DISRUPT FRAMEWORK

ROMANIA

TOOLKIT

Alliance 4Europe

EXPERT FORUM

ESGA

TABLE OF CONTENTS

Foreword

Romania occupies an important position in the European information environment, particularly in the context of ongoing regional instability and the persistent threat of foreign influence operations. As a Member State of the European Union and NATO, and as a country with a dynamic electoral landscape, Romania is exposed to influence operations that target democratic processes, public trust, and institutional credibility. These activities are not limited to electoral periods but form part of a broader landscape of hybrid threats, often intersecting with information manipulation, economic interests, and strategic narratives aimed at shaping public perception.

Beyond their immediate informational impact, such operations contribute to polarisation, undermine trust in institutions, and can weaken social cohesion over time. Electoral periods are particularly sensitive, as influence operations may seek to distort public debate, amplify misleading narratives, or exploit vulnerabilities in the information environment. Recent elections have also demonstrated the use of gendered smear campaigns and targeted harassment against women candidates and public figures, highlighting how influence operations can disproportionately affect participation in public life and democratic processes. This context makes the question of operational response both timely and critical, not only as a matter of security but also as a question of democratic resilience.

In Romania, civil society organisations, media actors, and independent researchers play a particularly important role in this landscape. They are often at the forefront of detection, analysis, and early warning, identifying emerging narratives, documenting cases, and bringing visibility to influence operations. Their work complements that of public institutions and forms a critical part of the national response ecosystem, particularly in a system where institutional monitoring capacity remains limited and response is often triggered by external signals.

At the same time, effective disruption depends on how these efforts connect with the broader system. Influence operations routinely span platforms, jurisdictions, and sectors, requiring coordination between civil society, public authorities, technology companies, regulators, and financial actors. In Romania, relevant capabilities exist across these domains, but coordination remains largely mandate-bound and case-specific, without consistently applied operational pathways linking detection to action. As a result, responses are often reactive and dependent on legal thresholds or complaint-driven processes.

Consultations conducted subsequently indicate that the Romanian response environment continues to evolve. Institutional awareness of disinformation and coordinated online manipulation appears higher following recent electoral experiences, and several authorities have introduced practical adjustments to procedures, communication practices, and inter-institutional contacts. However, levels of operational readiness remain uneven. While some institutions have developed specialised expertise and tools, others continue to face constraints related to staffing, technical capacity, or the routine integration of available capabilities into established workflows.

Taken together, these observations point to the continuing importance of operational coordination and implementation capacity. The effectiveness of response efforts may depend not only on the availability of relevant mandates, but also on the extent to which institutions are able to mobilise

specialist expertise, apply common procedures, route cases efficiently, and coordinate consistently during time-sensitive incidents.

The DISRUPT Toolkit is designed to support this coordination. It provides a structured way to organise existing capabilities, clarify roles, and sequence actions across the lifecycle of a case - from early detection to disruption and mitigation. By organising available measures into a shared operational logic, and by introducing a common vocabulary and repeatable workflows, the Toolkit aims to help practitioners understand *what can be done, when it can be done, and who can act*.

Dr. **Lumi Sarvela, Alliance4Europe** **Sorin Ionita, Expert Forum** **Angela Gramada, ESGA**

1. Introduction

Influence operations, including foreign information manipulation and interference (FIMI), coordinated inauthentic behaviour (CIB), and sanctions circumvention, present a sustained challenge to democratic processes, public trust, and national security. These activities evolve rapidly, often outpacing administrative procedures and legal response mechanisms, and frequently operate across institutional and sectoral boundaries.

In Romania, this challenge is shaped by a fragmented and mandate-bound institutional landscape, where responsibilities for addressing elements of the information environment are distributed across regulatory, electoral, financial, security, and communication authorities. Influence operations are not confined to specific events such as elections, but form part of a broader and persistent information environment in which manipulation, amplification, and hybrid threats can emerge across multiple domains.

In practice, detection, analysis, and early response are often driven by civil society organisations, media actors, and public reporting, while institutional action is typically triggered through complaints or once an incident reaches a level of public visibility. Key points of disruption are distributed across platforms, financial systems, regulatory authorities, and law enforcement bodies, rather than concentrated within a single actor. Public authorities play an essential role in legal enforcement and escalation, but effective response depends on how these actors operate within and across their mandates.

The Romanian ecosystem demonstrates broad institutional coverage but limited proactive monitoring and coordination, with most authorities acting within narrowly defined competences and lacking systematic detection capabilities. As identified in the consultation process, responses are often initiated only after formal complaints or external signals are received, and coordination takes place on a case-by-case basis rather than through structured workflows. This creates a gap between public signal, institutional assessment, and operational response—particularly in cases that do not clearly meet legal thresholds, such as coordinated inauthentic behaviour.

This toolkit presents a national localisation of the DISRUPT Framework, drawing on the DISRUPT Toolkit White Paper and on multi-stakeholder consultations conducted in Romania. It provides a structured operational framework to support coordinated action across public institutions, civil society, and the private sector, within existing mandates and roles.

The objective is not to propose institutional reform, but to enable more predictable, timely, and coordinated responses across the lifecycle of influence operations - from detection to disruption and mitigation. The Toolkit supports a *whole-of-society approach* by clarifying how different actors contribute, and how measures can be sequenced and combined in practice across sectors.

2. The DISRUPT Framework

The DISRUPT Framework is a country-agnostic operational model designed to structure responses to influence operations across three phases:

- **PREPARE** - collecting, securing, analysing, assessing, and documenting an influence operation
- **DISRUPT** - applying measures to disrupt ongoing activities
- **MITIGATE** - reducing harm and strengthening resilience.

The Framework is a combination of **phases, sub-phases, stages, measures, templates, workflows, and localised workflows**. Measures are the smallest operational building block of the framework: specific actions that can be taken to prepare, disrupt, or mitigate an influence operation. Workflows then organise these measures into step-by-step guidance for particular case types.

The Framework is designed to function across different national systems by focusing on sequencing rather than institutional redesign. It does not require new authorities or legal mandates. Instead, it provides a shared operational logic for moving from detection to analysis, from analysis to assessment, and from assessment to proportionate intervention.

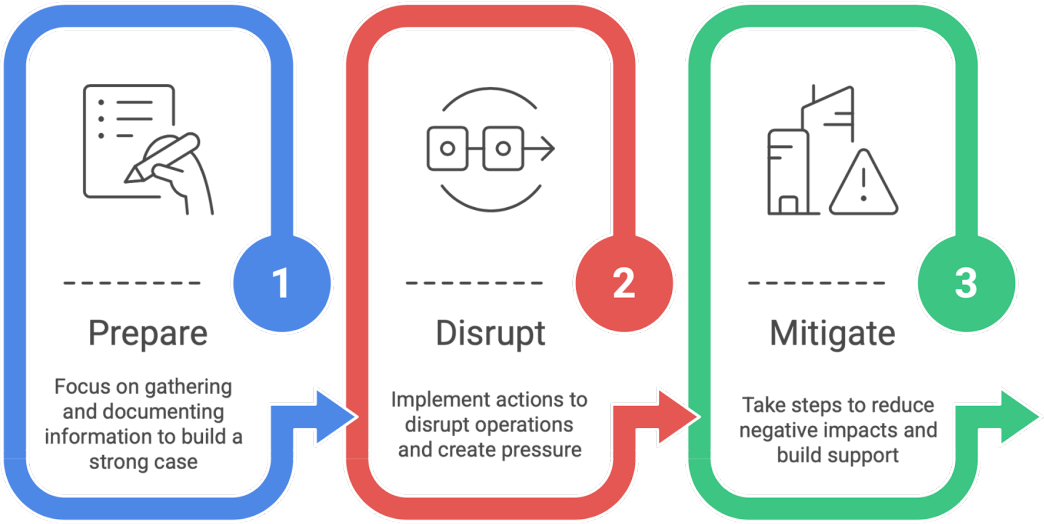
A central feature of the Framework is the use of decision points that help determine when a case has developed sufficiently to move from preparation into disruption, and when mitigation needs to be activated because disruption is delayed or insufficient. In this way, the Framework helps practitioners determine which measures are appropriate at which stage of an influence operation.

The framework also recognises that influence operations are not solely a state-level challenge. Early detection often depends on civil society organisations, researchers, journalists, and international coordination mechanisms, while regulatory and enforcement powers remain primarily with public authorities. The model therefore reflects a whole-of-society approach while preserving the distinction between monitoring, analysis, decision-making, implementation, and communication roles.

This Toolkit adapts that general framework to the Romanian context by mapping national actors, workflows, and constraints onto the common Prepare – Disrupt – Mitigate structure.

3. The Three Phases of the DISRUPT Framework

The DISRUPT Framework structures the response to influence operations across three core phases: **PREPARE, DISRUPT, and MITIGATE**. Each phase reflects a distinct operational objective and is associated with different types of measures, actors, and evidence requirements.



The phases should be understood as part of a **continuous lifecycle**, rather than as strictly linear steps. In practice, they may overlap, and multiple phases may be active at the same time.

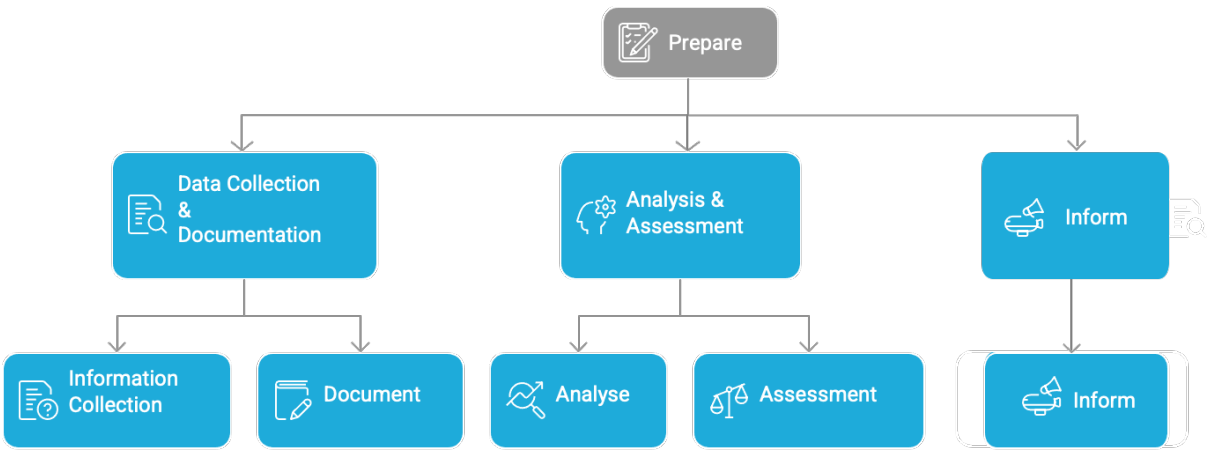
3.1 PREPARE

The PREPARE phase focuses on **building the evidentiary and analytical basis** for action.

It includes activities related to:

- identifying potential influence operations;
- collecting and securing relevant information;
- analysing behavioural patterns, narratives, and context;
- assessing whether a case is sufficiently developed to support further action.

The objective of this phase is to move from **initial signal to structured understanding**.



Outputs of the PREPARE phase typically include:

- documented case material;
- preliminary assessment of relevance and impact;
- identification of possible response pathways.

The PREPARE phase does not require full legal qualification or attribution. It provides the foundation for determining whether and how disruption measures can be applied.

3.2 DISRUPT

The DISRUPT phase focuses on **applying available measures to limit or stop the influence operation**.

This includes actions taken within existing mandates, such as:

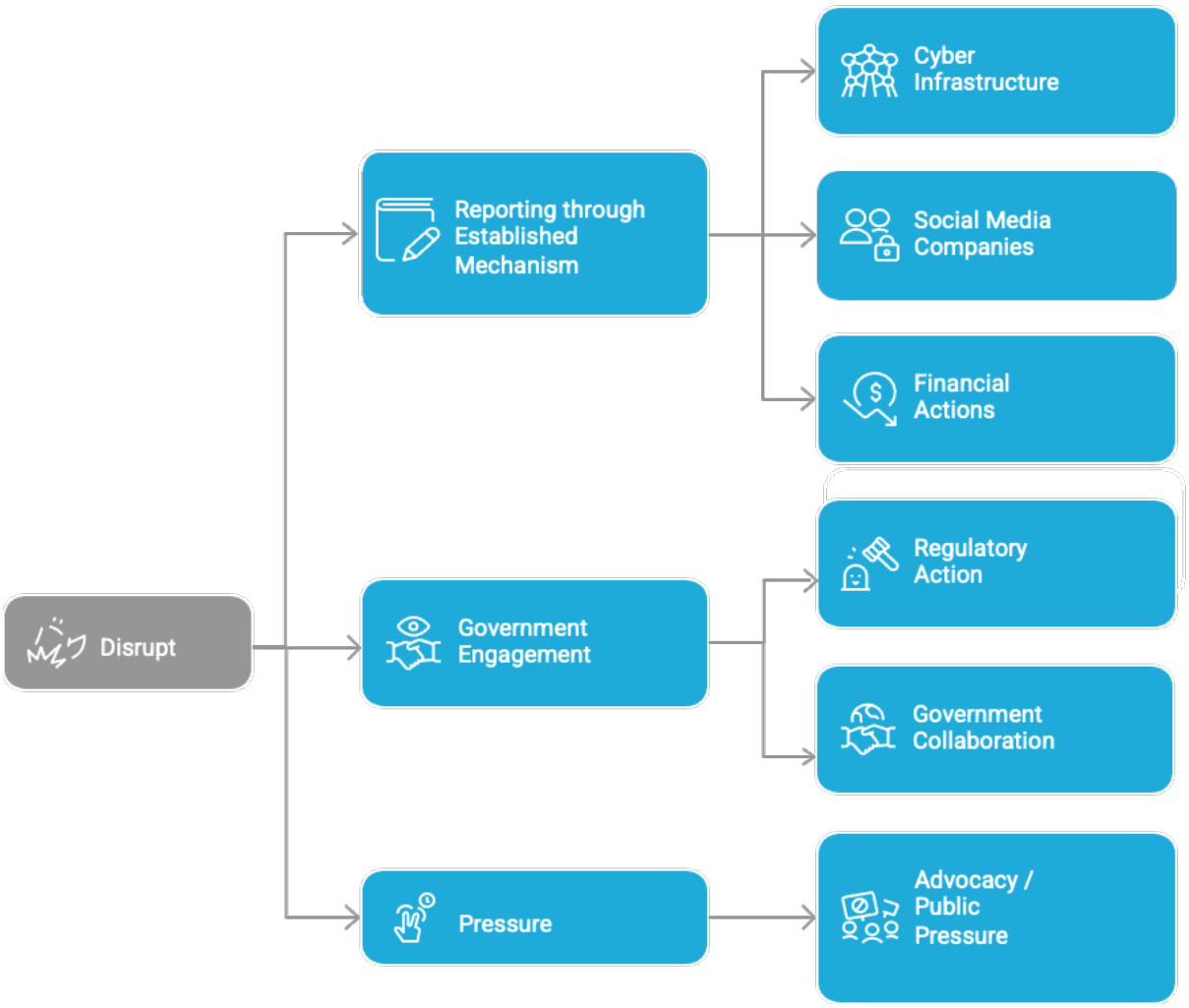
- regulatory or administrative measures;
- law enforcement or judicial processes where applicable;
- platform-related actions;
- diplomatic or coordination measures.

The objective of this phase is to translate analysis into **proportionate intervention**.

The selection of measures depends on:

- the nature of the activity;
- the available evidence;
- the applicable legal and institutional framework.

Not all cases will allow for strong enforcement measures. In such situations, the framework supports the use of other available actions, including coordination and communication measures, where appropriate.



A key principle is that, where possible, **measures may be applied in parallel**, rather than waiting for a single process to conclude.

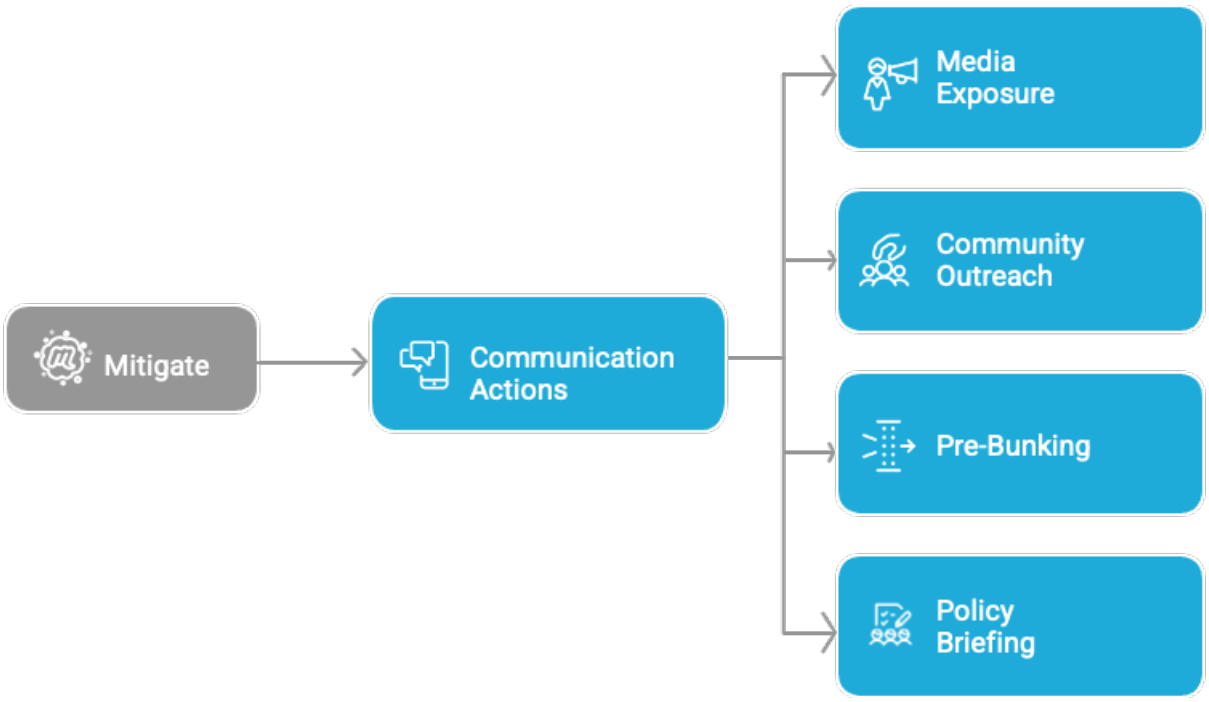
3.3 MITIGATE

The **MITIGATE** phase focuses on **reducing the impact of influence operations and strengthening resilience**.

It includes activities such as:

- public communication and awareness;
- contextualisation and explanation of the operation;
- capacity-building and training;
- support for institutional and societal resilience.

The objective of this phase is to **limit harm**, particularly where disruption is delayed, partial, or not feasible.



Mitigation is not only a final stage. In practice, it may be activated:

- alongside disruption measures;
- when disruption is not immediately available;
- after the main operational phase of a case has passed.

The MITIGATE phase also contributes to long-term preparedness by supporting learning and improving future responses.

3.4 Relationship Between the Phases

Together, they form a **continuous operational cycle**, supported by measures and workflows that guide practitioners from detection through to response and learning.

4. How to Use This Toolkit

This Toolkit is designed as a practical operational resource to support coordinated responses to influence operations across institutions and sectors.

The Toolkit should be used as a **combination of measures and workflows**, not as a rigid checklist. Measures are specific actions that can be taken to prepare, disrupt, or mitigate an influence operation. Workflows organise these measures into a logical sequence, showing how they can be combined and applied step-by-step in practice for different types of influence operations. In operational terms,

workflows are structured pathways that connect individual measures into an actionable process, helping practitioners move from detection to intervention

In operational use, the Toolkit helps practitioners:

- move from signal detection to structured analysis and assessment;
- identify which measures are available and appropriate at each stage;
- determine when and how to engage relevant actors;
- apply proportionate disruption or mitigation actions based on available evidence.

All cases should be understood through the three-phase lifecycle:

- **PREPARE** – collect, document, analyse, and assess evidence;
- **DISRUPT** – apply measures to limit or stop the operation;
- **MITIGATE** – reduce harm and strengthen resilience.

The Toolkit is also intended to support planning, training, and post-incident learning. Because the framework establishes a repeatable operational logic, it can be used to build shared standards, align expectations across sectors, and retain lessons from cases over time.

The Toolkit should therefore be applied **as a structured method to move from detection to proportionate intervention by selecting measures and combining them into workflows appropriate to the specific case**.

5. Purpose and Scope

The purpose of this toolkit is to provide a national operational reference for handling influence operations in Romania within existing mandates.

It has four objectives:

1. Clarify the national response sequence across the Prepare, Disrupt, and Mitigate phases.
2. Support more predictable coordination between relevant actors.
3. Localise the framework for two priority case types: coordinated inauthentic behaviour and sanctions-related cases.
4. Support whole-of-society cooperation by identifying where civil society, researchers, and international coordination mechanisms can strengthen response capacity.

The Toolkit is also intended to support implementation across institutions with differing levels of experience and operational capacity. While some authorities engage regularly with cases of information manipulation, others encounter them only occasionally. For this reason, the Toolkit combines strategic mapping with practical guidance, including referral pathways, evidence requirements, contact mechanisms, and examples of operational responses.

The Toolkit is designed to remain adaptable over time. As platform practices, legal frameworks, electoral procedures, and influence techniques continue to evolve, periodic review of workflows and operational guidance will help maintain its relevance and usability.

The toolkit does not replace institutional procedures or legal frameworks. It provides a shared operational layer intended to improve coordination, sequencing, and response timing.

6. National Response Structure in Romania

Romania's response to influence operations is characterised by a **distributed, mandate-bound institutional ecosystem**, where responsibilities are segmented across regulatory, security, electoral, and communication bodies.

Romania's response to influence operations is characterised by a distributed, mandate-bound institutional ecosystem, where responsibilities are segmented across regulatory, security, electoral, and communication bodies. In addition to formal institutional mandates, several inter-institutional coordination mechanisms address cybersecurity, hybrid threats, election integrity, and information risks. These provide channels for information exchange and situational awareness, although their structure, frequency, and operational role vary across sectors and policy areas.

The Romanian system operates primarily through complaint-driven activation, with limited proactive monitoring. As a result, response dynamics are shaped less by detection capacity and more by **legal competences, escalation pathways, and institutional triggers**.

Core inputs in the PREPARE phase - including detection, monitoring, and initial reporting - are largely generated by **civil society organisations, media actors, and public visibility**, while **disruption remains dependent on sector-specific authorities and legal thresholds.**

This creates a system in which effective response depends on **linking externally generated signals to institutional action pathways**, rather than on internally coordinated workflows.

6.1 Sectoral Breakdown of the Response Ecosystem

The Romanian landscape can be understood across 4 core sectors, each contributing distinct capabilities to the framework.

- **Government and regulatory authorities** provide access to key state actors across regulatory enforcement, electoral oversight, cybersecurity, and national security functions. This includes institutions such as ANCOM (Digital Services Coordinator), the National Audiovisual Council (CNA), the Romanian Presidency, and Parliamentary Committees (Culture, Defence, ITC). Their relevance lies primarily in the DISRUPT phase, where legal authority is required for enforcement, platform escalation, or administrative action. However, their operational role is

constrained by mandate-bound competences and reliance on formal complaints, limiting early-stage intervention.

- **Civil society organisations** form the largest and most diverse cohort within the Romanian ecosystem and play a critical role in shaping the PREPARE phase. This group includes investigative journalism initiatives, fact-checking organisations, and human rights groups working on gender equality and minority protection. These actors are often responsible for identifying emerging narratives, documenting influence operations, and generating the evidentiary basis required for disruption. In addition to their analytical role, they also contribute to mitigation through public awareness, advocacy, and engagement with both institutions and platforms.

- **Academic institutions** represent a smaller but strategically important segment of the ecosystem. Focused primarily on public universities with expertise in communication, political science, and media studies, they contribute methodological validation, analytical support, and longer-term capacity building. They play a supporting role across the PREPARE and MITIGATE phases, particularly in strengthening analytical rigour and training.

- **Media and journalism actors** provide both investigative and public-facing functions. The Romanian media landscape includes a combination of state-owned outlets, such as TVR and SRR, and independent platforms, including major online news providers. These actors contribute to verification, exposure and narrative clarification, supporting both the preparation of cases and the mitigation of their impact. By increasing visibility and shaping public understanding, they can also generate indirect pressure that supports disruption where formal enforcement pathways are limited or delayed.

Taken together, these sectors form a functionally interdependent but operationally fragmented ecosystem. Detection, assessment, disruption, and mitigation are distributed across actors rather than coordinated through a single workflow. The current mapping reflects a relatively balanced distribution of stakeholders across sectors, with 13 government and regulatory actors, 14 civil society organisations, 3 academic institutions, and 9 media actors. While this distribution demonstrates the breadth of the network, it also highlights the need for stronger operational workflows between actors.

Preparedness levels vary significantly across institutions and cannot be inferred solely from formal mandates. While some actors maintain regular exposure to platform governance issues, crisis communications, or hostile information activities, others engage with such challenges only during periods of heightened pressure, such as elections or major crises. As a result, institutions with similar legal competences may display markedly different levels of operational readiness. This points to the value of distinguishing between actors with permanent operational responsibilities, those requiring surge capacity during elections or crises, those primarily responsible for communication and referral functions, and those contributing specialised intelligence, technical, legal, or financial expertise.

6.2 Differentiation Within Civil Society

Civil society in Romania is not a single functional actor but a differentiated ecosystem composed of organisations with distinct roles across the Framework.:

- **Investigative and OSINT-focused actors** contribute to uncovering networks, behavioural patterns, and technical infrastructure linked to influence operations.;
- **Fact-checking organisations** focus on verifying and debunking false or misleading narratives;
- **Human rights organisations** provide expertise on vulnerable groups and rights-based impacts, including women and LGBTQIA+ communities;
- **Advocacy and policy organisations** support accountability, institutional engagement and public communication.

This differentiation is particularly important in the Romanian context, where **state-led monitoring capacity is limited and early detection depends heavily on non-state actors**. Civil society organisations therefore play a central role in identifying signals, preserving evidence, translating complex findings into formats that can be used by institutions, media, or platforms and disrupting.

At the same time, this diversity reflects structural fragmentation. Expertise is distributed across multiple organisations, and cooperation with public authorities is not systematically embedded. As a result, while civil society significantly expands national response capacity, its outputs are not consistently integrated into predictable institutional workflows, creating gaps between detection and disruption.

6.3 Regulatory and Institutional Context

The regulatory and institutional context in Romania is defined by strictly mandate-bound intervention and a fragmented distribution of competences. **No single authority connects the PREPARE, DISRUPT, and MITIGATE phases into a continuous operational process**. Instead, institutions act within clearly defined sectoral roles, with **disruption triggered primarily by legal qualification rather than operational urgency**.

- **ANCOM, as the Digital Services Coordinator**, plays a coordination role in relation to the Digital Services Act but does not exercise direct enforcement over content. Its primary function is to escalate cases to platforms or European mechanisms.
- **The National Audiovisual Council** operates within the audiovisual domain and can apply measures based on complaints.
- **Electoral authorities** act during election periods within a specific legal framework.
- **Law enforcement and prosecutorial bodies** intervene when criminal thresholds are met, and the data protection authority addresses violations related to personal data.
- **Security and intelligence actors** operate within national security mandates, and financial investigation bodies address illicit financial flows where relevant.

This institutional configuration results in a system where cases are processed through referrals between authorities, rather than through coordinated or parallel action. Platform engagement is similarly fragmented, with different authorities interacting with platforms independently. In many cases, **disruption measures are limited or indirect, and enforcement depends on the ability to meet specific legal thresholds**.

Another consequence of this institutional configuration concerns the movement of narratives and influence campaigns across jurisdictional and competence boundaries. Certain institutions are primarily responsible for addressing external dimensions of foreign information manipulation, while domestic amplification may fall under separate regulatory, electoral, law-enforcement, or national security competences. In practice, however, contemporary campaigns frequently move across these categories over the course of an operation.

This creates additional coordination challenges within a system that relies heavily on referrals between authorities. As cases move between mandates, questions arise regarding the thresholds that trigger referral, the evidentiary standards required to support transfer, the designation of a lead authority, the scope for parallel action by multiple institutions, and the mechanisms through which feedback is returned to the referring body. The extent to which such procedures are formalised has a direct bearing on the continuity and timeliness of institutional responses, particularly where campaigns evolve rapidly across regulatory and operational domains.

Taken together, these constraints contribute to a response environment in which **mitigation measures, including public communication, awareness-raising, and resilience-building, become the most consistently applied response tools**. While these measures can reduce harm, they do not replace the need for timely and effective disruption.

Table 1: Legal and Regulatory Instruments Relevant to Disruption in Romania

Legal / regulatory instrument	Main disruption relevance	Typical measures enabled	Main competent authority / authorities	Key limitation / operational note
Digital Services Act (DSA)	Platform-related disruption, illegal content handling, notice-and-action procedures, systemic risk escalation	Report Content; Reporting T/S Abuse; DSA Notice & Action Mechanism; Leveraging DSA Systemic Risk Obligations (Article 34–35 Reporting); Digital Service Coordinator Oversight	ANCOM (Digital Services Coordinator); European Commission in relevant cases; platforms	ANCOM mainly performs a coordination and escalation role rather than direct enforcement. Much action depends on platform responsiveness and EU-level procedures.

DSA out-of-court dispute settlement	Review of disputes concerning platform decisions under the DSA	DSA Out-of-court Dispute Settlement	Certified out-of-court dispute settlement bodies; platforms; users	Useful as a redress mechanism but does not typically provide immediate disruption. It is a structured but slower pathway.
DSA Trusted Flagger Mechanism	Faster escalation of certain categories of illegal content through recognised trusted flaggers	Report Illegal Content; Hate Speech; Incitement to Violence; platform escalation through trusted channels	Trusted flaggers, including the Elie Wiesel Institute; platforms; ANCOM in coordination role	Scope depends on the subject matter covered by the trusted flagger and on platform follow-through. It is effective for some categories of illegal content, but not a general anti-disinformation tool.
Romanian DSA implementation framework	National coordination for DSA-related cooperation and liaison with EU structures	Digital Service Coordinator Oversight; forwarding platform-related cases; coordination with EU mechanisms	ANCOM; relevant ministries	The framework reflects a coordination role rather than strong independent enforcement capacity, which limits speed and direct intervention.
Electoral legislation (AEP / BEC framework)	Election-period oversight of political communication, campaign conduct, and certain content-related violations	Election-related reporting; removal orders within electoral context; reporting illegal electoral content; platform escalation during election periods	Permanent Electoral Authority (AEP); Central Electoral Bureau (BEC); constituency electoral bureaus	Relevant mainly during electoral periods. Competences are time-bound and limited to the electoral framework.
Electoral silence period rules	Restriction of political campaigning and certain forms of electoral communication shortly before and during voting	Silence Period enforcement; election-related reporting; platform escalation	AEP; BEC; electoral authorities	Time-sensitive and limited to a narrow electoral window. Not a general counter-influence instrument.

Political advertising transparency legislation	Transparency and labelling obligations for online political campaigning and sponsored electoral content	Political Advertisement Transparency Legislation; escalation of unlabelled political ads; campaign finance scrutiny	BEC; AEP; Constitutional Court in relevant cases	Enforcement remains uneven and often case-specific. It is most relevant during campaigns and where electoral law is engaged.
Foreign finance legislation for political actors	Restriction of foreign funding for political parties and election campaigns	Foreign Finance Legislation; campaign finance scrutiny; electoral escalation	AEP; relevant electoral oversight bodies; prosecutors where offences arise	Applies only where foreign funding or unlawful campaign finance can be demonstrated. Evidence threshold is relatively high.
EU sanctions regime and national implementation	Disruption of activities linked to sanctioned individuals, entities, or financial flows; de-platforming and financial disruption	EU Sanctions for De-Platforming and Financial Disruption; Utilise Existing Sanctions Legislation; financial tracing; asset-freezing related referrals	Ministry of Foreign Affairs; ANAF; ONPCSB / FIU; law enforcement; EU-level mechanisms	Evidence-heavy and often cross-border. Effective action depends on proving links to sanctioned actors and coordinating across financial and governmental channels.
Anti-money laundering legislation (Law no. 129/2019 and related framework)	Financial tracing and enforcement in cases involving suspicious transactions, illicit financing, and sanctions-related financial activity	Freeze Banking Services; Crypto Exchange and Wallet; Payment Provider; financial tracing; suspicious transaction reporting	ONPCSB / FIU Romania; ANAF; prosecutors; financial institutions	Stronger in sanctions and financial cases than in broader influence operations. Capacity constraints remain, especially regarding crypto tracing and real-time financial disruption.
Romanian Criminal Code / national security and foreign interference provisions	Foreign interference, treason, espionage, and activity linked to hostile external actors or threats to national security	Invocation of Foreign Interference Legislation; Collaboration with Foreign Intelligence Services Legislation; criminal investigation; security-service escalation	Romanian Intelligence Service (SRI); DIICOT; Police; Prosecutor's Office	High evidentiary threshold. Used only where national security or foreign actor links can be supported in a legally actionable form.

Criminal law provisions on hate speech / incitement / extremist content	Disruption of hate speech, incitement to violence, extremist propaganda, and related illegal content	Hate Speech; Incitement to Violence; Report Illegal Content; Police reporting; prosecutorial action	Police; Prosecutor's Office; courts; trusted flaggers in platform escalation context	Requires content to cross criminal thresholds. Many influence incidents remain below that threshold and do not trigger rapid intervention.
Law on prevention and combating terrorism (Law no. 535/2004) and terrorist content framework	Removal and prosecution pathways for terrorist content and related online harms	Terrorist Content; Report Illegal Content; removal orders; platform escalation	ANCOM as competent authority for terrorist content online; SRI / anti-terror coordination structures; Police; Prosecutor's Office	Narrow scope, relevant only where content or activity falls within terrorism-related legal definitions.
GDPR and national data protection framework (including Law no. 190/2018)	Data misuse, unlawful profiling, doxxing, impersonation, privacy violations, and manipulation involving unlawfully processed personal data	Privacy & Data Protection Violations; GDPR complaints; Right to be Forgotten; regulatory escalation	ANSPDCP (Data Protection Authority)	Useful where influence activity overlaps with personal data misuse, but not a general anti-disinformation instrument. Effectiveness depends on proving unlawful processing or privacy harm.
Defamation under the Romanian Civil Code	Civil remedy in cases of reputational harm, smear campaigns, or false statements affecting individual rights	Defamation-related civil action; complaint-based legal proceedings	Civil courts; complainants	Defamation is no longer a criminal offence in Romania. It is a civil remedy and not a standard state-led disruption pathway.
Copyright and intellectual property law	Disruption of copied, manipulated, or falsely branded content through IP enforcement	Copyright takedown; Report Copyright Infringement; Intellectual Property Infringement; civil or criminal action	Rights holders; Police economic crime structures; prosecutors; courts; platforms	Narrow applicability. Most useful where protected content is reused without authorisation or where branding is misused.

Audio-visual media legislation / CNA framework	Broadcast and audiovisual regulatory action, including some online audiovisual content	Audio-visual regulatory action; content removal within scope; sanctions for regulated entities	National Audiovisual Council (CNA)	Limited to audiovisual scope, including relevant video-sharing and on-demand services under Romanian jurisdiction. Does not cover all online influence content, especially text-based content.
New Audiovisual Code (Decision no. 573/2025)	Updated oversight of audiovisual and certain digital media practices, including stronger disinformation-related standards within audiovisual regulation	Audio-visual regulatory action; sanctions within CNA competence; platform and broadcaster oversight within scope	CNA	Useful where content falls within the audiovisual regulatory perimeter, but not a general-purpose anti-IO instrument.
AI-generated / altered content labelling framework (PL-x No. 471/2023, if enacted / applied)	Labelling and regulatory response to deceptive AI-generated or altered audio-visual content	AI labelling enforcement; escalation to CNA; administrative sanctions	CNA; potentially prosecutors in relevant cases	Primarily relevant to deepfakes and manipulated audio-visual content. Scope and operational impact depend on implementation and enforcement practice.
EU AI Act	Potential future relevance where AI systems generate harmful or deceptive content affecting fundamental rights or regulated sectors	Regulatory escalation relating to AI-enabled harms; coordination with competent authorities	Competent authorities still being designated / sector-specific bodies	Not yet a primary rapid-response disruption tool in practice. More relevant as an emerging regulatory framework than an immediate operational pathway.
EMFA-related framework	Media governance, pluralism, and regulatory coordination in the media environment	Regulatory escalation; institutional coordination in media sector	Ministry of Culture; CNA; ANCOM; Parliament	More relevant to structural media governance than to rapid case disruption.

Consumer protection law	Potential disruption of misleading commercial claims, scam content, or deceptive monetised narratives	Regulatory complaints; consumer protection escalation	National Authority for Consumer Protection and other relevant regulators	Limited relevance to broader influence operations, but can be useful where manipulation overlaps with deceptive commercial conduct.

A key operational challenge in Romania is that these instruments are distributed across multiple legal domains and authorities, with significant variation in threshold, speed, and operational usability. In practice, disruption is rarely based on a single law specifically aimed at information manipulation. Instead, effective action depends on matching the case to the most appropriate available pathway, whether criminal law, sanctions implementation, electoral law, platform regulation, financial intelligence, data protection, or audiovisual regulation, while recognising that many pathways remain conditional on legal qualification rather than operational urgency.

6.4 Cross-Sector Interaction Across the Framework

Across the three phases of the Framework, interaction between sectors reflects the broader structural characteristics of the Romanian system.
This distribution of roles highlights the absence of a continuous operational workflow linking phases together. Instead, each phase is activated independently, depending on the nature of the case and the competence of the actors involved.

6.4.1 PREPARE

In Romania, PREPARE-phase activities remain significantly dependent on externally generated signals, including civil society monitoring, media investigations, citizen complaints, and international alerts. Institutional monitoring capacity exists in some areas, but is unevenly distributed across the ecosystem. Measures such as detection, initial reporting, narrative identification, and evidence collection are therefore often initiated outside government structures, with public authorities typically engaging once a case has been formally submitted or has reached a level of visibility that triggers review within their mandate.

The objective at this stage is to move from **public signal or complaint to incident qualification within sectoral competence**. However, because detection capacity is not institutionalised and inputs are not consolidated through a shared mechanism, early-stage coordination remains **reactive and fragmented rather than structured and analytical**. This results in delayed assessment, particularly in cases of coordinated inauthentic behaviour, where identification requires sustained monitoring and technical capability that are unevenly distributed across actors.

Preparedness at this stage depends not only on the availability of analytical tools, but also on the presence of dedicated personnel able to operate them continuously, interpret findings, and translate raw signals into actionable cases. Where monitoring capabilities are not matched by sufficient staffing and analytical capacity, the practical impact of available tools may be limited. As a result, readiness varies considerably between organisations even where access to technical resources appears comparable.

6.4.2 DISRUPT

In Romania, the DISRUPT phase is led by sector-specific authorities acting within their legal competences, depending on how an influence operation is qualified. This can include regulatory bodies such as ANCOM and the National Audiovisual Council, electoral authorities during campaign periods, law enforcement and prosecutors in cases involving criminal conduct, financial investigation bodies in sanctions-related cases, and data protection authorities where personal data violations are involved. Measures typically include referral or escalation to platforms, issuance of administrative decisions within sectoral mandates, initiation of legal or investigative procedures, or coordination with European mechanisms under the Digital Services Act.

In practice, this phase is constrained by the fact that most authorities do not exercise direct disruption powers and rely on escalation or referral mechanisms rather than immediate intervention. ANCOM, for example, primarily forwards cases to platforms or EU structures, while other institutions act only when a case clearly falls within their specific legal remit. As a result, many influence operations do not reach the threshold required for action, particularly in cases of coordinated inauthentic behaviour that do not constitute a clear legal violation.

Disruption capacity also varies according to platform, content type, and timing. Platform responsiveness is not uniform, with some services responding more rapidly during periods of heightened scrutiny, such as elections, while others follow longer or more procedural review processes. Operational constraints can further affect the speed and scale of intervention, particularly where reporting and escalation mechanisms rely on manual processes and large numbers of accounts, pages, or pieces of content require simultaneous assessment. As a result, the effectiveness of disruption measures is influenced not only by legal competences, but also by the practical capacity of institutions to prepare, document, and escalate cases in a timely manner.

This creates a structural gap between PREPARE and DISRUPT, where cases may be identified but not acted upon in a timely or coordinated manner. The transition between phases therefore remains dependent on legal qualification rather than operational urgency, leading to possible delays, sequential handling of incidents across institutions, and limited use of parallel disruption measures.

6.4.3 MITIGATE

MITIGATE-phase measures are primarily communication- and awareness-based, led by public authorities, government communication structures, and supported by civil society and media actors. Measures include public clarification, awareness campaigns, contextualisation of incidents, and resilience-focused messaging, particularly in cases where influence operations have already reached

a level of public visibility. Institutions such as the **Ministry of Foreign Affairs** and other public bodies play a central role in shaping official narratives and providing explanations, while civil society and media contribute to amplification, fact-checking, and public engagement.

The objective at this stage is to **reduce the impact of influence operations by clarifying information, correcting narratives, and reinforcing public understanding**. Mitigation is particularly relevant for sectoral ministries whose policy areas may become targets of panic narratives, false alerts, manipulated statistics, or conspiracy claims. This is especially relevant in sectors such as health, energy, environment, agriculture, and critical infrastructure, where public trust and behavioural responses can have direct policy consequences. In such contexts, the effectiveness of mitigation efforts often depends on the timely provision of clear information, the visibility of credible subject-matter expertise, and the consistency of messaging across institutions.

However, because mitigation is often triggered only after incidents become publicly visible, it tends to function as a reactive response rather than as part of a coordinated operational workflow. In the absence of strong disruption mechanisms, mitigation frequently becomes the primary response tool, placing greater emphasis on communication rather than intervention. As a result, **while mitigation can reduce harm, it does not address the underlying operational drivers of influence activities and is rarely integrated with earlier-phase actions in a structured manner**.

6.5 Fragmentation and Coordination

Both the institutional and non-governmental response landscape in Romania are structurally fragmented. Responsibilities are distributed across multiple authorities with clearly defined sectoral mandates, while detection, reporting, and initial analysis are largely generated by civil society, media, and public visibility. However, the mechanisms linking these inputs to institutional action remain weakly formalised and primarily dependent on complaint-driven processes. Several recurrent coordination gaps are identified:

- no shared incident definition across institutions, leading to inconsistent case qualification;
- no common escalation threshold to trigger cross-sector involvement;
- no predefined workflow between authorities;
- absence of standard referral procedures, including common evidence requirements and case-transfer formats;
- inconsistent feedback loops following referrals, limiting institutional learning and case visibility across the system;
- varying levels of institutional readiness and specialist analytical capacity across ministries and agencies;
- limited capacity for simultaneous multi-platform response during high-volume incidents;
- uneven familiarity with Digital Services Act procedures and platform escalation mechanisms across institutions;
- no structured transition from disruption to mitigation when intervention is delayed or not feasible;

This fragmentation does not indicate a lack of institutional actors or mandates. Romania has a diverse ecosystem covering regulatory oversight, electoral processes, financial investigation, data protection, and national security. However, these capacities operate within a **mandate-bound and reactive governance model**, where intervention is typically triggered only once a complaint is received or a legal threshold is met. As a result, cases are often passed from one institution to another instead of being handled together. Early-stage influence operations are usually not addressed, and the ability to disrupt them is limited. This means that responses tend to focus on communication and public awareness once the issue becomes visible, rather than on timely and coordinated action to stop it earlier.

The Framework helps address this by introducing a shared operational logic. Rather than replacing institutional mandates, it clarifies how distributed capacities can be connected through common decision points and parallel pathways by:

- structuring how measures are sequenced;
- clarifying which actors contribute at each stage;
- enabling parallel deployment of measures;
- linking external detection to institutional pathways.

Effectiveness depends on coordination across fragmentation, not its removal.

6.6 Operational Implication

In Romania,

- **PREPARE measures** are largely **externally driven**, relying on civil society, media, and public complaints rather than institutional monitoring, with limited analytical capacity within state actors.
- **DISRUPT measures** are **limited and mandate-bound**, with most authorities relying on referrals, platform escalation, or legal thresholds, rather than direct and timely intervention.
- **MITIGATE measures** are **the most consistently applied**, particularly through public communication, awareness-raising, and resilience-focused responses once incidents become visible.

At the same time, the system contains **all necessary functional components** for an effective response. The primary challenge lies in connecting these components through:

- shared escalation triggers;
- clearer workflows;
- both parallel and sequential deployment of measures.

7. Current Operational Pattern in Romania

Consultation findings indicate that the response to influence operations in Romania develops through a **complaint-driven, mandate-bound process**, rather than through a unified or linear operational workflow. While a range of activities exist across the PREPARE, DISRUPT, and MITIGATE phases, these are not consistently connected through shared sequencing or coordination mechanisms. Instead, actions are triggered primarily by **formal complaints, public visibility, and legal competences**, rather than by a coordinated lifecycle approach.

In practice, detection, assessment, disruption, and communication are carried out by different actors operating within their own mandates. Civil society, media, and citizens play a central role in identifying and reporting incidents, while public authorities assess and act only within their specific legal domains. The transition between phases depends on whether a case meets the relevant legal or administrative threshold. Where this qualification is unclear or not met, cases may be delayed, referred across institutions, or move directly into mitigation measures, particularly through communication and awareness responses.

Table 2. Observed workflow pat

Phase	Step	Examples of Measures	Output
PREPARE	Data Collection & Documentation	Social Listening; Narrative Monitoring; Find and Collect Publicly Available Content; Scraping; Monitoring by civil society and media actors; Inputs submitted to authorities (e.g. CNA, ANCOM)	Initial signal detection and documented observations
PREPARE	Analysis & Assessment	Document; Create Evidence Repository; Actor Mapping; Identify Pattern of Behaviour; CIB identification (limited, non-centralised); Attribution (where possible); Legality assessment by competent authority	Analytical and legal qualification of the case
PREPARE → DISRUPT	Inform	Send Alert; Submit Complaint; Send Email; Briefing; Forwarding to relevant authority or platform (e.g. ANCOM, CNA, electoral bodies)	Case routed to competent authority or platform
DISRUPT	Competence Qualification	Determining whether the case fits criminal, administrative, electoral, data protection, or platform pathway (e.g. police/prosecutor, CNA, ANSPDCP)	Decision on whether disruption is possible
DISRUPT	Enforcement / Action	Report Content; Report Channel; Platform engagement (often via ANCOM or CNA); Criminal investigation (Police / Prosecutor); Financial investigation; GDPR enforcement; Referral to EU mechanisms under DSA	Referral, platform response, or legal/administrative action
MITIGATE	Communication Actions	Public communication; Media exposure; Fact-checking; Narrative clarification; Awareness campaigns; Government messaging (ministries, MFA, public institutions)	Public response and impact mitigation

8. Standard National Workflow

The following workflow reflects a structured application of the framework within existing mandates.

Standard National Workflow
STEP 1. DATA COLLECTION & DOCUMENTATION A potential case is identified through monitoring, international cooperation, or institutional awareness.
STEP 2. ANALYSIS & ASSESSMENT Relevant actors assess context, relevance, and available information.
STEP 3. INFORM Once sufficient confidence is reached, the case is routed to the appropriate authority or authorities. **IMPORTANT: MULTI AGENCY TRIAGE** Where multiple mandates may apply, relevant institutions clarify responsibilities, identify applicable legal pathways, and determine whether parallel action is possible.
STEP 4. DISRUPTION Where applicable, multiple response tracks are activated simultaneously within their respective mandates. **IMPORTANT: PLATFORM / EXTERNAL ENGAGEMENT** Where relevant, platforms, service providers, financial actors, or European mechanisms are engaged through established escalation and cooperation channels. When needed, legal actions are taken.
STEP 5. MITIGATION If disruption is limited or delayed, communication and awareness measures are activated. **IMPORTANT: PUBLIC COMMUNICATION COORDINATION** Where public communication is required, institutions align factual messaging, timing, and communication responsibilities.
STEP 6. CASE CLOSURE After stabilisation, the case is documented and reviewed.

This workflow reflects the Framework's central logic: moving from detection to assessment and then to proportionate intervention through a structured sequence of measures and workflows.

9. Application to Coordinated Inauthentic Behaviour

Coordinated inauthentic behaviour presents a specific operational challenge in Romania due to the **limited availability of proactive monitoring, the absence of centralised analytical capability, and the reliance on complaint-driven processes**. Unlike other types of influence operations that may be linked to clearly defined legal violations, CIB often operates in a grey zone, where coordinated activity is difficult to detect, evidence is fragmented, and legal qualification is uncertain.

Many disruption pathways depend on:

- platform responsiveness and willingness to act on reported CIB;
- the ability to attribute activity to foreign, coordinated, or sanctioned actors;
- whether the case meets legal, regulatory, or policy thresholds for intervention.

As a result, the application of the DISRUPT Framework to CIB cases highlights structural constraints across all three phases, particularly in the transition from PREPARE to DISRUPT.

The table below illustrates how the DISRUPT Framework is operationalised in Romania for CIB-type cases.

Table 3. CIB workflow overview

Phase	What this typically involves in Romania	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge primarily through civil society monitoring, media reporting, and public complaints, rather than systematic institutional detection. Activities such as social listening, narrative monitoring, account tracking, behavioural monitoring, and collection of publicly available content are conducted in a distributed and non-centralised way. Cases are documented through observable lists and archiving, while initial patterns and network characteristics may be identified. In Romania, this phase is not institutionally centralised and relies heavily on civil society organisations, investigative journalists, and external reporting, with limited proactive involvement from state actors.	Preserve evidence, document coordinated behaviour in a structured way, and build a defensible record of channels, accounts, content, and patterns before assets are removed or changed.	1.1 Find and Collect Publicly Available Content, 1.2 Narrative Monitoring, 1.3 Account Monitoring, 1.4 Behavioural Monitoring, 2.1 Observable list, 2.2 Offline Archiving, 2.3 Online Archiving, 2.4 Hash Evidence
PREPARE → DISRUPT	The case is assessed based on whether behaviour appears coordinated, whether it causes	Determine whether the case meets thresholds for action and identify	3.1 CIB Detection Tree, 3.2 CIB Algorithm, 3.3 Analyse Content, 3.4 Identify links

	harm, and whether it can be linked to a specific legal or regulatory violation within institutional mandates. Attribution and infrastructure mapping are often limited, and escalation depends on whether a competent authority (e.g. CNA, ANCOM, ANSPDCP, electoral bodies, or law enforcement) can act within its remit. In Romania, this stage is constrained by the absence of shared thresholds and reliance on legal qualification, meaning that many cases of coordinated behaviour do not progress to action.	viable escalation routes, particularly through platform reporting, regulatory bodies, or legal pathways, where applicable.	between actor and threat actor, 3.5 Identify Infrastructure, 3.5 Behaviour Analysis (DISARM), 4.1 Inauthentic Behaviour, 4.2 Legality, 4.3 Attribution, 4.4 Harm, 4.5 Imminent Risk, 4.6 Foreign Interference
DISRUPT	Action is taken depending on available platform, legal, regulatory, and administrative pathways, rather than through direct technical or coordinated institutional disruption. This includes platform reporting, escalation via ANCOM under the DSA framework, actions by CNA within audiovisual scope, GDPR-related measures by ANSPDCP, and criminal investigation where thresholds are met. In Romania, disruption is often indirect and dependent on platform responsiveness or legal qualification, with limited capacity for independent infrastructure or network-level intervention.	Use available disruption measures without assuming that formal enforcement will be possible or timely. Focus on platform escalation, regulatory engagement, and legal pathways, while recognising constraints in direct disruption capacity.	6.1 Hosting, 6.2 Domain, 6.3 Revoke SSL certificates, 6.4 Content Delivery Network, 6.5 Web Application Firewall, 7.1 Report Content, 7.2 Report Channel, 7.3 Report Coordinated Inauthentic Behaviour, 7.4 Contact Platform Representatives, 7.5 CoC Rapid Response System, 7.6 Advertising, 8.1 Demonetise Operation Assets, 8.2 Investor, 9.1 DSA, 9.2 EU Sanctions for De-Platforming and Financial Disruption, 9.3 Invocation of Foreign Interference Legislation, 9.4 Defamation, 9.5 Silence Period, 9.6 Political Advertisement Transparency Legislation, 10.1 Counter FIMI Agency, 10.2 Ministry of Foreign Affairs, 10.3 Security Services, 10.4 Interior Ministry, 10.6 Prosecutor
MITIGATE	Where disruption is delayed, not feasible, or dependent on platform action, communication and awareness measures become the primary response. This includes media reporting, fact-checking, public clarification, government messaging, and awareness campaigns led by public institutions, civil society, and media actors.	Strengthen public resilience, explain manipulation techniques, and increase awareness, while maintaining pressure on platforms and institutions to act.	5.1 Publish Report, 5.2 Send Alert, 5.3 Send Email, 5.4 Briefing, 11.1 Engage Political Actor, 11.2 Engage Advocacy Actors, 11.3 Engage Journalist, 12.1 Media Exposure

	In Romania, mitigation is consistently applied and often becomes the dominant response, particularly once incidents reach public visibility.		

The application of the DISRUPT Framework to CIB in Romania demonstrates that the primary limitation lies not in the absence of relevant actors, but in the **lack of shared operational triggers and analytical capacity to move from detection to action**. The system is able to observe and communicate about coordinated activity, but struggles to qualify and disrupt it in a timely and consistent manner.

This results in a response model where CIB is **more likely to be mitigated than disrupted**, with intervention occurring after public visibility rather than during the early stages of the operation. Strengthening this pathway would require clearer definitions, improved analytical capacity, and more structured escalation mechanisms linking detection to institutional action.

11. Application to Sanctions-Related Cases

Sanctions-related influence operations in Romania represent a category of cases where **legal frameworks are more clearly applicable than in other types of information manipulation**. Unlike coordinated inauthentic behaviour, sanctions circumvention involves financial flows, ownership structures, or content linked to sanctioned entities, which can fall under EU sanctions regimes and national enforcement mechanisms. This creates **stronger legal grounds for disruption**, but operationalisation remains complex, evidence-heavy, and often dependent on cross-border coordination.

The Romanian ecosystem demonstrates **more structured pathways for handling sanctions-related cases** than for other types of influence operations, particularly through financial investigation bodies such as the AML Office and ANAF, as well as law enforcement and prosecutorial authorities. Detection typically relies on identifying suspicious financial activity, tracing ownership and control structures, and establishing links between entities and sanctioned actors. This requires structured evidence collection, including documentation of financial flows, corporate linkages, and transactional patterns, often supported by investigative reporting and external analysis.

The transition from detection to disruption is **more actionable than in CIB cases**, but still dependent on several key factors:

- the ability to demonstrate a link between activity and a sanctioned individual or entity;
- the availability of sufficient financial and legal evidence to meet enforcement thresholds;
- coordination with competent national authorities and, where required, EU-level mechanisms;
- the involvement of financial institutions, service providers, and platforms in enforcing restrictions.

Disruption pathways in sanctions cases are broader and more legally grounded than in other types of influence operations. They include:

- financial investigation and enforcement measures led by competent authorities;
- reporting sanctioned entities, content, or financial activity to platforms and service providers;
- targeting financial and technical infrastructure, including payment systems and intermediary actors;
- invoking EU sanctions frameworks and related regulatory instruments;
- escalation to government actors, including ministries, financial intelligence units, and security services.

In the Romanian context, **government and enforcement actors play a central role** in disruption. Institutions responsible for financial investigation, law enforcement, and national security contribute to evidence gathering, enforcement, and escalation. However, as highlighted in the consultation findings, coordination across institutions remains **mandate-bound and case-specific**, and escalation pathways are not always clearly defined or consistently applied.

Despite stronger legal grounding, disruption is not always immediate. Many measures - particularly those involving financial enforcement, legal proceedings, or EU-level coordination - require **significant evidence and extended timeframes**. As a result, mitigation through communication and exposure remains an important complementary approach. Media reporting, civil society engagement, and public communication are often used to increase visibility and apply pressure on institutions and service providers, particularly where formal enforcement is delayed.

Overall, sanctions-related cases in Romania demonstrate a **more structured and enforceable disruption environment compared to CIB**, but effectiveness remains dependent on legal qualification, institutional coordination, and the ability to translate analytical findings into actionable evidence within existing frameworks.

The table below illustrates how the DISRUPT Framework is operationalised in Romania for sanctions-related cases.

Table 4. Sanctions workflow overview

Phase	What this typically involves in Romania	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through financial irregularities, investigative reporting, civil society inputs, and institutional referrals, rather than proactive monitoring. Activities include collection of publicly available information, identification of ownership structures, tracking financial flows, and mapping links between individuals, entities, and sanctioned actors. Documentation is developed through evidence repositories, archiving, and	Preserve evidence, map financial and organisational structures, and document links between actors, assets, and potential sanctions exposure.	1.1 Find and Collect Publicly Available Content, 1.2 Narrative Monitoring, 1.3 Account Monitoring, 1.4 Behavioural Monitoring, 2.1 Observable list, 2.2 Offline Archiving, 2.3 Online Archiving, 2.4 Hash Evidence

	structured analysis of networks and transactions. In Romania, this phase relies on financial investigation bodies (e.g. AML Office, ANAF), civil society, and media, with limited systematic detection across institutions.		
PREPARE → DISRUPT	The case is assessed to determine whether financial activity is linked to sanctioned individuals, entities, or prohibited transactions, and whether legal thresholds are met. This includes identifying ownership, control structures, financial flows, and jurisdictional links. In Romania, escalation depends on whether the case can be qualified within financial, criminal, or EU sanctions frameworks, often requiring a high evidentiary threshold and coordination with EU-level mechanisms.	Determine whether the case meets legal thresholds for sanctions-related action and identify viable escalation routes, particularly through financial investigation, regulatory, or prosecutorial pathways.	3.1 CIB Detection Tree, 3.2 CIB Algorithm, 3.3 Analyse Content, 3.4 Identify links between actor and threat actor, 3.5 Identify Infrastructure, 3.5 Behaviour Analysis (DISARM), 4.1 Inauthentic Behaviour, 4.2 Legality, 4.3 Attribution, 4.4 Harm, 4.5 Imminent Risk, 4.6 Foreign Interference
DISRUPT	Action is taken through financial enforcement, regulatory measures, and legal proceedings, rather than platform-based disruption alone. This includes financial tracing and investigation (AML Office, ANAF), criminal investigation (police/prosecutor), and coordination with EU sanctions mechanisms. Where relevant, platform-related actions may complement financial measures. In Romania, disruption is more structured than in CIB cases but remains evidence-heavy and dependent on legal qualification, often requiring cross-border coordination.	Apply financial, legal, and regulatory measures to restrict or disrupt sanctioned activity, while coordinating with EU-level mechanisms where required. Combine financial investigation, legal enforcement, and institutional escalation where possible.	6.1 Hosting, 6.2 Domain, 6.3 Revoke SSL certificates, 6.4 Content Delivery Network, 6.5 Web Application Firewall, 7.1 Report Content, 7.2 Report Channel, 7.3 Report Coordinated Inauthentic Behaviour, 7.4 Contact Platform Representatives, 7.5 CoC Rapid Response System, 7.6 Advertising, 8.1 Demonetise Operation Assets, 8.2 Investor, 9.1 DSA, 9.2 EU Sanctions for De-Platforming and Financial Disruption, 9.3 Invocation of Foreign Interference Legislation, 9.4 Defamation, 9.5 Silence Period, 9.6 Political Advertisement Transparency Legislation, 10.1 Counter FIMI Agency, 10.2 Ministry of Foreign

			Affairs, 10.3 Security Services, 10.4 Interior Ministry, 10.6 Prosecutor
MITIGATE	Where enforcement is ongoing or delayed, communication and awareness measures are used to explain sanctions implications, expose networks, and reinforce compliance expectations. This includes public reporting, media exposure, and institutional communication. In Romania, mitigation supports enforcement by increasing visibility and reinforcing legitimacy, particularly in complex or cross-border cases.	Reinforce awareness of sanctions regimes, expose non-compliant behaviour, and support enforcement through public communication and transparency.	5.1 Publish Report, 5.2 Send Alert, 5.3 Send Email, 5.4 Briefing, 11.1 Engage Political Actor, 11.2 Engage Advocacy Actors, 11.3 Engage Journalist, 12.1 Media Exposure

12. Minimum Operational Readiness

To apply the Toolkit effectively in Romania, institutions and practitioners should ensure the availability of basic coordination capabilities, alongside clearly defined actions that operationalise them within the existing, distributed response ecosystem.

In the Romanian context, minimum operational readiness is particularly important because relevant capabilities already exist across public authorities, financial investigation bodies, regulators, law enforcement, and civil society actors, but they are not consistently connected through shared triggers or predefined workflows. As highlighted in the consultation findings, the system operates primarily through complaint-driven activation and mandate-bound intervention, which limits early-stage coordination and timely disruption.

Readiness therefore depends not only on institutional capacity in isolation, but on the ability to receive and recognise signals, document cases in a structured way, route them efficiently to the competent authority, and coordinate actions across mandates. It also requires the ability to activate communication and mitigation measures where disruption is delayed, not feasible, or dependent on external actors such as platforms or EU-level mechanisms.

Table 5. Minimum Readiness Capability

Capability	Description	Operational actions (what actors can do)
Signal intake	Mechanism for receiving and reviewing alerts	Receive signals primarily through complaints, civil society organisations, media reporting, citizens, or institutional referrals; review incoming cases within institutional mandates (e.g. CNA, ANCOM, ANSPDCP, electoral bodies); prioritise based on risk factors such as elections, public harm, sanctions relevance, foreign interference, or

		national security implications; acknowledge receipt and initiate initial assessment.
Specialist staffing	Availability of trained analytical, legal, investigative, and communications personnel able to sustain case handling.	Assign staff responsible for monitoring, case assessment, evidence review, legal qualification, platform engagement, and public communication; ensure continuity of operations during prolonged incidents; maintain institutional knowledge and analytical expertise; support effective use of available tools and monitoring capabilities.
Case tracking	Basic documentation of cases	Open a case file within the competent authority; record key information such as source, content, actor, platform, timeline, and potential legal relevance; update case status; maintain an evidence repository; document referrals and transfers between institutions as cases move across mandates.
Routing clarity	Understanding of institutional competences	Identify the competent authority depending on case type, for example CNA for audiovisual content, ANCOM for DSA-related escalation, ANSPDCP for data protection issues, electoral authorities (AEP/BEC) for election-related cases, police/prosecutor for criminal thresholds, financial investigation bodies (AML Office, ANAF) for sanctions-related cases, or security services for national security concerns; route cases accordingly and clarify responsibilities early.
Evidence standards	Consistent approach to documentation	Collect and preserve evidence, including screenshots, URLs, metadata, archived content, and platform identifiers; document financial or ownership links where relevant; apply structured documentation so evidence can support platform reporting, legal proceedings, financial enforcement, or escalation to national or EU-level mechanisms.
Platform readiness	Understanding of platform reporting channels, escalation pathways, and evidence requirements.	Maintain current knowledge of platform procedures; identify relevant reporting and escalation mechanisms; prepare documentation in formats accepted by platforms; engage Digital Services Act pathways where applicable; coordinate with national and European counterparts when escalation is required.
Coordination channels	Ability to engage relevant actors	Contact relevant stakeholders, including regulators, law enforcement, financial investigation bodies, platforms, civil society organisations, and media; share information securely; coordinate referrals between institutions; align actions where possible (e.g. platform reporting alongside legal or regulatory steps), despite mandate-bound constraints.
Inter-agency feedback	Mechanisms for tracking referrals and communicating outcomes between institutions.	Confirm receipt of referred cases; provide updates on status and actions taken; communicate outcomes to referring organisations where appropriate; support institutional learning by ensuring visibility of case progression across mandates.

Communication capacity	Preparedness for public messaging	Prepare public communication, clarifications, alerts, and briefings; determine when communication should remain internal and when public messaging is required; engage ministries, public institutions, media, and civil society actors; ensure messaging is timely and consistent, particularly when mitigation becomes necessary due to limited disruption options.
Surge capacity	Ability to manage sudden increases in incident volume during elections, crises, or major public events.	Prioritise cases according to risk and impact; reallocate staff and resources during high-demand periods; activate temporary coordination arrangements; manage large volumes of complaints, referrals, or reporting requests without disrupting routine operations.
Learning mechanisms	Ability to capture lessons learned	Conduct post-case reviews within institutions; identify gaps in coordination, escalation, and response; update internal procedures; where possible, share lessons across institutions and with external partners; support gradual development of more structured coordination practices.

These elements support the Framework's role as a coordination standard and operational reference. In Romania, they are particularly important because the main operational challenge is not the absence of relevant actors, but the absence of consistent sequencing between them. Minimum readiness therefore means ensuring that existing capacities can be connected quickly enough to support timely and proportionate action across the lifecycle of influence operations.

13. Conclusion

The application of the DISRUPT Framework in Romania demonstrates that the country possesses a broad but unevenly connected ecosystem for addressing influence operations, including CIB and sanctions-related activities. Relevant actors exist across public authorities, financial investigation bodies, regulators, law enforcement, civil society, and media. However, analytical capacity and proactive monitoring remain limited within state institutions, and detection is largely driven by civil society, media reporting, and public complaints, rather than systematic institutional processes.

The primary challenge is therefore not only disruption, but also the **early identification and structured assessment of cases**, as well as the consistent translation of signals into timely and effective action. In many cases, response pathways depend on whether an incident can be qualified within a specific legal mandate, or on escalation to platforms and EU-level mechanisms. This creates a gap between **public signal, institutional assessment, and operational response**, particularly in cases such as CIB, where activities often fall below clear legal thresholds.

Sanctions-related cases demonstrate a more structured and enforceable pathway, as they benefit from clearer legal grounding under EU frameworks and established financial investigation mechanisms. These cases enable a broader range of disruption measures, including financial enforcement, legal action, and regulatory intervention. However, effective disruption remains

dependent on evidence thresholds, inter-institutional coordination, and the ability to link financial activity to sanctioned entities, often requiring cross-border cooperation.

Across both case types, the findings point to a structural issue: Romania has a wide range of relevant actors and mandates, but these are not consistently connected through **shared operational triggers, predefined escalation pathways, or coordinated workflows**. As a result, responses are often complaint-driven, sequential, and reactive, with mitigation—particularly through communication and awareness—frequently becoming the most visible response once incidents reach public attention.

The DISRUPT Framework addresses this gap by providing a common structure for organising actions across the full lifecycle of an influence operation—from detection and assessment to disruption and mitigation. Its value in the Romanian context lies not in introducing new mandates, but in **connecting existing actors, clarifying when and how they engage, and enabling more predictable coordination across phases**.

The findings suggest that Romania's principal challenge is increasingly one of operational standardisation rather than institutional absence. Relevant actors, legal mandates, and response pathways are already present across the ecosystem. However, their effectiveness is constrained by inconsistent coordination practices, varying levels of operational readiness, uneven analytical capacity, and limited integration between detection, disruption, and mitigation activities. As a result, the effectiveness of the overall system depends less on the creation of new structures than on the ability of existing actors to function as a connected operational network through clear handovers, predictable workflows, effective platform engagement, and coordinated communication practices.

Strengthening operational readiness in Romania will therefore depend on:

- improving clarity on institutional roles and competence-based routing;
- establishing shared escalation triggers and more predictable coordination mechanisms across institutions;
- strengthening analytical capacity and evidence collection to support legal and regulatory action;
- reinforcing communication and mitigation strategies where disruption is delayed, limited, or dependent on external actors.

By embedding these elements, the Framework can support Romania in moving from a **reactive, complaint-driven system toward a more structured and coordinated operational response**.

Annex 1: Minimum Questions for Initial Case Handling

When receiving a potential influence-operation case, institutions should consider the following questions:

Annex 2: Overview of the DISRUPT Framework in Romania

Phase	Function	Measure	Sub-measures
PREPARE	Data Collection and Documentation	Information Collection	Find and Collect Publicly Available Content; Social Listening; Scraping; Threat Intelligence Monitoring Tool; Agent-based Crawling; Gain Proprietary Intelligence / Infiltration; Purchase Data; Interview; Freedom of Information Request
PREPARE	Data Collection and Documentation	Document	Observable List; Create Evidence Repository; Offline Archiving; Online Archiving; Screenshots; Hash Evidence
PREPARE	Data Collection and Documentation	Monitoring	Monitor and Track Operation Activity; Narrative Monitoring; Account Monitoring; Behavioural Monitoring; Crowdsourced Monitoring
PREPARE	Analysis and Assessment	Analyse	CIB Detection; Manual CIB Detection; CIB Algorithm; Actor Mapping; Analyse Content; Identify Deepfake; Identify AI-rewritten Content; Identify Identical Content; Identify Source of Content; Identify Illegal Content
PREPARE	Analysis and Assessment	Assessment	Inauthentic Behaviour; Legality; Attribution; Imminent Risk; Foreign Interference; Identify Links Between Actor and Threat Actor; Identify Funding; Identify Ownership Structure (UBO); Identify Personnel Affiliations; Identify Partnerships, Clients, and Service Providers; Identify Amplification; Identify Pattern of Behaviour; Check Sanctions Status
PREPARE	Analysis and Assessment	Infrastructure Analysis	Identify Infrastructure; Domain Analysis; URL Analysis; IP Analysis; Software Components Analysis; Services; Identify AI Generation Tool; Fact-check; Behaviour Analysis (DISARM)
DISRUPT	Inform	Inform	Publish Report; Send Alert; Send Email; Briefing; Policy Briefs
DISRUPT	Report Through Established Mechanisms	Cyber Infrastructure	Hosting; Copyright Takedown; Reporting T/S Abuse; DSA Notice & Action Mechanism; Domain; Fraudulent Registration Information; Domain Sanctions Violations; Website Components; Revoke SSL Certificates; Content Delivery Network; Web Application Firewall; Remove Search Engine Results; The Right to be Forgotten
DISRUPT	Report Through Established Mechanisms	Social Media Companies	Report Content; Incitement to Violence; Hate Speech; Terrorist Content; Intellectual Property Infringement; Privacy & Data Protection Violations; Defamation; Sanctioned Content; Report Channel; Sanctioned Actor; Report as Spam; Impersonation; Report Illegal Content; Report Coordinated Inauthentic Behaviour; Report Copyright Infringement; Direct Platform Engagement; Contact Platform Representatives; CoC Rapid Response System; Unlabelled Political Ads; Advertising; Monetisation

DISRUPT	Report Through Established Mechanisms	Financial Actions	Demonetise Operation Assets; Ad Network; Ad Buyer; Investor; Financial Services; Freeze Banking Services; Financial Intelligence Units; Payment Provider; Crypto Exchange and Wallet
DISRUPT	Report Through Established Mechanisms	Regulatory Action	DSA; DSA Out-of-court Dispute Settlement; Leveraging DSA Systemic Risk Obligations (Article 34–35 Reporting); DSA Trusted Flagger Mechanism; Digital Service Coordinator Oversight; EU Sanctions for De-Platforming and Financial Disruption; Propose New Sanctions; Utilise Existing Sanctions Legislation; Invocation of Foreign Interference Legislation; Foreign Finance Legislation; Collaboration with Foreign Intelligence Services Legislation; Foreign Agent Legislation; Silence Period; Political Advertisement Transparency Legislation; GDPR; Defamation; Intellectual Property Infringement; Terrorism Laws
DISRUPT	Government Engagement	Government Collaboration	Ministry of Foreign Affairs; Security Services; Interior Ministry; Audio-Visual Regulator; Prosecutor; Police; Military; Electoral Authorities; Digital Service Coordinator; EU Institutions; National Institutes for Cyber Security; Ombudsman Office; Data Protection Regulator; Consumer Protection Regulator; Chancellery of the Prime Minister
DISRUPT	Pressure	Public Pressure	Engage Political Actor; Engage MEP; Engage MP; Engage Political Party; Engage Council / Minister; Engage Advocacy Actors; Engage Advocacy Network; Engage Activist Group; Engage Public; Engage Private Sector; Engage Interest Group; Engage Company; Engage Journalist; Written Question to Institutions (Officially); Open Letter; Civil Society Joint Letter; Online Petition; Media Exposure; Name and Shame; Behavioural Exposure; Expose Actor and Intentions; Expose Affiliations
MITIGATE	Communication Actions	Communication Actions	Publish Fact-check; Policy Briefs; Pre-bunking; Narrative Inoculation; Community Outreach; Work with Religious Leaders; Community Leaders; Employers / Unions; Footwork; Engage Public; Public Education on Manipulation Techniques; Influencer Partnerships; Youth-focused Messaging; Flood the Information Space with Positive Narratives