination mechanisms would strengthen collective situational awareness and alignment of disruption in multi-state incidents. Crucially, the framework is intended to ethically **protect fundamental rights** within a democratic system, including the rights to freedom of expression and association.

The Disruption Toolkit represents a united European solution to a global challenge. It builds on years of theoretical research funded by the Horizon Europe Programme (e.g. the DISARM Framework), as well as on the experience of the Counter Disinformation Network (CDN), the EU-funded European Digital Media Observatory (EDMO) network, the Polish Resilience Council, the Digital Service Act implementation and the Code of Conduct on Disinformation Rapid Response System.

The Disruption Framework represents a scalable, concrete model to achieve the objectives of the European Democracy Shield and truly protect citizens from influence operations.

Key Takeaways for Decision-Makers

- **By disrupting influence operations, we protect free and democratic discourse**, acting on manipulative, inauthentic behaviour and threat actor infrastructure, rather than ever-changing content or narratives.
- **The gap is operational timing, not capability** - Member States already possess detection, regulatory and mitigation capacity. The recurring vulnerability lies in delayed escalation and uncoordinated workflows between detection and disruption.
- **Response and resilience require standardisation, not centralisation.** - The framework model (Prepare → Disrupt → Mitigate) sets a basic standard for evidence gathering, analysis and then points towards countermeasures. This improves coordination while fully respecting subsidiarity and national mandates.
- **Early disruption reduces systemic harm** - Structured disruption reduces the exposure of citizens to influence operations, reducing over-reliance on post-impact communication and reputational repair.
- **Whole-of-society capacity can be operationalised** - Civil society, media and independent monitoring actors frequently detect incidents first. Structured workflows and coordination mechanisms ensure early warning strengthens institutional response without transferring enforcement authority.
- **A common operational language enhances EU interoperability** - Embedding the framework within the European Democracy Shield architecture - including coordination through the Democracy Resilience Centre - would improve cross-border incident alignment and collective response coherence without requiring legal harmonisation.

1. Introduction

Democratic societies increasingly operate within an information environment shaped by persistent, coordinated and adaptive influence operations (IO). These operations range from coordinated inauthentic behaviour and impersonation to narrative manipulation linked to geopolitical, economic or societal objectives. Rather than targeting a single institution, such operations exploit the openness of democratic systems, the distribution of public authority across administrative bodies, and the time required for legal qualification of harmful conduct.

This whitepaper outlines the newly created IO Disruption Toolkit: a Disruption Framework, its proposed workflows, the technology to operationalise it (Disruption Platform), and the structures proposed to deploy it. It outlines a proposal for Europe's whole-of-society defence against authoritarian forces' influence operations.

The framework is designed for use by both public authorities and non-state actors, including civil society organisations engaged in monitoring and analysing influence operations. It therefore reflects an operational reality observed across Member States: relevant capabilities exist across governmental and non-governmental actors, but without a coherent operationalisation layer. The framework adopts a distributed democratic resilience model that relies on understanding and connecting the competencies of different non-government and government actors to detecting, analysing, and responding to influence operations.

The toolkit presents a blueprint for how to utilise the strengths of these actors to mount a whole-of-society defence of democracy against influence operations, within democratic safeguards.

The white paper starts by defining the challenge of countering IOs, explains the objective of the DISRUPT Toolkit and justifies the need for a DISRUPT Framework. After the literature review, methodology, and examples of disruption case studies, the white paper describes in detail the IO Disruption Framework with all its phases and components. Then, the text presents the general workflows and how those have been localised to four different national realities. It also includes a mapping and assessment of each country's counter-IO capabilities. The white paper then delves into what it takes to operationalise a whole-of-society approach, defining actors' roles and ways of working together coherently. Finally, the white paper presents the Disruption Platform before putting forward a set of recommendations.

1.1 The Challenge

Through a series of expert interviews, workshops, extensive literature review, and operational work with civil society and government agencies across Europe, a series of challenges were identified when it comes to the EU's Counter-IO operations.

Three dynamics in particular complicate detection, qualification and response.

First, distinguishing coordinated inauthentic behaviour (CIB) from legitimate collective action is often difficult in practice. Coordination alone is not evidence of manipulation. Users frequently organise around legitimate causes, campaigns, or shared interests, generating synchronised posting patterns, mass commenting, or coordinated amplification that can resemble influence operations at a behavioural level. At the same time, contemporary influence operations increasingly rely on real users, micro-incentives, or loosely organised networks rather than clearly identifiable bot infrastructures. This convergence blurs the boundary between authentic mobilisation and manipulative coordination, complicating both analysis and policy responses.

Second, a persistent policy dilemma concerns the distinction between illegal conduct and behaviour that is harmful but lawful. Many practices that distort the information environment - such as large-scale amplification of misleading narratives, manipulative framing, emotionally polarising content, or coordinated agenda-setting - do not necessarily violate specific national laws. Consequently, the legal threshold for state intervention is often not met even when societal impact is significant. In operational terms, many influence operations focus less on persuading users directly and more on triggering platform algorithms that reward engagement.

Third, the recommendation architectures of very large online platforms (VLOPs) create systemic amplification risks. Coordinated engagement signals - such as commenting, sharing or viewing - can be used to influence ranking systems that prioritise popularity and interaction. Consequently, relatively small networks can rapidly amplify polarising or misleading content to large audiences. This dynamic shifts the operational focus from individual pieces of content to the interaction between coordinated behaviour and platform design.

Together, these dynamics create a complex operational environment in which influence operations can escalate rapidly while institutional responses remain constrained by evidentiary thresholds, legal mandates and coordination procedures.

An **Influence Operation** is an organised, deliberate effort to manipulate the beliefs, behaviours, or decisions of a target audience using illegal content, illegal activity, inauthentic behaviour, covert activity, or foreign interference. This definition aims to safeguard fundamental rights and freedoms.

Influence operations have become increasingly complex, relying more on inauthentic amplification, information laundering, proxies, deepfake impersonations, and a wide range of other technology-oriented manipulative techniques. While civil society is rapidly adapting, funding remains scarce, and the research and response required often extend beyond existing mandates and work cultures.

Relevant capabilities to counter IOs exist in Europe, but are distributed across government institutions, OSINT practitioners, journalists, independent researchers, fact-checking organisations, strategic communicators, lawyers, cybersecurity professionals and other public-interest actors.

Public authorities retain responsibility for enforcing laws, procuring proprietary data, protecting national security, taking diplomatic actions, and international coordination while respecting the fundamental rights of citizens. However, non-governmental actors frequently identify emerging influence operations earlier due to specialised monitoring capacities and community proximity. In practice, they function as an early-warning layer and have more freedom to take civil-society-specific actions rapidly, such as public pressure campaigns, as they often don't have to seek approval from a complex hierarchy. Across EU Member States, significant institutional capabilities already exist to address different aspects of influence operations. Authorities responsible for security, electoral integrity, media regulation, cyber security, strategic communication and law enforcement all contribute to protecting democratic processes. However, these competences have generally evolved sectorally. As a result, responses to influence operations frequently are late or do not work to disrupt the enabling infrastructure, as each institution acts within its own mandate and timeline.

This structural challenge creates a recurring vulnerability. Influence operations tend to unfold rapidly and across domains, while non-government actors usually only flag the issue, and governmental response is often delayed. Earlier intervention - where it would have the greatest effect - is frequently constrained by uncertainty regarding competence, evidentiary thresholds, or coordination responsibilities.

The consequence is a pattern: signals are detected, relevance is assessed in parallel by multiple actors, escalation is cautious, and once public impact is already visible, the response commonly ends up being simple communication and damage control. This dynamic does not reflect

institutional failure. Rather, it reflects the absence of a shared operational model, mandates, and coordination that enable authorities to act proportionately and coherently within existing legal frameworks.

At the European Union level, policy initiatives increasingly recognise the need to strengthen democratic resilience against systemic risks affecting public discourse and democratic processes. Instruments addressing platform accountability (such as the Digital Services Act), transparency, electoral integrity and hybrid threats strengthen structural safeguards. However, coordinated incident response to ongoing influence operations requires shared operational logic connecting these instruments in practice and a faster reaction time

At the national level, Member States address similar incidents through different operational and political realities, using different coordination logics, action thresholds, and workflows. Limited capacity, existing legal frameworks, and a lack of clear mandates to coordinate or act limit government actions, while funding constraints limit civil society. This diversity is consistent with national competence and subsidiarity. However, it also creates an asymmetry: influence operations can exploit differences in response timing and institutional interpretation across jurisdictions.

One clear example is the diversity in how digital sanction enforcement is carried out across Member States. Most Member States surveyed have laws in place on sanction enforcement, but no comprehensive and integrated enforcement or monitoring mechanisms.

A shared operational approach does not require harmonisation of legal mandates. Instead, it requires a common understanding of *when* institutions act relative to one another, and how information and responsibility move across incident phases.

The work presented in this white paper responds to this need. It develops an operational framework for public authorities to detect, assess, disrupt and mitigate influence operations in a coordinated manner while preserving national competences and democratic safeguards. The Framework is based on a lifecycle model consisting of three functional phases:

- **PREPARE** - data collection, documentation, attribution and qualification of an influence operation;
- **DISRUPT** - who to contact, when and how to disrupt ongoing activities.
- **MITIGATE** - mitigating the harm from the operation and building long-term resilience.

1.2 Disruption Toolkit's Objective

The overarching objective of the Disruption Toolkit is to empower practitioners to act in a coordinated manner against the threats they see.

The sub-objectives of the Toolkit are:

1. Enable rapid response against threats when they appear;
2. Giving practitioners more agency to face the threats they identify by equipping them with a toolbox of actions they can take to disrupt or mitigate them;
3. Help governments and civil society coordinate with each other better, understanding the mandates and strengths of each other;
4. Provide the EU Member States with a tool to understand the legal, regulatory enforcement, capacity, and mandate gaps needed to effectively and rapidly respond to an influence operation;
5. Provide the community with a common taxonomy of actions that the community can collaboratively build on and integrate into the coordination infrastructure.

The central objective is not to create new powers, but to enable proportionate action earlier in the operational cycle by clarifying mandates and capabilities.

1.3 Why a Framework?

While European and national policy instruments address transparency, accountability and systemic risk reduction, operational cooperation between competent authorities remains a necessary complement. A shared Disruption Framework can provide interoperability across national systems while respecting subsidiarity and institutional diversity. The Framework can contribute to the efforts to unify and streamline European defence of democracy under the European Democracy Shield.

The Framework is not a replacement for national approaches, but a coordination standard and toolbox. It enables Member States to retain their institutional structures while improving predictability of response, facilitating cross-border and national understanding of mandates and capacities, and supporting proportionate intervention consistent with fundamental rights.

Furthermore, different actors may observe the same behaviour. Yet, each interprets it separately and considers different disruption or mitigation options. Some prepare analysis, others consider regulatory thresholds, while others evaluate whether platform reporting or public exposure is appropriate. Because these decisions are not guided by a shared progression

from signal to response, action often occurs late and primarily in the form of public communication after visibility has already been achieved. The issue is a lack of a structured method to determine which disruption measures are appropriate at which stage.

The Framework addresses this gap. **It provides a stepwise operational logic (workflows) that supports defenders in moving from detection to analysis, analysis to assessment, and from assessment to proportionate intervention.**

This aims to help organisations understand the steps to take to secure evidence ahead of a disruption, and how to evaluate that evidence to ensure the case actually is an influence operation, and move through the disruption process. It also aims to help actors tie specific cases to both regulatory disruption instruments and softer instruments, such as platform policy and public pressure.

The phases clarify the evidence required and suitable response options, ranging from documentation and coordination to platform reporting, regulatory actions or public exposure.

The objective is to **enable earlier, informed selection of countermeasures during the lifecycle of an influence operation**, rather than reacting only after impact has occurred.

The Framework establishes a repeatable, interoperable operational standard applicable across Member States. By aligning timing, escalation logic and countermeasure selection, the framework enhances preparedness, strengthens cross-border interoperability and improves coordinated response capacity - without harmonising law or centralising authority.

In doing so, it establishes a common operational sequencing standard capable of reducing structural delays in democratic response.

This aligns with the EU's approach to democracy defence, which recognises that preparedness, response and societal resilience must operate in coordination rather than isolation.

The framework, therefore, constitutes a scalable European operational standard capable of reinforcing democratic resilience across the EU while fully respecting institutional diversity.

The following sections describe the analytical basis for the framework, its development methodology, the operational workflows it enables, and the comparative insights derived from national consultations. The report concludes with recommendations for national implementation and for integration within European democratic resilience architecture.

2. Literature Review

A growing body of frameworks and methodologies has emerged to help researchers, governments, and civil society actors analyse and respond to disinformation and influence operations. While these initiatives differ in scope and design, they collectively provide important building blocks for understanding and countering information manipulation. This Framework builds on these existing approaches and seeks to operationalise their complementary strengths.

Several frameworks have contributed significantly to the behavioural analysis of influence operations. The [DISARM Framework](#) provides a widely adopted taxonomy of tactics, techniques, and procedures (TTPs) used in influence operations, enabling practitioners to describe operations through a shared vocabulary. This behavioural approach marked an important shift in the field from analysing the accuracy of individual claims to examining the operational methods used by threat actors. However, while DISARM offers an extensive catalogue of techniques and potential countermeasures, it does not provide a structured operational workflow for coordinating disruption responses.

Other initiatives have focused on conceptual and strategic models for disruption. The [D-RAIL Framework](#) aggregates several existing approaches into a flexible “chain of influence” model designed to identify points adversarial operations can be disrupted. Similarly, the [Pyramid of Pain](#), adapted from cybersecurity to the information manipulation domain, provides a heuristic for prioritising disruption efforts based on the cost imposed on adversaries. These models offer valuable strategic guidance for identifying high-impact intervention points, but they remain largely conceptual and require additional operationalisation for real-time response activities.

A number of frameworks address specific components of the counter-disinformation response ecosystem. The [RESIST 2 toolkit](#), developed for strategic communicators, provides structured guidance for monitoring information environments and designing communication responses. The [CeMAS Integrated FIMI Response Model](#) offers a whole-of-society perspective by mapping countermeasures across different actors and societal resilience mechanisms. Meanwhile, the [RADAR framework](#) translates the Digital Services Act into a structured system for documenting regulatory risks and potential platform non-compliance. Each of these initiatives contributes important capabilities - communication strategy, societal coordination, or regulatory escalation - but none provides an end-to-end operational methodology for disrupting influence operations.

Finally, emerging frameworks such as the [EU DisinfoLab Response-Impact Framework](#) introduce mechanisms for evaluating the effectiveness of counter-disinformation interventions over time. By linking responses to measurable outcomes, this approach provides a critical foundation for evidence-based learning and long-term strategic evaluation. However, its application requires monitoring capacities that remain limited across the counter-IO ecosystem.

Taken together, these frameworks demonstrate significant progress in the field, but also highlight persistent fragmentation. **Existing approaches often focus on individual components - such as behavioural analysis, communication response, regulatory enforcement, or impact evaluation - rather than providing a fully integrated operational model.** As a result, practitioners frequently rely on a combination of tools and ad-hoc coordination to respond to influence operations.

The Disruption Framework presented in this report builds directly on these contributions. It integrates the behavioural insights of frameworks such as DISARM, the prioritisation logic of the Pyramid of Pain, the coordination principles of CeMAS, the regulatory leverage of RADAR, and the communication and evaluation approaches of RESIST and the EU DisinfoLab framework. By combining these elements into a structured **Prepare - Disrupt - Mitigate** workflow, the Framework aims to provide practitioners with a practical methodology for coordinating disruption activities across actors, tools, and jurisdictions while maintaining compatibility with existing standards and practices.

3. Methodology and Definitions

The project followed a three-stage co-creation methodology designed to ensure that the framework would be both operationally practical and institutionally applicable.

The first step entailed a literature review and initial conversations with experts to avoid duplicating any existing work and utilising as much as possible.

The second step was to develop a general framework and workflows that could be localised to the context of different EU countries. The last step was the localisation of the workflows to 4 project countries: Poland, Bulgaria, Romania, and the Czech Republic

The process began with creating a structure for the framework and laying out the preparation, disruption, and mitigation measures used during the two years of operating the Counter Disinformation Network. Thereafter, operational practitioners actively engaged in countering influence operations were convened to give their input and feedback.

Rather than collecting descriptive information, this phase functioned as a design exercise. Practitioners evaluated whether the proposed structures matched real operational dynamics and identified where actions typically fail or occur too late.

The experience of the participants validated the structure of the disruption framework while also adding new components and safeguards. Two general consultations were organised, where groups of people could provide feedback to the general framework.

Thereafter, parts of the framework were subsequently tested, and the full framework was localised with national authorities and civil society actors in four EU countries. The localisation happened through two national workshops: one with non-government actors, another with government actors. The purpose of this phase was not to redesign the framework but to determine how it could function within national institutional structures.

Workshops mapped responsibilities across authorities and CSOs, examining how the general methodology aligned with existing mandates.

This stage translated the general methodology into national workflows by clarifying who would act at each phase and how signals could move between actors.

Participants identified: monitoring and detection actors, analytical and investigative bodies, regulatory or enforcement authorities, public communication roles, and coordination mechanisms.

Through this phase, we identified gaps in existing systems and proposed remedies within existing mandates. The exercise demonstrated that the framework could operate within existing mandates through procedural alignment rather than institutional reform.

Findings were compared across the four countries, showing strong capacity to mitigate the potential harm of operations but weaker disruption coordination. The primary difference concerned the timing of shared responsibility recognition. The consistency of this pattern indicated a systemic coordination challenge suitable for a common operational methodology.

The final framework integrates practitioner-validated operational logic with institutionally adapted workflows. It therefore functions as a deployable coordination standard grounded in both operational practice and administrative feasibility.

Alongside the framework and workflow development, the threat intelligence database and DISRUPT platform, Threat Intelligence Database and Coordination Platform (TRANSCRIPT), were developed. To ensure that the platform would respect the interests of as wide a community as possible, an advisory board with leading experts from EU government agencies, fact-checkers,

investigative journalists, OSINT researchers, academics, and technology providers was created. Three meetings were convened, where they were consulted.

In total, over 170 practitioners were consulted, including members of the EDMO, CAAD, and CDN networks.

This sequencing ensured that the framework was first validated against real operational practice and only then adapted to administrative and legal environments.

The localisation exercises did not aim to evaluate national performance. Instead, they sought to identify recurring coordination patterns and structural bottlenecks common across administrations operating under different legal and organisational conditions.

4. Disruption Case Studies

Disruption may not yet be a widely recognised concept. The examples in this section illustrate how disruption has worked in practice. One highlights the power of media scrutiny, another demonstrates the value of government collaboration, and the final example shows how platforms themselves can act against such operations.

4.1 French Elections Network - Public Pressure

During the 2024 European Parliament elections and snap legislative elections in France, members of the CDN identified [a network of Facebook pages posing as different segments of French society](#). These pages impersonated groups such as the French African diaspora, Muslims, liberals, and the far-right. They published unlabelled political advertisements and shared images containing obfuscated text designed to discredit Macron and Ukraine while attempting to evade Meta's automated content moderation systems.

The pages were all operated from the Sahel region and paid for advertisements using a wide range of currencies. Reporting the case to Meta did not lead to the pages being removed, nor did it prompt action from French or EU authorities, as far as researchers could tell. However, after a Politico journalist contacted Meta for comment ahead of [publishing a story about the operation](#), the entire network was taken down within hours.

4.2 Sanction Enforcement - Regulatory Response

Following the European Parliament election in 2024, [Science Feedback](#) and Alliance4Europe published a series of [reports](#) showing that sanctioned Russian entities remained accessible to European audiences on major social media platforms. The initial reports aimed to alert platforms to the issue and assess whether they would take action once it had been brought to their attention.

Several months later, a follow-up [report](#) was published demonstrating that most platforms had taken very limited action. TikTok was the notable exception, responding rapidly after a [New York Times article](#) covered the findings and highlighted more than 700 violations. The second report argued that the platforms' inaction could constitute a systemic risk.

In the following months, regulators and government agencies across Europe engaged with the platforms, leading to the removal or geofencing of a large majority of the identified pages. Pavel Durov, the founder of Telegram, also made a public statement ten days after the report's publication, confirming in communication with the competent regulator, the Belgian Digital Service Coordinator, that the Digital Services Act required Telegram to geofence Russian media from European audiences.

4.3 Doppelganger on Bluesky - Platform Collaboration

Following [CeMAS's](#) discovery of an automated way to track the sanctioned Russian coordinated inauthentic behaviour network Doppelganger, the CDN had monitored the operation and worked to disrupt it across platforms. [During the German elections, Doppelganger expanded its activities to Bluesky](#). The operation utilised a nearly identical pattern of behaviour and content on the platform, allowing researchers to identify it.

By mapping these behavioural patterns, collecting examples, and sharing these examples with Bluesky, the platform was able to block the operation from functioning there. In contrast, although X was provided with the same information about the operation on its platform, the operation continues there as it has done.

5. DISRUPT - Influence Operation Disruption Framework

The Disruption Framework is an open-source community tool that aims to be a living resource that supports the wider community of defenders.

This Framework forms a foundation of common definitions, actions and measures classified in different operational phases. The Framework is the backbone of the toolkit. It was shaped and validated by the community. It is not intended to be static; rather, it is designed to evolve through community feedback, iteration, and collective improvement.

The Framework has a series of components, from less to more granular:

1. **Phases** - three phases determining what series of actions one is preparing to undertake: prepare, disrupt and mitigate.
2. **Sub-phases** - a way to break down phases into smaller collections of measures. Sub-phases include Data Collection and Documentation, Analysis and Assessment, Inform, Report Through Established Mechanisms, Government Engagement, Pressure and Communication Actions.
3. **Stage** - collections of measures that are focused on achieving a specific goal, such as documenting evidence or disrupting social media assets.
4. **Measures** - specific operational actions that can be taken to prepare, disrupt, or mitigate an influence operation. Examples include relying on the DSA Trusted Flagger Mechanism, engaging political parties or copyright takedowns. Measures represent the smallest building block of the framework.

The Framework also includes:

5. **Templates** - guides and copy-pastable text that can be used to practically conduct the measures.
6. **Workflows** - step-by-step instructions on how to disrupt a specific type of operation, such as sanctions circumvention or deepfakes.
7. **Localised Workflows** - a workflow adapted to national legislation, government mandates, civil society capabilities, and existing structures in a specific country.

5.1 Object of Framework

The primary object of the framework is threat actors - entities that conduct influence operations. These may include hostile states, terrorist and extremist groups, authoritarian political parties, and companies (e.g. mercenaries), though the framework's definition is not limited to these examples.

Threat actors typically consist of groups operating under a unifying structure, such as a government (e.g. Russia) or a terrorist organisation (e.g. Daesh). Individuals are generally not

considered threat actors, with a few exceptions - e.g. oligarchs who maintain extensive ecosystems around them. In practice, disrupting a threat actor most often involves targeting the activities and capabilities they control.

In addition to threat actors conducting influence operations, the framework identifies two other objects: service providers and social media platforms.

The framework provides guidance to help practitioners use the reporting and enforcement mechanisms of social media platforms and service providers (e.g. hosting, domain, payment, etc.) to report and disrupt operations. While this approach can lead to action, additional tools - such as legislation, regulatory engagement, legal measures, government pressure, or public scrutiny- may often be required. For this reason, these service providers and platforms are frequently the direct targets of specific measures within the framework.

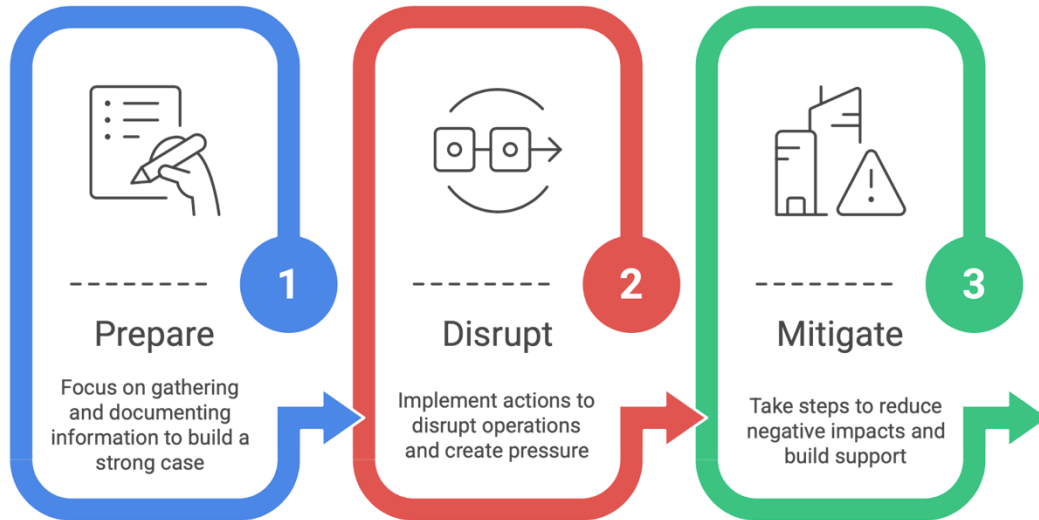
5.2 Framework Phases Overview

The Framework guides practitioners and authorities through a progression from data collection, analysis to intervention by linking each stage of analysis to a set of appropriate countermeasures.

The three phases divide the measures based on their overarching objective:

- Preparation → collecting, securing, analysing, and validating evidence.
- Disruption → dismantling the operational capabilities of an operation
- Mitigation → addressing the harm caused by the operation and building resilience against it.

Framework Phases

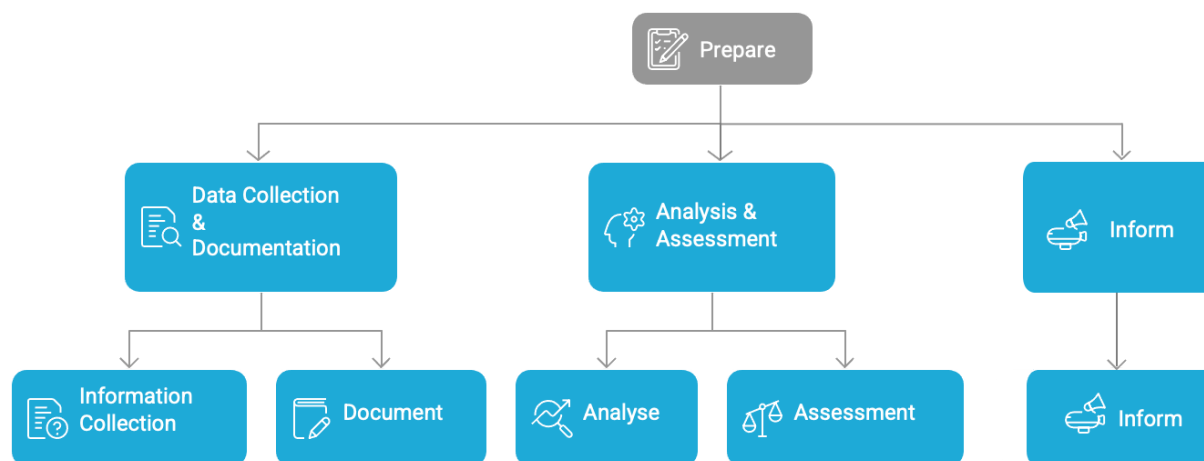


5.3 Phase One: Prepare

Collecting, securing, analysing, assessing, and documenting an influence operation.

It is not always straightforward to determine with certainty whether observed activity constitutes an influence operation. When identifying a potential case, it is necessary to verify that the suspected activity is indeed an influence operation and *that sufficient evidence exists to support this conclusion*. At this stage, uncertainty is expected, and intervention is premature.

The purpose of the first phase is to transform isolated observations into a structured body of evidence that can be collectively evaluated. Monitoring actors - including specialised civil society organisations, researchers and public authorities - document patterns in a consistent manner so that coordinated activity can be distinguished from ordinary online behaviour.



The objective of this phase is to establish whether the identified activity constitutes an influence operation and to enable defenders to develop a shared understanding of the case. If the findings withstand assessment, the output of this phase will be some type of informational resource, such as a report, alert, email or slide deck that presents the evidence.

This phase consists of three main sub-phases: Data Collection and Documentation, Analysis and Assessment, and Inform.

Data Collection and Documentation

The Data Collection and Documentation sub-phase focuses on gathering and securing both openly available and proprietary information. It provides recommendations on tools that can be used and will, in the future, also aggregate guides and open-source projects.

This category of measures ensures that observed activity is recorded in a verifiable and shareable manner, enabling multiple actors to assess the same information and operate on a common evidentiary basis.

Analysis and Assessment

The Analysis and Assessment sub-phase determines whether disruption can be justified.

The Analyse stage aims to provide practitioners with a range of measures to examine a case, including:

- identifying coordinated inauthentic behaviour,
- analysing content for inauthenticity, origin, or illegality,
- identify links between the operation and a threat actor,
- Mapping the infrastructure used in the operation,

- Analyse behavioural patterns and the factuality of claims.

The **Assessment stage** provides users with six categories of yes/no questions designed to determine whether a case qualifies as an influence operation. These categories are:

- Inauthentic Behaviour
- Legality
- Attribution
- Imminent Risk
- Foreign Interference

If at least one of the questions can be answered “yes” with at least 80% certainty, according to the Professional Head of Intelligence Assessment (PHIA) [Probability Yardstick](#), practitioners can proceed to the disruption kill chain.

Inform

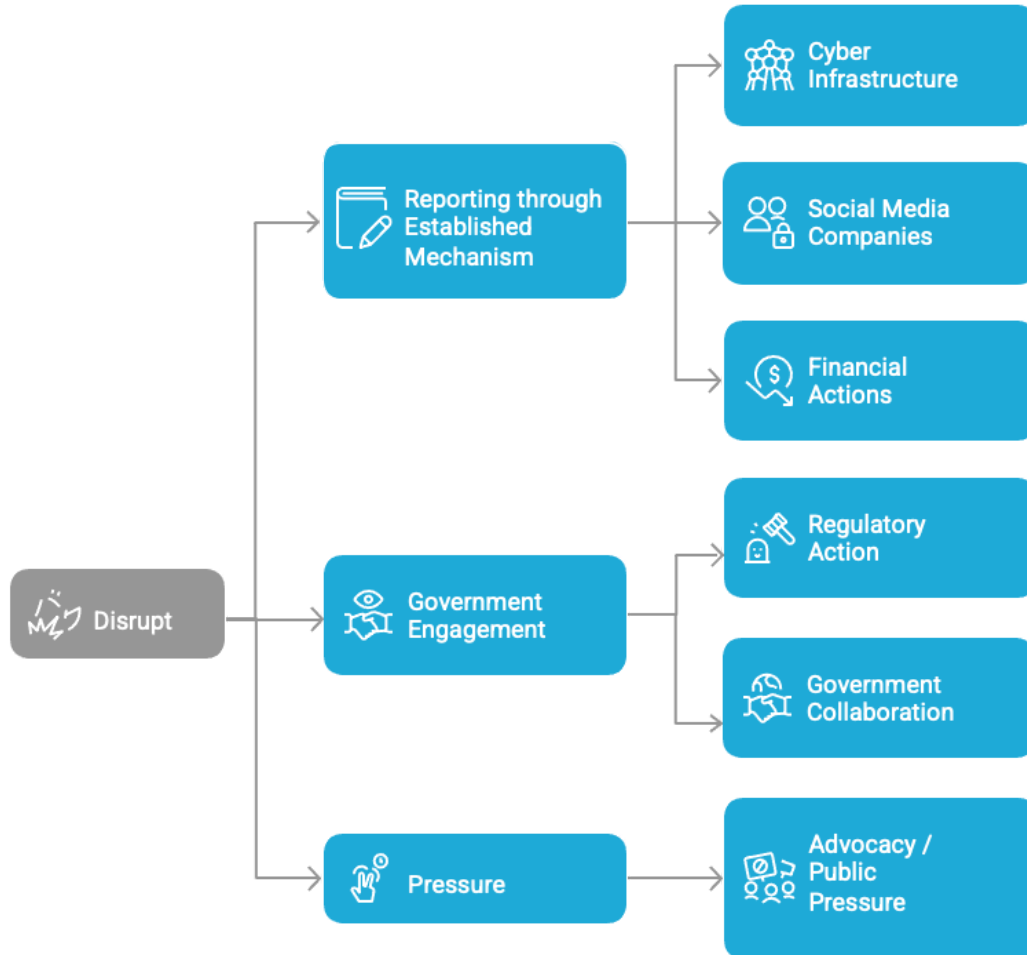
The final sub-phase consists of a single stage: Inform. This stage involves producing an informational resource - such as an alert, report, email or other communication format - that presents the findings of the analysis. This output can be shared with relevant stakeholders to motivate engagement in the disruption efforts or to justify specific disruption requests.

5.4 Phase Two: Disruption

Once the influence operation has been qualified, the objective shifts from collection, analysis, and assessment to **Disruption**. The framework does not prescribe a single response. Instead, it guides users in selecting proportionate measures based on the specificities of the case. Because influence operations rely simultaneously on perceived credibility, technical infrastructure and audience engagement, responses may combine different categories of measures and escalate progressively.

Disruption includes a range of actions, including using platforms, service providers, and financial sector procedures, utilising legislation, engaging competent authorities and utilising public pressure.

The defining feature is timing: action occurs while the operation is unfolding. The framework outlines what actions are rapid to take, and which ones require more time, enabling actors to utilise rapid response measures when needed.



The sub-phase called **Report Through Established Mechanisms** relies on the social media platforms, service providers (e.g. hosting companies), and financial institutions' existing reporting mechanisms. Utilising these can lead to rapid resolution of a disruption, and can be the path of least resistance. Therefore, the framework provides guides and templates on how to utilise a wide range of these mechanisms.

The sub-phase **Government Engagement** relies on utilising legislation and government collaboration. This sub-phase is most effective when localised to a specific national context.

The first stage in this sub-phase, **Regulatory Action**, outlines all the criminal, regulatory, and civil laws that can be used to disrupt an influence operation. These include laws such as sanctions legislation and the DSA, but also copyright and Anti-Money Laundering and Financing of Terrorism (AML/CTF) laws. In cases when the measures describe EU legislation, the measures describe the specific law. Otherwise, they describe types of laws, as these laws differ widely between different countries. The localised versions of the framework quote the specific national legislation.

Stage 2, **Government Collaboration**, outlines the different types of government agencies that usually have mandates related to countering influence operations and provides advice on how to collaborate with them. By understanding their mandates, users will know who to go to for what type of cases.

The last sub-phase under the disruption phase is **Pressure**. The pressure sub-phase has one stage, called **Advocacy and Public Pressure**. This stage focuses on building public pressure through public statements, articles, and citizen-facing actions to push social media platforms and service providers to act against the influence operation. This entails mobilising political actors to make statements, call representatives of the companies to testify in committees, or ask government agencies formal questions. It also entails mobilising advocacy actors to organise joint actions, driving attention to the case. It can also involve engaging the public, inviting them to sign online petitions or join offline actions, such as demonstrations. Journalists have a strong role, where they can ask the companies for comments and interviews. Finally, private sector organisations, such as companies or interest groups, can be engaged to make public statements or use their advocacy capabilities to build political support for your disruption measures.

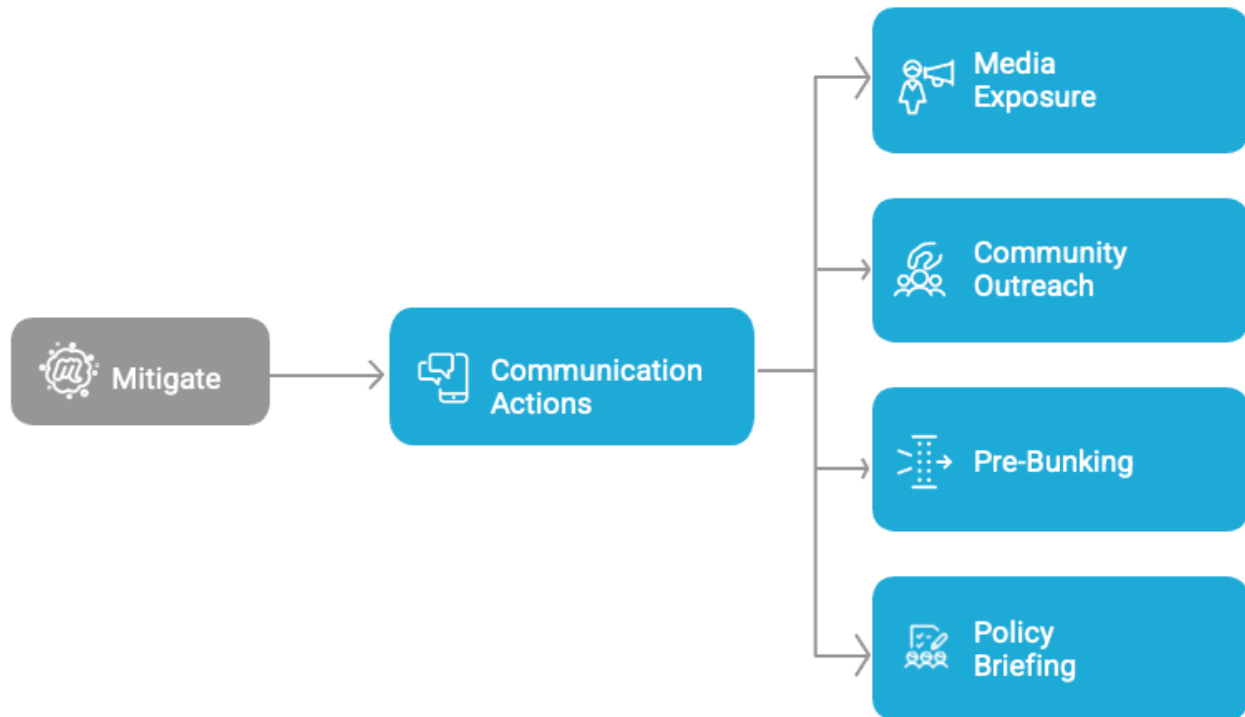
5.5 Phase Three: Mitigate

Immediate harm reduction and reduction reducing long-term harm.

This phase was not part of the initial project and has therefore not been expanded extensively. Its inclusion is intended to enable future expansion of the framework. In future iterations, this phase may incorporate components related to policy development, education, and other resilience-building activities.

Disruption can take a substantial amount of time to achieve, which results in the influence operation being able to reach its target audience. When an influence operation reaches the public, disruption measures alone are no longer sufficient. Even after technical, procedural or regulatory interventions are applied, narratives may continue to circulate, affected communities may experience harm, and public trust may be weakened.

The objective of this phase is therefore to rapidly mitigate the harm the operation causes, reduce societal impact and reinforce resilience against similar future activity. Mitigation measures aim to restore shared understanding, supporting affected groups and increasing public awareness of manipulation techniques. Rather than targeting the operation itself, mitigation addresses its consequences.



Once the activity becomes widely visible, clear and credible communication becomes essential. Competent authorities and public-interest actors provide context, clarify facts and explain the nature of the manipulation. Across all participating countries, this capability proved comparatively strong.

The framework does not replace existing communication or resilience efforts. Instead, it complements them by ensuring mitigation is not the primary or only response. Earlier disruption reduces harm; mitigation mends or mitigates the damage already done.

The phase has one sub-phase and stage, both called **Communication Actions**. They utilise:

1. **Media Exposure** to inoculate and inform the public about the operation.
2. **Community Outreach** to utilise trusted individuals in the community to inform and educate the population against the operation.
3. **Pre-Bunking** entails working with strategic communicators to preempt operations and try to counter their effects without directly engaging with them.
4. **Policy Briefing** aims to inform policymakers about the operation and propose policy responses that could ensure that the operation is less successful or unable to operate in the future.

6. General Workflows

As part of the general disruption methodology, standardised workflows were developed for the most recurrent categories of influence operations identified through practitioner consultations and accumulated operational experience within the Counter Disinformation Network.

These workflows make a selection of measures from the DISRUPT Framework, outlining how and when in the process to use them to disrupt an operation.

These disruption workflows include countering the following typologies:

1. Coordinated inauthentic behaviour;
2. Deepfakes and manipulated content;
3. Sanctions circumvention;
4. Impersonation;
5. Doxing;
6. Gendered smear campaign targeting political candidates.

The selection of these categories reflects common influence operation types rather than isolated content types. They represent structural forms of influence operations that appear consistently across jurisdictions and political contexts.

The workflows are designed as modular, interoperable operational standards capable of adoption across diverse national systems. They provide a common operational language that can be applied across Member States, enabling predictable coordination while preserving national legal mandates. **This scalability is central to the Framework's potential role within broader democratic resilience architectures.**

While each workflow follows the same phased structure, the mix of countermeasures differs depending on the nature of the influence operation.

While sanctions circumvention operations clearly violate the law and can therefore be countered more readily through legal tools, coordinated inauthentic behaviour operations are often not illegal. As a result, responding to them frequently requires greater reliance on platform engagement or on identifying other legal violations. These may include, for example, trademark infringements where CIB operations impersonate a real entity.

These differences demonstrate the Framework's flexibility and scalability. The Framework can be adopted as a common sequencing standard while preserving full national discretion regarding legal authority and institutional competence.

7. Country Localisation

The Disruption Framework is designed as a general methodology that can be localised to different national contexts. It was tested and adapted through national consultations and ecosystem mapping exercises conducted in Czechia, Bulgaria, Poland and Romania.

The objective of this localisation process was not to redesign national institutional arrangements. Rather, it aimed to determine how actors can utilise existing legislation, structures, expertise, and government agencies within each country for disruption.

Across all four countries, the same core Framework logic applied (**Prepare** → **Disrupt** → **Mitigate**). Differences emerged primarily in which actors, laws, tools, and mechanisms became relevant at different stages of evidence maturity, and in which phases of the Framework were currently strongest in practice.

In all countries, relevant capabilities were present but were distributed across multiple institutions and external actors. **Early detection frequently originated from non-governmental actors, while regulatory and enforcement powers remained primarily with public authorities.**

Workshop participants described similar patterns in how incidents progressed across actors. Signals of potential influence operations were often available at an early stage, but responsibility for disruption was sometimes unclear. Communication responses tended to be relatively well developed, but were frequently implemented later in the response process.

More detailed analyses of coordination challenges are available for each country. National authorities have received dedicated reports containing additional findings. Some localised frameworks are not publicly available in accordance with the preferences of the respective national authorities. Interested readers may contact the authors for further information

7.1 The Czech Republic

Czechia's localisation combined institutional and civil society consultations with the most comprehensive stakeholder mapping in the four-country initiative. A total of **249 strategic**

individuals and organisations were identified across government, civil society, academia, media and technical sectors, forming the most granular national ecosystem in the project.

This mapping shows that Czechia has a broad and active diverse landscape of actors engaged in countering FIMI. However, this landscape remains fragmented and is largely based on informal cooperation between institutions and independent actors, with some overlap in activities across organisations. The primary challenge is therefore not the absence of capability, but **coordination, sequencing, and continuity** - particularly during periods of institutional transition. Some capabilities have already been reduced following the recent government transition.

The national consultation confirmed that all lifecycle phases are covered by at least one actor. Detection and analytical capabilities are particularly strong within:

- BIS (Security Information Service);
- NUKIB (National Cyber and Information Security Agency)
- KRIT & CHH (Crisis Information Team and Centre Against Hybrid Threats, Ministry of the Interior)
- Cyber and hybrid structures within the Ministry of Defence

Mitigation capacity is well developed, especially through KRIT's coordination of government communication. However, no single institutional workflow consistently links detection, disruption and mitigation into a coherent end-to-end operational sequence. Currently, there is also a marked lack of political will by the government to operate one, so other actors would need to do so.

The mapping also highlights a high concentration of independent expertise:

- 76 CSOs and think tanks
- 64 academic institutions
- 42 media and journalism entities
- 56 government and state administration actors
- 11 political and diplomatic entities

This diversified ecosystem provides an important resilience buffer. In the context of political turnover and restructuring of strategic communication capacity, anchoring localisation within this broader non-government ecosystem can help preserve monitoring capacity and ensure continuity beyond changes in executive structures.

7.2 Bulgaria

Bulgaria's localisation combined institutional and civil society consultations with comprehensive stakeholder mapping across government, regulatory, civil society, academic, media and technology sectors. A total of **133 strategic entities** were identified, confirming that Bulgaria's counter-FIMI ecosystem is not institutionally absent - it is structurally distributed.

Consultations confirmed relevant competences across:

- Ministry of Foreign Affairs (attribution and diplomatic response);
- Ministry of Defence (strategic communication and NATO alignment);
- Communications Regulation Commission (Digital Services Coordinator);
- Council for Electronic Media;
- Law enforcement and prosecutorial bodies.

Bulgaria, therefore, has the institutional architecture required to respond to influence operations. In practice, however, action is typically triggered only once specific legal thresholds are reached, and responses follow formal legal procedures. This means that early detection, disruption, and mitigation are not always linked through a continuous operational workflow across institutions.

Bulgaria hosts a concentrated cluster of advanced technology and OSINT actors - including Ontotext, Sensika and Adatapro - capable of sophisticated data analysis, behavioural pattern identification and infrastructure-level assessment. This technical ecosystem provides the operational muscle required for early detection and infrastructure-focused disruption measures.

The mapping shows a diversified ecosystem:

- 45 government and regulatory actors;
- 28 media and journalism entities;
- 24 civil society organisations;
- 19 academic institutions;
- 17 specialised technology firms.

In contrast to systems where detection capacity sits primarily within government, Bulgaria's strength lies in:

- Private-sector analytical depth;

- Academic research integration;
- Hybrid security-sector collaboration;
- Cross-border OSINT engagement.

7.3 Poland

Poland's localisation combined national government and civil society consultations with structured ecosystem mapping. A total of **89 strategic individuals and organisations** were identified across government, civil society, academia, media and platform representatives.

Consultations confirmed strong institutional coverage, including:

- Advanced analytical monitoring capacity (notably NASK);
- Criminal investigative capability (Cyber Crime Bureau, Prosecutor's Office);
- Diplomatic escalation pathways (Ministry of Foreign Affairs);
- Sanctions enforcement competence (Ministry of Interior and Administration);
- Cyber defence structures (Cyber Space Command);
- Cross-government coordination bodies (Department of National Security);
- Public communication capacity (Government Information Centre);
- Civil Society advisory structures (Resilience Council).

All lifecycle phases are institutionally covered. However, these functions often operate in parallel rather than through a shared operational sequence. Responses are typically triggered through criminal thresholds, sanctions designation or diplomatic escalation, resulting in a legally coherent but sometimes operationally delayed response model.

Poland's stakeholder mapping also demonstrates a strong civil society and technical detection ecosystem:

- 36 civil society organisations
- 14 academic institutions
- 12 media and journalism entities
- 19 government/regulatory bodies

This configuration supports early detection, OSINT and behavioural monitoring, analytical classification of coordinated behaviour, research-informed workflow testing, and platform engagement under DSA procedures.

As a result, Poland demonstrates particular strengths in:

- Early case detection;
- OSINT and behavioural monitoring;
- Analytical classification of coordinated inauthentic behaviour;
- Research-informed workflow testing;
- Platform engagement under Digital Services Act procedures.

7.4 Romania

Romania’s localisation combined national consultations with ecosystem mapping. A total of **39 strategic organisations** were identified across government, regulatory authorities, civil society, academia, media and security structures. While smaller than the ecosystems mapped in other countries, Romania’s network is relatively balanced and includes the key institutions required to respond to influence operations.

The consultations indicated that escalation often depends less on institutional mandates and tends to occur reactively and in a rather improvised manner, once an issue becomes publicly visible, rather than being triggered at an early analytical stage.

Romania’s government ecosystem includes:

- ANCOM (Digital Services Coordinator under the DSA);
- National Audiovisual Council (CNA);
- Permanent Electoral Authority (AEP);
- Central Electoral Bureau (BEC, temporary institution with correspondents in territory);
- Financial investigation and AML bodies;
- Ministry of Foreign Affairs (resilience and external coordination);
- Ministry of Interior
- Parliamentary committees (Culture and Mass Media, Defence, ITC);
- DNSC, coordinating civilian security and cyber-resilience actors at the government level;
- Cyberint, the specialised structure of SRI (the intelligence service), dealing with online threats to national security.

All framework phases are institutionally covered. However, consultation findings suggest that the current response model is largely complaint-driven, meaning that action is often initiated after reports or formal complaints are submitted rather than through proactive operational coordination. The system is also more clear-cut during the official electoral campaign period, when the BEC is established with broad powers to administer the elections, oversee their integrity and rule on irregularities; it is less so in the periods in between.

Romania's configuration provides several important strengths:

- Direct access to DSA enforcement mechanisms (ANCOM) and broadcast regulation (CNA);
- Strong investigative journalism, OSINT, and fact-checking capability;
- Active civil society organisations, including groups working on gender and human rights;
- Security and resilience alignment via DNSC and E-ARC.

This ecosystem supports strong mitigation capacity and credible escalation channels, but would benefit from clearer triggers and coordination mechanisms for earlier-stage responses.

7.5 Comparative Analysis of the Countries

The cross-country analysis reveals a consistent structural pattern across all four participating Member States, while also highlighting different national entry points into the disruption lifecycle. The consultations show that the ecosystems countering influence operations in Czechia, Poland, Romania and Bulgaria differ in their institutional arrangements, but face many of the same operational challenges. **This combination of national diversity and shared structural challenges makes it possible to standardise how responses are sequenced, without requiring countries to harmonise their legal authorities and or institutional responsibilities.**

7.5.1 Shared Structural Strengths

Across all four countries, the following core capacities are present:

- Established monitoring and analytical capacity within public institutions and/or civil society;
- Strong mitigation capability, particularly in public communication and contextualisation, once influence activity becomes visible;
- Policy-level awareness of influence operations as a democratic resilience issue.

These strengths indicate that the main challenge is not a lack of institutional competence or awareness but rather operational alignment and coordination. The key building blocks required for effective disruption already exist in each system.

7.5.3 Recurring Operational Gaps

Despite national variation, consultations identified similar structural coordination challenges across all systems:

1. **Disruption Timing Gap** - Intervention often occurs after influence activity becomes publicly visible, rather than during its escalation phase. Institutions frequently wait for legal certainty even in cases where procedural or platform-based measures could be activated earlier.
2. **Fragmented Escalation Pathways** - Multiple authorities may hold relevant competencies, but predefined sequencing between detection, decision-making and intervention is often absent. As a result, escalation frequently depends on informal coordination.
3. **Underutilisation of Procedural Tools** - Platform reporting mechanisms, regulatory escalation channels and infrastructure-based disruption measures exist, but are unevenly understood or applied across institutions.
4. **Parallel Assessment Processes** - Monitoring outputs are often assessed independently by different actors, which can delay the collective qualification of influence operations.

These gaps are not unique to any single jurisdiction. Rather, they reflect a broader structural misalignment between rapidly evolving, cross-border influence operations and nationally segmented decision-making processes. In some countries, however, certain aspects of this structure are expected due to existing legal frameworks and institutional mandates..

7.5.4 Coordination Challenge

While the overall structural pattern is consistent across countries, differences emerge in three main areas:

1. **Early Warning Maturity** - some systems integrate civil society and institutional monitoring more closely than others, enabling earlier identification of potential influence operations.
2. **Platform Escalation Leverage** - familiarity with platform notice-and-action mechanisms and regulatory tools varies between countries, affecting how effectively actors can escalate cases.
3. **Institutional Sequencing** - clarity regarding which authority leads at different evidence thresholds differs between jurisdictions.

7.5.5 Systemic Nature of the Challenge

The recurrence of similar patterns across four distinct administrative systems confirms that the issue is systemic rather than country-specific.

Influence operations:

- unfold in real time;
- exploit cross-border platform infrastructures;
- combine narrative, behavioural and technical components.

Institutional responses, by contrast:

- remain mandate-bound;
- rely on sectoral qualification;
- activate sequentially rather than in parallel.

This structural mismatch increases systemic exposure across interconnected European information environments.

Without a shared operational workflow standard, Member States risk:

- Over-reliance on post-impact mitigation;
- Inconsistent activation of available countermeasures;
- Reduced interoperability during cross-border incidents;
- Duplication of analytical effort without coordinated escalation.

7.5.6 Strategic Added Value of a Standardised Framework

The comparative findings demonstrate that a common disruption methodology provides added value precisely because national systems differ.

By standardising sequencing rather than authority, the framework:

- Accelerates transition from detection to proportionate intervention;
- Clarifies escalation triggers without altering mandates;
- Enables parallel handling across regulatory, platform and enforcement pathways;
- Connects civil society to institutional response;
- Strengthens cross-border interoperability;
- Supports structured documentation and shared learning.

The framework, therefore, functions as a coordination layer that:

- Preserves subsidiarity;
- Respects national legal competences;
- Enhances interoperability within the EU democratic resilience architecture.

Standardisation in this context does not mean centralisation. It means establishing a shared operational grammar and situational awareness of existing mandates, capabilities, and structures. The consultations across four Member States demonstrate that such a grammar and situational awareness is both feasible and necessary.

8. Integrating Gender Considerations into the DISRUPT Framework

Influence operations increasingly exploit gendered narratives and tactics to undermine the credibility and participation of public figures, particularly women in politics, journalism, and civil society. [Research](#) from #ShePersisted shows that such campaigns frequently rely on sexualised disinformation, synthetic media, coordinated harassment, and intimidation tactics to delegitimise targets and discourage participation in democratic processes.

The development of the framework's gender-aware components combined desk research with targeted consultations with civil society organisations specialised in gendered disinformation and online harassment. These consultations ensured that the workflows reflect both existing research and practical operational experience in responding to gendered influence campaigns.

Gendered disinformation campaigns rarely rely on a single tactic. Instead, they typically combine multiple influence operation techniques - such as smear narratives, deepfakes, harassment, impersonation, and doxing - which may appear sequentially or simultaneously and often escalate over time. **From an operational perspective, these campaigns function as a multi-layered influence operation**, combining narrative manipulation with amplification infrastructure and intimidation tactics.

Integrating Gender into the Disruption Framework

The Disruption Framework addresses **gendered influence operations through integrated workflows rather than through a separate response architecture**. This approach ensures that gendered campaigns can be detected, analysed, disrupted, and mitigated using the same evidence-based operational logic applied to other influence operations.

Gender considerations are incorporated where they strengthen operational capabilities, particularly in:

- **Narrative detection**, including the identification of sexualised smear narratives and delegitimisation campaigns;
- **Synthetic media analysis**, including deepfake or manipulated intimate imagery;
- **Behavioural monitoring**, including coordinated harassment and intimidation patterns;
- **Legal and regulatory escalation**, including privacy violations, non-consensual intimate imagery, or defamation.

By embedding these elements into existing workflows, practitioners can identify gendered influence campaigns without creating parallel governance structures or identity-based enforcement mechanisms.

Gendered Campaign Patterns

Research indicates that gendered influence operations tend to appear in a limited number of recurring campaign patterns. These include:

- **Sexualised delegitimisation campaigns**, in which false accusations related to sexual behaviour or morality are used to undermine credibility;
- **Synthetic intimate imagery campaigns**, involving manipulated or AI-generated sexual content;
- **Coordinated harassment campaigns**, aimed at silencing or intimidating targets;
- **Doxing campaigns**, where personal information is exposed to create real-world risk.

In practice, **these tactics frequently overlap**. A smear narrative may first spread through coordinated posts, followed by the introduction of synthetic media, and eventually escalate into harassment or doxing. **Because these campaigns operate across multiple layers, effective disruption must address both the narrative and the supporting infrastructure.**

The campaign patterns integrated into the framework were derived from research literature and practitioner consultations with civil society organisations specialising in gendered disinformation.

Operational Value

Integrating gender-aware workflows strengthens the Framework's ability to respond to influence operations that seek to suppress participation in democratic processes through intimidation and delegitimisation. At the same time, it preserves the framework's core principles of neutrality, proportionality, respect for rights, and evidence-based disruption. By embedding gender considerations into operational workflows rather than creating separate

governance structures, the framework enables practitioners to respond effectively to gendered influence campaigns while maintaining a consistent methodology for countering influence operations more broadly.

9. Structured Cooperation Rather Than Ad Hoc Coordination

Across countries, cooperation often relies on informal relationships and personal networks. While effective in individual cases, such arrangements lack predictability, continuity and scalability.

9.1 Establishing Structured Communication Channels

Detection of influence operations is often distributed across civil society organisations, researchers, investigative journalists and specialised monitoring units within government. Without predictable routing mechanisms, early signals may remain isolated or be assessed in parallel.

To operationalise this capacity, institutions may:

- designate clear institutional contact points;
- define documentation standards required for escalation;
- establish secure channels for structured information exchange;

9.2 Defining Flagging, Escalation, and Delegation Triggers

Whole-of-society coordination requires clarity on when cooperation should begin.

These include:

- confirmation of coordinated behaviour;
- emergence of amplification risk;
- indications of societal impact.

Member States can integrate these triggers into existing coordination mechanisms by:

- defining thresholds for inter-agency notification;
- clarifying which authorities assess proportionality at each stage;
- identifying when platform or regulatory mechanisms should be activated.

This enables earlier and proportionate intervention without centralising authority.

9.3. Mapping Countermeasures to Competent Authorities

A whole-of-society approach is effective only if actors understand which disruption options exist and who holds competence to activate them.

Mapping the measures outlined in the DISRUPT Framework towards the mandates and capacities of authorities and national legislation would be an important step towards that.

This mapping exercise expands operational awareness without requiring new legal instruments.

9.4. Integrating Civil Society into Advisory Coordination

Civil society actors frequently provide early contextual analysis and technical expertise. They can also take certain measures more quickly - or undertake actions that governments cannot take at all - while governments have access to authorities and measures that are not available to civil society.

To leverage this complementarity, governments can establish standing or temporary working groups that bring together civil society organisations and relevant public authorities.

The Framework supports the creation of such working groups based on localised workflows. These groups would combine civil society and government actors around specific tasks and could be activated when a workflow-specific type of influence operation is detected. By relying on predefined escalation paths, this structure enables faster and better coordinated responses.

While national working groups operate independently and within their own mandates, they could also be connected through a broader European network.

Such a decentralised yet connected democracy-defence structure would support joint methodology development, shared technology procurement, capacity-sharing during major events and crises, and collaborative policy development.

10. Whole of Society Approach

Influence operations exploit societal divisions, information asymmetries and procedural fragmentation. Therefore, effective disruption requires coordination across public authorities, civil society, policymakers, technical actors and networks.

The consultations demonstrated that no single actor possesses all the necessary capabilities. Monitoring expertise frequently resides within specialised civil society organisations. Regulatory and enforcement authority lies with public institutions. Public trust is shaped by media, community leaders and civil society intermediaries.

A whole-of-society approach does not dissolve institutional responsibility. It clarifies how distinct roles interact within a shared operational logic.

10.1 Roles in a Distributed System

The Framework distinguishes functional roles rather than prescribing institutional arrangements. It specifies types of actors, legislation and government agencies that may be involved.

This distinction allows the model to operate across diverse national systems while adapting to existing mandates and organisational structures.

Four core functions are identified within the lifecycle:

- **Detection actors** - identify, document and qualify patterns of coordinated behaviour;
- **Decision authorities** - assess proportionality and determine appropriate escalation within their legal competencies;
- **Implementation actors** - carry out platform-based, regulatory, procedural or infrastructure-related measures;
- **Communication and resilience actors** - provide contextual explanation, public clarification and longer-term societal stabilisation.

These functions may be performed by different organisations depending on the national context. In some cases, a single institution may perform multiple roles. What remains constant is not the institutional configuration, but the operational sequence.

By defining roles rather than institutions, DISRUPT allows government and non-government actors to coordinate their actions through a shared escalation process. This preserves institutional responsibility while reducing fragmentation and duplication.

10.2 Actors

While most of the actions proposed by the Framework can be carried out by a range of actors, the Framework identifies those best placed to undertake them. A single organisation may

perform multiple roles. What matters is the sequencing: evidence moves predictably from detection to decision to action.

The following section outlines the mandates of these actors and where they are best positioned within the disruption kill-chain.

Government Ministries and Agencies

Ministries and their agencies, such as foreign ministries or specialised counter-FIMI bodies, often have mandates to monitor and respond to digital threats. Ministries typically host strategic communication units, can propose legislation, and produce comprehensive analytical reports. In some cases, ministries are also given a coordination role, overseeing national efforts to address influence operations. A smaller number of specialised agencies have explicit mandates to detect, analyse, and disrupt influence operations, although such institutions remain relatively rare.

Ministries are often strongest in the disruption and mitigation phases, where they can apply public pressure and, in some cases, legal or regulatory leverage on service providers and social media platforms to act against an operation. For detection and analysis, ministries frequently rely on input from specialised agencies, other government bodies, or civil society organisations.

Regulators

Regulators are enforcing specific laws or regulatory frameworks. Their oversight and enforcement powers may allow them to access proprietary information and take legal actions that can lead to the disruption of influence operations.

Regulators are strongest in the **preparation and disruption phases**. They frequently act on leads provided by other actors and then gather evidence to initiate regulatory enforcement actions.

Security and Intelligence Services

Security Services and intelligence services may hold mandates related to countering domestic and foreign influence operations. These mandates and capabilities differ widely, but may include access to proprietary information, infiltration of hostile networks, provision of intelligence assessments to other agencies, and the ability to support arrests or investigations under national security legislation.

In most cases, these services are best positioned to contribute to the preparation and disruption phases, particularly by accessing non-public information and supporting legal or investigative actions in coordination with other authorities. Mitigation activities are more often carried out by civil society organisations or other government bodies.

Law Enforcement

Law enforcement, including police forces and judicial authorities, is responsible for investigating potential criminal activity and taking legal actions in cases where influence operations violate the law. The capabilities and resources available to investigate digital crimes of this nature vary significantly between Member States.

Law enforcement actors are typically best positioned in the preparation and disruption phases, where they can gather evidence and initiate legal proceedings. In many cases, they rely on monitoring conducted by third parties to identify potential cases.

Government Research Institutes

Government-funded research institutes are often tasked with producing knowledge and analysis related to influence operations. Their work may include policy-oriented studies, post-incident investigations, and the development of methodologies and analytical frameworks. In some cases, institutes also conduct live monitoring or operational support, although this is relatively uncommon.

These institutions are most commonly active in the preparation and mitigation phases, contributing to evidence development, analytical understanding and policy recommendations.

OSINT Researchers

OSINT researchers collect and analyse data from public sources. Rather than focusing solely on individual claims, they often analyse broader narratives, attribute activities to specific actors, examine the infrastructure used in influence operations, and assess potential systemic risks.

They are typically best positioned in the preparation phase and disruption phases, where they help build cases, document evidence, and report findings to relevant authorities or platforms. Mitigation activities are generally carried out by other actors.

Journalists

Journalists can broadly be divided into two groups: reporters and investigative journalists.

Reporters are often strongest in the disruption and mitigation phases. They can draw public attention to influence operations, question companies or institutions about their responses, and complex issues to the public in accessible terms.

Investigative journalists, who often work with reporters, are more active in the preparation and disruption phases, conducting in-depth investigations, interviewing sources, infiltrating networks where possible and exposing the actors behind influence operations.

Fact-checkers

Fact-checkers are well-positioned to engage with the preparation and disruption phases. They are also journalists, but given the scope and focus of their work, deserve their own category.

In the preparation phase, they can identify emerging cases and verify the accuracy of the claims used in influence operations. In the disruption phase, they can report misleading content and communicate findings to platforms and relevant authorities. Fact-checking can, in some cases, also support mitigation through the publication of fact-check articles targeted at specific audiences. However, these efforts are most effective when combined with the activities of other actors, such as strategic communicators.

Cybersecurity Professionals

Cybersecurity professionals are best positioned in the preparation and mitigation phases. During the preparation phase, their technical expertise can help investigate the technical infrastructure used in influence operations. In the mitigation phase, they can help develop recommendations to address the technical vulnerabilities that enabled the influence operation, such as weaknesses in platform policies related to inauthentic behaviour or spam.

Strategic Communicators

Strategic communicators are professionals responsible for shaping and coordinating public messaging within governments, institutions, or organisations. They are best placed in the **mitigation phase**, where they translate analytical findings into clear public communication, raise awareness of influence operations, mitigate their impact, and coordinate messaging across institutions to ensure responses are timely, consistent, and credible.

Campaigners

Campaigners can support the disruption and mitigation phases by mobilising public attention around influence operations and advocating for responses from platforms, institutions, or policymakers. Through organised campaigns, they can help maintain pressure on relevant actors to address harmful activities.

Activists

Activists can mobilise support online and offline, organising protests or other peaceful actions to draw attention to a situation. While they are a relatively underexplored partner in disruption efforts, activist networks can amplify awareness and contribute to broader societal responses.

Elected officials

Elected politicians hold public influence through their institutional roles. They are often quoted by the media, maintain social media profiles, and can raise issues in parliament or other political forums. They have a role overseeing legislation and regulation, with a role to play in initiating policy and regulatory processes.

These tools allow them to contribute to disruption efforts, for example, by applying political pressure on the service providers or public authorities. They can also play an important role in the mitigation phase by raising awareness and proposing or initiating policy responses, or applying political pressure on other decision-makers.

Influencers

Influencers - whether on social media or within specific professional or community contexts - can play a significant role in the **mitigation phase**. By reaching targeted audiences and lending credibility to messaging, they can help disseminate accurate information and counter the impact of influence operations.

Legal professionals

Lawyers can be important actors in the **disruption phase**, utilising civil law tools to challenge influence operations. This may include legal action related to intellectual property, defamation, or other applicable laws. Lawyers can also help protect other actors against Strategic Lawsuit Against Public Participation (SLAPP) suits.

Coordination

To facilitate coordination between all of these actors, Alliance4Europe has developed a **new platform for knowledge aggregation, structured information exchange, and disruption coordination**.

Actor	Role / Description	Primary Phase(s) of Intervention
Ministries & Government Agencies	Coordinate national responses, apply political or regulatory pressure, and produce strategic analysis or policy responses.	Disruption, Mitigation
Regulators	Enforce laws and regulatory frameworks, access proprietary information, and initiate enforcement actions.	Preparation, Disruption
Security & Intelligence Services	Collect intelligence, investigate hostile actors, and support disruption under national security mandates.	Preparation, Disruption

Law Enforcement	Investigate illegal activities and pursue legal action against influence operations that violate the law.	Preparation, Disruption
Government Research Institutes	Produce research, analysis, methodologies, and policy recommendations related to influence operations.	Preparation, Mitigation
OSINT Researchers	Analyse open-source data to identify patterns, attribute actors, and document influence operations.	Preparation, Disruption
Journalists	Investigate and expose influence operations, raise public awareness, and hold actors accountable.	Preparation, Disruption, Mitigation
Fact-checkers	Verify claims used in influence operations and report misleading content to platforms and authorities.	Preparation, Disruption
Cybersecurity Professionals	Investigate technical infrastructure and recommend solutions to address vulnerabilities exploited by influence operations.	Preparation, Mitigation
Strategic Communicators	Translate findings into clear messaging, raise awareness, and mitigate the impact of influence operations.	Mitigation
Campaigners	Mobilise public attention and advocate for responses from institutions and platforms.	Disruption, Mitigation
Activists	Organise public mobilisation and protests to draw attention to influence operations.	Disruption, Mitigation
Politicians	Use political platforms and institutional authority to raise issues, apply pressure, and propose policy responses.	Disruption, Mitigation
Influencers	Reach targeted audiences and amplify messaging that counters influence operations.	Mitigation
Lawyers	Use legal tools such as intellectual property, defamation, or other civil law mechanisms to challenge operations and protect actors from SLAPP suits.	Disruption

Table 1: Overview of Actor Roles in Disruption Framework

11. Threat Intelligence Database and Coordination Platform (TRANSCRIPT) - Technical Operationalisation

The Framework and workflows have also been integrated into the newly developed threat intelligence database, the Threat Intelligence Database and Coordination Platform (TRANSCRIPT). TRANSCRIPT is designed to provide democratic countries and the European Institutions with a coordination and knowledge-aggregation platform that enables collective responses to influence operations. It functions as a digital research infrastructure supporting analysis, coordination, and disruption activities.

TRANSCRIPT supports:

- Standardised and collaborative case documentation;
- Collaborative attribution of actors;
- Disruption tracking and coordination;
- Narrative framework development, mapping, and fact-checking aggregation;
- Cross-jurisdictional knowledge sharing.

TRANSCRIPT operates as a single digital environment with three core layers.

First, a database layer enabling the collective aggregation of information on actors, cases, narratives and distribution channels.

Second, a smart text editor allows users to draft reports while automatically linking entries within the database.

Third, a “Disrupt” function uses the DISRUPT Framework and its workflows to suggest concrete measures for disrupting a specific influence operation.

This knowledge infrastructure strengthens preparedness by accelerating the identification of emerging patterns, providing evidence of systemic regulatory non-compliance, and improving interoperability between actors across Member States.

12. Recommendations

The consultations demonstrate that Member States possess significant analytical and mitigation capacity. The principal opportunity lies in strengthening structured coordinated action focused on disruption during the early stages of influence operations.

The following recommendations outline pathways through which both the EU and Member States can enhance coordination and interoperability.

12.1 EU Level: Democracy Shield

As the European Union advances its democratic resilience architecture, DISRUPT framework offers a structured and immediately deployable operational coordination model capable of strengthening coherence across Member States.

Influence operations increasingly transcend national borders, targeting multiple societies simultaneously through shared platforms and synchronised narratives. The Digital Services Act, FIMI-related coordination mechanisms, such as the Rapid Alert System, and hybrid threat cooperation structures address important dimensions of this systemic risk environment.

The disruption framework complements and aims to support these instruments by providing a structured operational sequencing logic that connects detection, assessment, disruption and mitigation across jurisdictions. In doing so, it strengthens coordinated incident management and enhances interoperability between Member States without altering institutional competences.

Within the Democracy Shield architecture, the framework could function as an operational coordination model supporting structured incident management across Member States and EU institutions. Leveraging the framework, implementation steps would include:

- Recognising the lifecycle model (Detection → Assessment → Disruption → Mitigation) as a shared operational reference for influence incident management;
- Encouraging alignment across Commission Directorates General and Services, EEAS, and national governments, law enforcement, regulators, and strategic communications efforts.

- Promoting aligned documentation, evidence standards, and case-classification standards to improve comparability and cross-border situational awareness;
- Supporting structured cross-border incident coordination mechanisms when influence operations affect multiple Member States simultaneously;
- Facilitating interoperability between national authorities through shared terminology;
- Adopting the methodology within EU-level coordination bodies, including for example, the Centre for Democratic Resilience, as a reference framework for democratic threat response.
- Supporting EU and national law enforcement across key areas, including the Digital Services Act, sanctions enforcement, as well as potential overlap with a range of online harms, with potential links to unlawful activities.
- Systematised tracking of the intersection between cyber threats and influence operations, effectively sharing data between cybersecurity and counter-IO practitioners, and taking concerted actions to tackle threats.
- More comprehensively integrating efforts to counter influence operations and FIMI within the larger framework to counter hybrid and cyber threats.
- Highlighting efforts to counter FIMI and influence operations within the EU's cybersecurity programmes.
- Ensuring that the upcoming long-term EU budget, Multiannual Financial Framework (MFF) integrates investment in information integrity in resilience, in line with the commitments made in the Democracy Shield.
- Including efforts to counter information threats within commitments to counter hybrid threats within MFF programmes including the European Competitiveness Fund, AgoraEU, and Readiness2030, among others.

The EU needs a strategic coordination node for countering cross-border influence operations, ensuring that national detection outputs and disruption measures are aligned in timing and proportionality, along with EU measures. By operating on the basis of a shared framework logic, an initiative like the Centre for Democratic Resilience, for example, could enhance collective situational awareness without centralising enforcement authority.

Importantly, this approach standardises operational workflows rather than redistributing power. It does not require harmonisation of national mandates or expansion of EU competences. Instead, it establishes a common operational language and workflow structure that enables faster and more coherent collective response

Within a broader democratic resilience framework, the disruption methodology can function as the operational layer linking early warning systems, regulatory instruments, and structured institutional coordination. In doing so, it transforms existing capabilities into a predictable, interoperable European response architecture.

12.2 National Level

Member States can strengthen preparedness and coordinated response capacity through the following measures:

- **Clarifying escalation and coordination triggers** - Defining evidence-based handover thresholds between detection actors and competent authorities reduces hesitation and parallel assessment. Establishing clear triggers for inter-agency notification ensures that proportionate disruption measures are considered before influence operations reach peak amplification. It clarifies timing.
- **Expanding non-criminal disruption pathways** - A significant number of procedural, regulatory and platform-based measures are available below criminal thresholds. Systematically mapping and operationalising these tools - including notice-and-action procedures, regulatory referrals and infrastructure interventions - broadens the disruption toolkit and enables graduated response. This expands operational awareness rather than legal competence.
- **Structuring engagement with civil society** - Civil society and monitoring actors frequently detect influence operations at early stages. Formalising routing mechanisms through which qualified signals can inform competent authorities enhances early warning without transferring enforcement responsibility. Structured advisory or liaison mechanisms ensure distributed detection capacity strengthens institutional decision-making while preserving accountability.
- **Embedding knowledge aggregation** - Institutionalising standardised documentation strengthens preparedness over time. Mapping applied measures against outcomes improves proportionality and accelerates response in future incidents. Embedding knowledge aggregation at the national level also facilitates interoperability with cross-border coordination mechanisms.
- **Strategic Effect at National Level** - Collectively, these steps enhance earlier and more proportionate disruption; reduced reliance on post-impact mitigation; greater

predictability in inter-agency coordination; stronger alignment with emerging European resilience standards.

- **Strengthening the enforcement of the Digital Services Act** in line with overall European efforts.
- **Strengthen sanction enforcement** by more systematically tracking sanctions violations in the information space.
- **Strengthening law enforcement on online harms** which are often corollary to FIMI and influence operations, including cyberattacks.
- **Align national and European funding** to tackle information integrity, cybersecurity, and information threats.
- **Operationalising a whole-of-government approach** - connecting relevant ministries, authorities, and agencies to collaborate on the issue.

12.3 Funding Coordination

To maximise resilience impact, funding strategies should support the development of operational coordination infrastructure and long-term capabilities, rather than focusing predominantly on short-term or event-driven projects. This is especially important for CSOs, which constitute a significant part of the counter-IO ecosystem, but rarely receive stable, long-term funding. Sustained support would allow these actors to build durable capacity, retain expertise, and contribute more effectively to continuous monitoring and disruption efforts.

Strategic investment within existing democratic resilience instruments could prioritise:

- Setting up operational collaboration structures connecting civil society;
- Long-term tooling and tech provision to civil society;
- Early warning documentation systems;
- Knowledge aggregation platforms and structured workflow mechanisms;
- reinforcing structured engagement between civil society and competent authorities.

Targeted investment in coordination architecture strengthens timing, interoperability and collective resilience.

The new Multiannual Financial Framework (MFF) 2028-2034 provides an opportunity to support these activities under Horizon Europe, the European Competitiveness Fund, Readiness2030 and the Agora Programme. In line with the flexibility principle of the Commission MFF proposal, it is vital to ensure coherent funding across the comprehensive research to deployment and prevention chain.

13. Conclusion

Influence operations are adaptive, cross-border and strategically sequenced. Democracy defence measures remain institutionally bounded and procedurally cautious. The resulting gap is not one of authority or awareness, but of operational timing.

The findings confirm that effective disruption capacity is not solely a technical challenge, but a governance and coordination challenge. Influence operations exploit procedural fragmentation as much as informational vulnerabilities, making structured workflows across mandates and institutional levels a central requirement of democratic resilience.

The consultations conducted across four Member States confirm that detection capacity exists, mitigation capability is strong, and some relevant legal and procedural tools are available. What is often missing is a structured progression that connects early signals to proportionate disruption before amplification peaks.

The DISRUPT framework presented in this report addresses that coordination gap. It does not introduce new mandates or centralise authority. Instead, it standardises workflows. By linking evidence maturity to countermeasure selection and clarifying escalation triggers, it enables earlier and more predictable action within existing institutional structures.

The localisation process demonstrates that the framework is adaptable across diverse administrative systems. Its logic is interoperable without requiring legal harmonisation. It strengthens disruption without compromising democratic safeguards.

As influence operations increasingly transcend national borders, Member States benefit from shared operational language and aligned escalation concepts. Standardisation at the level of process - rather than power - enhances collective resilience while respecting subsidiarity.

The framework represents a structured contribution to European democratic resilience architecture. It provides a ready-to-adopt European operational standard for coordinated disruption of influence operations and is immediately suitable for structured pilot implementation within the European Democracy Shield architecture. It offers a scalable coordination standard capable of reinforcing democratic resilience across the EU. Its value lies not in replacing existing systems, but in connecting them - transforming distributed capacity into structured, proportionate and timely disruption.

Adoption of a shared standard IO framework would reduce strategic asymmetry between coordinated hostile actors and procedurally fragmented democratic responses.