DISRUPT FRAMEWORK

BULGARIA

TOOLKIT

Alliance 4Europe

CSD | CENTER FOR THE STUDY OF DEMOCRACY

TABLE OF CONTENTS

Foreword

Influence operations have become a persistent feature of the contemporary information environment. In Bulgaria, as across Europe, these operations increasingly combine information manipulation, coordinated online behaviour, and financial or regulatory circumvention. They exploit structural vulnerabilities in the media and digital ecosystem, adapt quickly to political and societal developments, and often operate below the threshold of clear legal violation.

Much of the early detection, analysis, and evidence gathering related to these operations is carried out by civil society organisations, independent researchers, and media actors. This work is often conducted with limited resources, yet it plays a critical role in identifying threats and informing response. At the same time, key levers for disruption sit with the technology industry, including platforms, infrastructure providers, and financial and advertising services. Public institutions remain essential for legal enforcement, attribution, and coordination, but no single actor can address this challenge alone.

In Bulgaria, relevant competences are distributed across multiple institutions, while coordination across sectors often remains ad hoc. Responses are frequently triggered only once legal or procedural thresholds are met, which can delay action. In parallel, the absence of a shared operational language and standardised processes across actors makes cooperation more difficult and can lead to fragmented responses.

Establishing a common taxonomy and clearer workflows is therefore not a technical exercise, but a practical necessity. It enables actors to understand each other's assessments, align expectations, and act more quickly and coherently. For civil society, this also helps ensure that evidence and analysis can be more effectively used by institutions and other partners.

The current environment further highlights the urgency of strengthening this coordination. Electoral processes, geopolitical tensions, and rapid technological developments, including the growing use of artificial intelligence, continue to expand both the scale and sophistication of influence operations. Responses that rely solely on case by case reactions or formal legal thresholds risk being too slow or too fragmented to be effective.

This Toolkit has been developed to respond to these challenges. It translates the DISRUPT Framework into the Bulgarian context, drawing on the experience of practitioners across civil society, institutions, and the private sector. 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*. It is intended as a practical resource to support cooperation across sectors, improve predictability in responses, and strengthen the overall resilience of the system.

Addressing influence operations requires a *whole of society effort*.

Dr. Lumi Sarvela , Alliance4Europe **Rositsa Dzhekova, Center for The Study of Democracy**

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 practice, detection, analysis, and early response are often driven by civil society organisations, independent researchers, and media actors, while key points of disruption frequently sit with the technology industry. Public authorities play an essential role in legal enforcement, attribution, and coordination, but effective response depends on how these actors operate together.

In Bulgaria, relevant competences are distributed across multiple institutions, while civil society organisations play a central role in monitoring and early detection. Experience has been developed through international cooperation, election-related response, and implementation of European Union instruments such as sanctions regimes and the Digital Services Act. However, responses are typically triggered only once legal or procedural thresholds are met, and coordination tends to occur on a case-by-case basis rather than through a structured operational approach across institutions and sectors.

This toolkit presents a national localisation of the DISRUPT Framework, drawing on the DISRUPT Toolkit White Paper and on multi-stakeholder consultations conducted in Bulgaria. 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 helping practitioners identify 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.

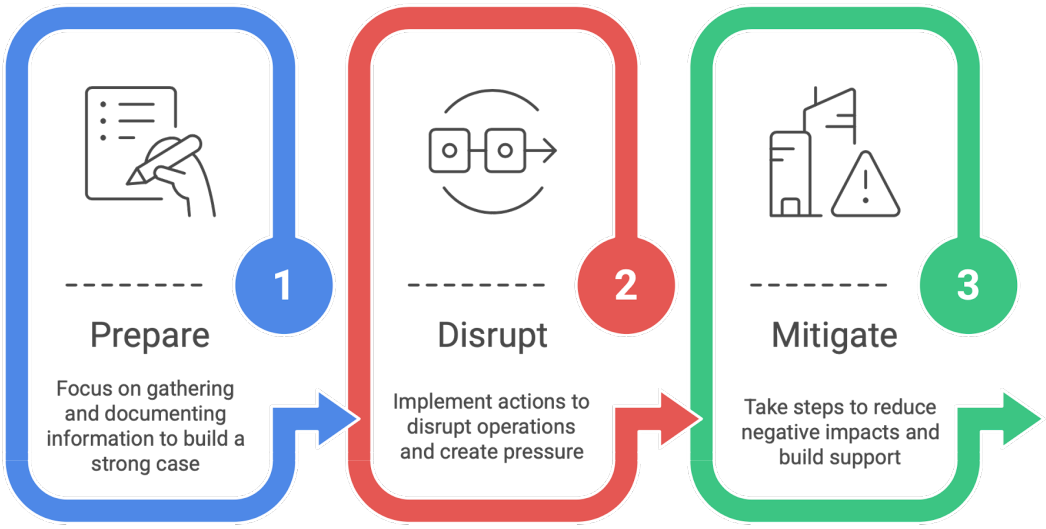
A central feature of the Framework is the use of decision points that help determine when a case has developed sufficiently to move from preparation into disruption, and when mitigation needs to be activated because disruption is delayed or insufficient. In this way, the Framework helps practitioners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

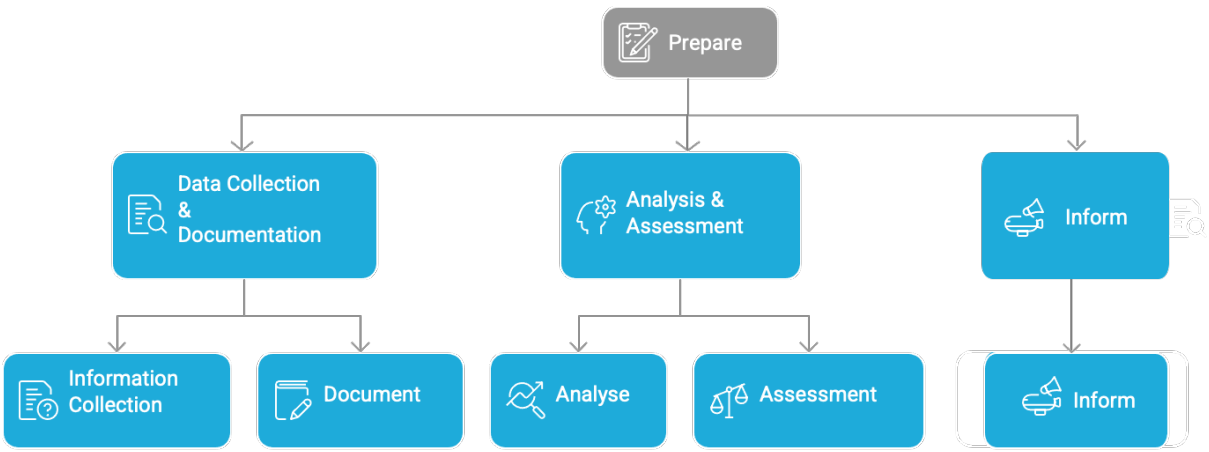
3.1 PREPARE

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:

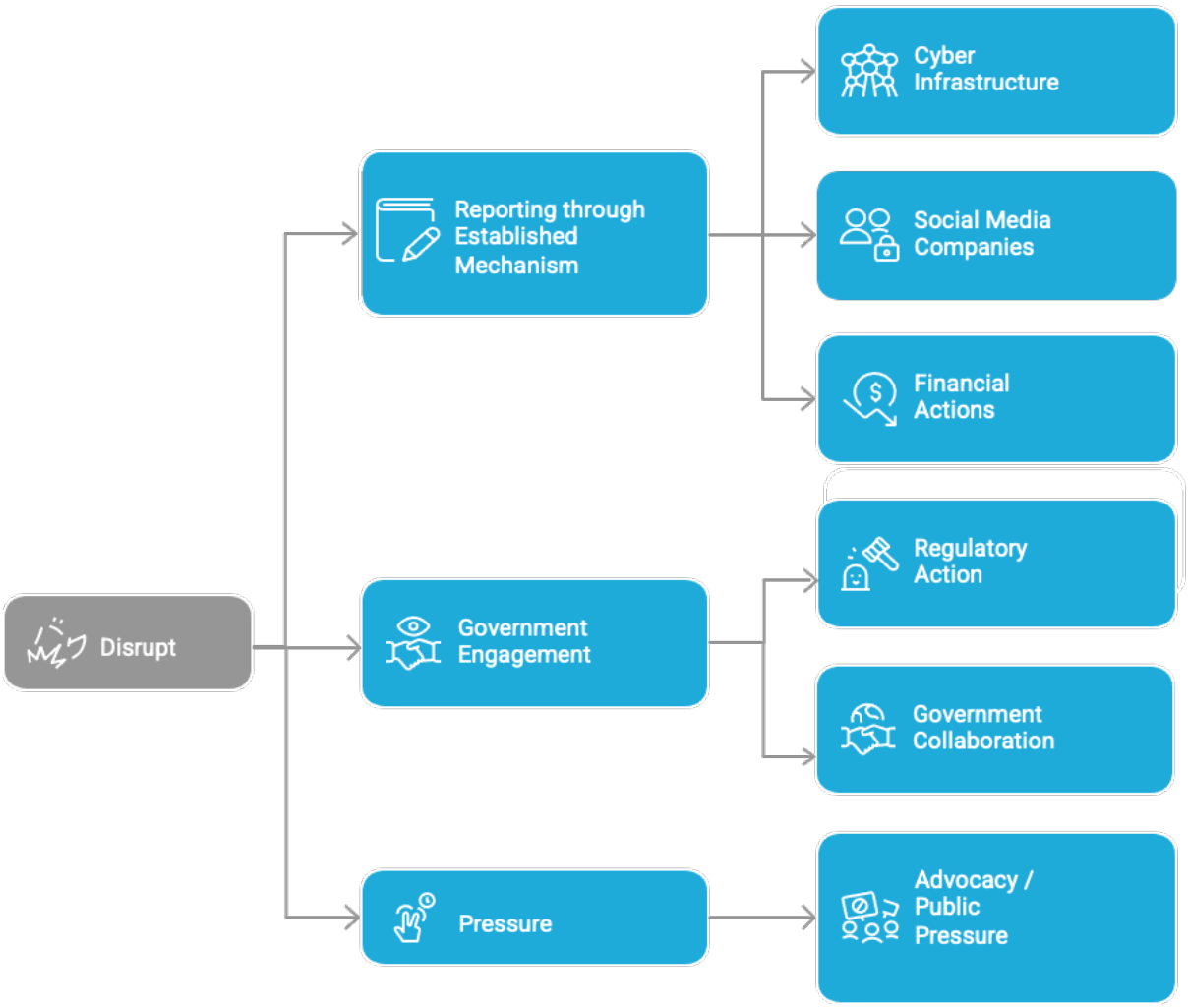
- regulatory or administrative measures;
- law enforcement or judicial processes where applicable;
- platform-related actions;
- diplomatic or coordination measures.

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.

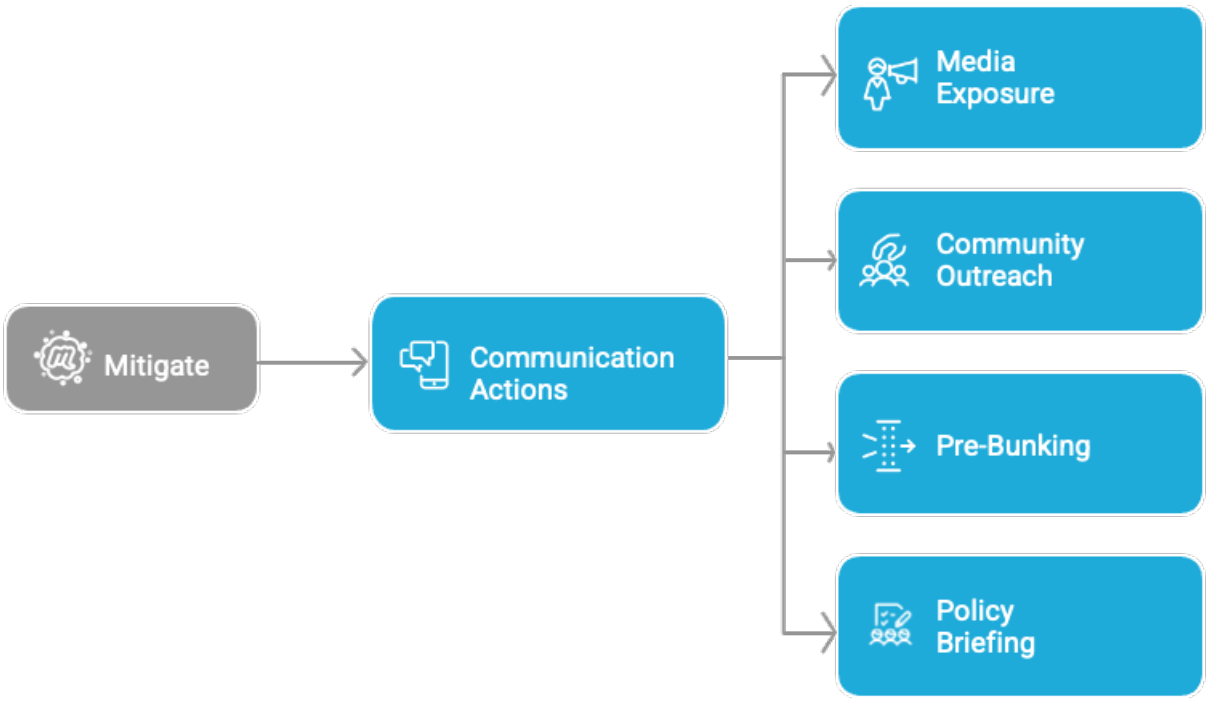
3.3 MITIGATE

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 Bulgaria 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 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 Bulgaria

Bulgaria's response to influence operations is shaped by **a diversified and multi-sectoral stakeholder ecosystem**, spanning public institutions, civil society, media, academia and a specialised technology and OSINT sector.

Competences are formally distributed across government institutions with distinct mandates, including diplomatic coordination, threat assessment, regulatory oversight, enforcement, and public communication. At the same time, core operation inputs - particularly in the PREPARE phase - are largely **generated outside government**, particularly by civil society, journalists, and technical actors.

As a result, effective response depends on **structured coordination across sectors** linking distributed detection and analysis to institutional decision-making and intervention.

6.1 Sectoral Breakdown of the Response Ecosystem

The Bulgarian landscape can be understood across five core sectors, each contributing distinct capabilities:

- **Government and regulatory authorities**
  Responsible for activating formal measures, including regulatory action, investigation, sanctions coordination, and diplomatic engagement.
- **Media and journalism actors**
  Contribute verification measures (eg. fact-checking, investigative exposure), generate public pressure and support mitigation through public communication.
- **Civil society organisations**
  Led many PREPARE-phase measures, including monitoring, documentation, analysis, and evidence building.
- **Academic and research institutions**
  Provide methodological validation and analytical depth.
- **Technology and OSINT actors**
  Enable data-driven measures such as network analysis, behavioural detection and infrastructure mapping.

The sectors are functionally distinct but **operationally interdependent**.

6.2 Differentiation Within Civil Society

Civil society in Bulgaria is **not a single functional actor,** but a **fragmented and specialised ecosystem**, with different organisations contributing at different stages of the Framework.

Key functional groupings include:

- **Investigative organisations** uncover networks and relationships (eg. actor mapping, attribution), financial links, and influence structures.
- **Fact-checkers** assess content accuracy and narrative manipulation (eg. verification, debunking).
- **Policy and research organisations** provide structured analysis and reporting.
- **Advocacy and rights-based organisations** support accountability and rights-based oversight.

In operational terms, **civil society provides a distributed capability for evidence collection, documentation and early- stage analysis, which feeds into institutional processes.**

6.3 Technology and OSINT as a Core Operational Layer

A defining feature of the Bulgarian context is the presence of a strong and specialised technology and OSINT sector, which plays a central role across all phases of the framework.

Key technology and OSINT actors include:

- Center for the Study of Democracy (CSD) (OSINT)
- Ontotext
- Sensika
- Adatapro

These actors provide capabilities that enable:

- large-scale data ingestion and analysis
- detection of coordinated inauthentic behaviour
- mapping of influence networks and infrastructure
- real-time analytical support for decision-making

This technical capacity is critical in enabling the transition from **data collection to operationally actionable disruption**, bridging the gap between detection and intervention.

6.4 Regulatory and Institutional Context

Regulatory authorities play an important role in the DISRUPT phase, particularly through measures such as content removal, platform engagement, and administrative sanctions.

However, the Bulgarian regulatory environment remains partially operationalised. The Communications Regulation Commission (CRC) has been designated as the Digital Services Coordinator (DSC), but operational capacity remains limited, including:

  - small team size
  - no systematic monitoring capability
  - limited investigative powers
  - limited leverage over platform behaviour

Similarly, the Council for Electronic Media operates within a **narrow legal scope**, primarily addressing registered audiovisual services.

As a result, regulatory measures - particularly those linked to platform governance under the Digital Services Act - are currently **case-dependent rather than systematically deployable in Bulgaria**, where enforcement is still limited

At the same time, disruption in Bulgaria does not rely on a single regulatory framework, but on a combination of legal and institutional instruments spanning multiple domains. These include criminal law, electoral law, media regulation, financial intelligence, data protection, and platform governance mechanisms, while sanctions regimes remain limited in their applicability.

The table below summarises the principal legal and regulatory instruments available for disruption in Bulgaria, and the types of measures they enable.

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

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, systemic risk escalation	Report Content; DSA Notice & Action Mechanism; Reporting T/S Abuse; Digital Service Coordinator Oversight; Leveraging DSA Systemic Risk Obligations	Communications Regulation Commission (CRC) as DSC; Council for Electronic Media (CEM) for video-sharing platforms; Commission for Personal Data Protection (CPDP) for data processing aspects; European Commission in relevant cases	CRC has formal coordinator role but limited operational capacity, limited investigative powers, no systematic monitoring, and limited leverage over algorithmic amplification
Electronic Communications Act amendments implementing the DSA	National legal basis for DSC designation and DSA implementation	Digital Service Coordinator Oversight; forwarding orders regarding illegal content	CRC	Institutional framework exists, but operational disruption capacity remains limited
Radio and Television Act	Audio-visual media regulation, illegal broadcast content, hate-inciting media content, complaints handling	Regulatory Action; Report Illegal Content; Audio-visual legislation; complaint-based action	Council for Electronic Media (CEM)	Applies mainly where services fall within formal regulatory scope; hybrid and unregistered formats create loopholes

European Media Freedom Act (EMFA)	Media freedom and governance context relevant to disruption involving media ecosystems	Potentially supports media-related regulatory and protection pathways	Ministry of Culture and other implementing bodies	Preparedness for implementation remains low; wider national implementation unclear
Bulgarian Criminal Code – Article 103	Harmful service to a foreign government or organisation	Foreign Agent Legislation; Invocation of Foreign Interference Legislation; Prosecutorial action	Prosecutor's Office; SANS/SIA as intelligence feeders	Requires high evidentiary threshold and formal criminal process
Bulgarian Criminal Code – Article 105 (Espionage)	Foreign intelligence collaboration, espionage-linked interference	Security Services; Prosecutor; Collaboration with Foreign Intelligence Services Legislation	Prosecutor's Office; SANS; SIA	Used where foreign service links can be demonstrated; threshold is high
Bulgarian Criminal Code – Article 108	Anti-democratic / fascist propaganda	Hate speech / anti-democratic content disruption; prosecution pathways	Prosecutor's Office; law enforcement	Enforcement may be uneven and content must clearly meet legal threshold
Bulgarian Criminal Code – Article 108a (Terrorism)	Terrorist content and terrorism-linked foreign interference	Report Content; Terrorism Laws; Security Service / Prosecutor action	Prosecutor's Office; law enforcement; security services	Criminal threshold required
Bulgarian Criminal Code – Article 109	Group activities supporting anti-state or related crimes	Foreign interference and extremist organisation disruption	Prosecutor's Office; law enforcement; security services	Requires legally supportable evidence of coordinated unlawful activity
Bulgarian Criminal Code – Article 320a	Cyber-enabled terrorist threats	Cyber-related escalation and criminal investigation	Prosecutor's Office; GDCOC / cybercrime units	Applies only where threat threshold is met
Bulgarian Criminal Code – Articles 146–148 (Insult / Defamation / Aggravated Defamation)	Defamation and reputational attacks	Legal action; complaint-based prosecution; potential reporting and exposure measures	Victim-driven proceedings; courts	Usually private prosecution, not a general state-led disruption tool

Article 162(1) Criminal Code	Incitement to discrimination, violence, or hatred	Hate speech / incitement disruption; criminal reporting	Prosecutor's Office	Framework notes reluctance of prosecutors to initiate proceedings in practice
Article 164(1) Criminal Code	Religious hatred	Hate speech-related disruption	Prosecutor's Office	Same threshold and enforcement constraints as above
Constitution of the Republic of Bulgaria – Article 39(2)	Restriction of speech used for incitement to violence, enmity, forcible constitutional change, crime	Supports legal framing of incitement-related disruption	Courts; relevant competent authorities	Constitutional basis, but operationalisation depends on specific statutory law
Law on Protection from Discrimination	Administrative/civil pathway for discriminatory conduct, harassment, instigation to discrimination	Complaints, administrative follow-up, supporting mitigation/disruption	Commission for Protection from Discrimination and relevant institutions	Not a primary counter-FIMI instrument, but relevant where discriminatory narratives or harms are present
Measures Against Money Laundering Act (MAMLA)	Financial tracing, money laundering-linked disruption, funding analysis	Identify Funding; Financial Intelligence Units; Freeze Banking Services; financial intelligence dissemination	Financial Intelligence Directorate within SANS (FID-SANS); downstream investigation/prosecution bodies	FIU is administrative in model and depends on other bodies for coercive action
Law on Measures against Financing of Terrorism (LMFT)	Autonomous national restrictive measures relating to terrorism financing	Freeze Banking Services; Financial disruption; sanctions-type measures	Council of Ministers on motion from MFA, Interior Minister, SANS Chair, or Prosecutor General	Specialised regime, not a general autonomous sanctions system for all influence cases
Law on International Restrictive Measures / national framework for implementation of international sanctions	Implementation of UN/EU sanctions and sanctions-related disruption	Utilise Existing Sanctions Legislation; Propose New Sanctions; Check Sanctions Status; Domain Sanctions Violations	Ministry of Foreign Affairs; Council of Ministers; Prosecutor's Office; other competent authorities depending on sector	Bulgaria does not have a broad autonomous national sanctions regime outside UN/EU implementation, except specific areas such as

				terrorism financing
EU sanctions regime / restrictive measures	De-platforming, financial disruption, sanctions circumvention response	EU Sanctions for De-Platforming and Financial Disruption; Utilise Existing Sanctions Legislation	MFA as initiator/coordinator; Council of Ministers for national implementation; EU institutions for listing processes	Requires strong evidence and legal justification, often slow and procedural. Note: sanctions regimes remain structurally limited in their practical application.
Bulgarian Electoral Code	Electoral silence, campaign restrictions, election-related interference	Silence Period enforcement; election-related reporting and intervention	Central Election Commission (CEC); Municipal and District Election Commissions; prosecution authorities where relevant	Relevant mainly in election periods; no general online targeting regime
Political Parties Law	Foreign financing restrictions and party funding controls	Foreign Finance Legislation; funding scrutiny	National Audit Office; election authorities; other relevant bodies	Focused on political finance, not broad information operations
Public Procurement Act	Restrictions relevant to financing and public-contract linked actors	Supporting funding / ownership scrutiny	Relevant public oversight bodies	Indirect relevance
National Audit Office Act	Oversight relevant to party finance and compliance	Funding oversight; possible escalation in political finance cases	National Audit Office	Indirect relevance for broader IO cases
GDPR / personal data protection framework	Data misuse, unlawful processing, targeting, profiling, privacy violations	GDPR-based complaints; Privacy & Data Protection Violations	Commission for Personal Data Protection (CPDP)	Useful where manipulation relies on unlawful data practices; not a general

				disinformation prohibition tool
Bulgarian Copyright and Neighbouring Rights Act	Copyright-based takedown and platform reporting	Copyright takedown; Report Copyright Infringement	Rights holders; courts; platforms; relevant enforcement bodies	Useful where protected content is misused, but narrow in scope
Act on Mandatory Deposit of Printed and Other Works / print media registration framework	Registration and traceability of certain media actors	Supporting ownership / traceability measures	Relevant registration authorities	Limited utility against online and hybrid formats
National Security Strategy	Framing influence operations as national security issue	Supports security-sector engagement and attribution	MFA; security services; executive authorities	Strategic framing tool rather than direct standalone enforcement basis
AI Act (EU)	Future relevance for AI-generated manipulation, deepfakes, high-risk AI systems	Potential future AI-related disruption and oversight measures	Ministry of Electronic Governance appears to be lead agency in preparation phase	Bulgaria has not yet designated the final competent authority; implementation remains incomplete

A key operational challenge in Bulgaria is that these instruments are **distributed across multiple legal domains and authorities**, with significant variation in readiness, scope, and enforceability. In practice, disruption is rarely based on a single information manipulation related law. Instead, effective action depends on matching the case to the **most appropriate available legal pathway** - for example, criminal law, sanctions law, electoral law, platform regulation, financial intelligence, or data protection - while recognising that some pathways remain **weakly operationalised or institutionally constrained**.

6.5 Cross-Sector Interaction Across the Framework

The DISRUPT Framework structures how these actors interact across the three phases: **Prepare, Disrupt, and Mitigate**.

6.5.1 PREPARE

Measures such as:

- information collection (OSINT, scraping, monitoring)
- documentation and evidence preservation
- behavioural and network analysis

are primarily carried out by **civil society, media, and technical actors**, with government actors playing a validation role.

6.5.2 DISRUPT

Measures such as:

- regulatory action
- platform reporting and escalation
- financial disruption
- legal and investigative action
- diplomatic coordination

are led by **government authorities and civil society**, but rely on externally generated evidence and technical identification of targets and infrastructure.

6.5.3 MITIGATE

Mitigation is a shared responsibility. Measures such as:

- public communication
- fact-checking and debunking
- narrative exposure
- public awareness and resilience-building

are **shared across government, media, and civil society**, combining authority, reach, and credibility.

6.6 Fragmentation and Coordination

Both government and civil society in Bulgaria are structurally fragmented, with expertise, authority, and access distributed across multiple actors.

The Framework addresses this by providing **a shared operational logic that enables coordination across fragmentation** 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.

6.7 Operational Implication

In Bulgaria:

- PREPARE measures are **distributed and largely driven by non-state actors, especially civil society organisations.;**
- DISRUPT measures are **institutionally controlled but evidence-dependent;**
- MITIGATE measures are **collective and societal.**

The framework provides a mechanism to connect these layers into a coherent operational workflow.

7. Current Operational Pattern in Bulgaria

Consultation findings indicate that influence operation response in Bulgaria develops through a distributed, multi-actor process, rather than in a linear institutional workflow.

While the DISRUPT Framework provides a structured model, actual practice reflects **uneven capability, fragmented detection, and threshold-based activation of measures**.

Table 2. Observed workflow pattern

Phase	Step	Examples of Measures	Output
PREPARE	Data Collection & Documentation	Social Listening; Narrative Monitoring; Find and Collect Publicly Available Content; Scraping; Crowdsourced Monitoring; Fact-check	Initial awareness
PREPARE	Analysis and Assessment	Document; Create Evidence Repository; Actor Mapping; Identify Pattern of Behaviour; Behaviour Analysis (DISARM); Identify Source of Content; Identify Identical Content; Attribution; Legality; Imminent Risk	Confirmed or assessed case
PREPARE → DISRUPT	Inform	Inform; Send Alert; Send Email; Briefing	
DISRUPT	Report Through Established Mechanisms	Report Content; DSA Notice & Action Mechanism; Reporting T/S Abuse; Report	Enforcement or referral

		Coordinated Inauthentic Behaviour; Digital Service Coordinator Oversight; Regulatory Action; Government Collaboration; Engage Political Actor; Engage MP; Engage Political Party; Security Services; Prosecutor; Financial Intelligence Units; Freeze Banking Services; Demonetise Operation Assets	
MITIGATE	Communication Actions	Publish Fact-check; Media Exposure; Name and Shame; Behavioural Exposure; Communication Actions; Pre-bunking; Narrative Inoculation; Public Education on Manipulation Techniques; Community Outreach; Influencer Partnerships	Public response

This pattern demonstrates that **timing and coordination are critical factors, particularly where response mechanisms are activated later in the lifecycle**.

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.
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 (CIB) cases are characterised by patterns of behaviour, coordination, and amplification rather than isolated instances of illegal content. As a result, effective response depends less on single content violations and more on the ability to document, analyse, and demonstrate coordinated activity over time.

In the Bulgarian context, stakeholder consultations indicate that early awareness of such cases typically originates outside formal state structures, including civil society organisations, researchers, and international partners. Institutional engagement becomes more likely once sufficient verification has been established, particularly where the case intersects with a clearly defined legal or regulatory pathway.

Table 3. CIB workflow overview

Phase	What this typically involves in Bulgaria	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through external monitoring, research, or partner notification. Cases are documented and initial patterns identified.	Preserve evidence and document coordination patterns in a structured way.	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 for severity, attribution, and possible routes for action, including legal, platform, or institutional pathways.	Determine whether the case meets thresholds for action and identify escalation routes.	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, 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 legal and procedural tools. Measures may involve platforms, regulators, financial disruption, or government actors.	Use the strongest available disruption measure without assuming formal enforcement is always 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, 10.5 Audio-Visual Regulator, 10.6 Prosecutor, 10.7 Communications Regulation Commission, 10.8 Ministry of Defence (Information Center)
MITIGATE	Where disruption is delayed or incomplete, communication and awareness measures are used to reduce impact.	Strengthen public resilience and expose manipulation techniques.	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 the Bulgarian context, the operationalisation of CIB response is shaped by three structural factors.

First, **evidence quality is central**. Most institutional actors can act only where legal certainty exists. As a result, measures such as *2.1 Observable list*, *2.3 Online Archiving*, and *2.4 Hash Evidence* are critical in ensuring that cases can move beyond detection toward action.

Second, **routing determines effectiveness**. The transition from PREPARE to DISRUPT depends on correctly identifying which pathway is viable - whether platform-based (e.g. *7.3 Report Coordinated*

Inauthentic Behaviour), regulatory (e.g. *9.1 DSA*), or institutional (e.g. *10.2 Ministry of Foreign Affairs*). In practice, cases often stall where no clear route is identified.

Third, **institutional capacity remains limited and fragmented**. Authorities such as the Communications Regulation Commission and the Council for Electronic Media operate within constrained mandates, while coordination across actors is decentralised. This increases reliance on external actors for early detection and documentation, and makes measures such as *5.1 Publish Report* and *11.3 Engage Journalist* particularly important in triggering response.

For Bulgarian practitioners, the main operational implication is that CIB response often depends on the quality of documentation, the clarity of routing, and the ability to connect external early warning with institutional processes. The Framework is therefore particularly useful in helping practitioners move from detection and documentation toward the most appropriate available response measure within existing mandates.

10. Application to Sanctions-Related Cases

Sanctions-related cases differ from CIB in that they are more directly anchored in formal legal and policy frameworks, particularly at EU and international level. However, their effective handling remains dependent on sequencing, evidence preparation, and the ability to activate the appropriate institutional pathway.

In the Bulgarian context, sanctions enforcement is characterised by a **distributed institutional landscape**, where responsibilities are divided across multiple actors, including the Ministry of Foreign Affairs, the Council of Ministers, regulatory authorities, and law enforcement bodies. As a result, response does not follow a single operational pathway, but rather depends on how clearly a case can be linked to a specific legal basis and competent authority.

Early stages of response therefore place particular emphasis on **evidence building**, especially demonstrating a verifiable link between the activity and a sanctioned entity, as well as establishing that the activity constitutes a violation under the applicable legal framework. Without this, institutional action is unlikely.

The transition from preparation to disruption is primarily a matter of **routing**: identifying whether the case should proceed through regulatory mechanisms (e.g. platform governance), administrative enforcement, financial disruption, or diplomatic and sanctions procedures. In practice, delays often occur at this stage due to unclear mandates, limited coordination, or insufficient evidentiary thresholds.

Disruption itself is implemented through competent authorities acting within their legal mandates, often requiring coordination across multiple bodies. This makes **sequencing and alignment of actions critical**, as fragmented escalation can reduce effectiveness.

Where enforcement is partial or delayed, mitigation measures - including limiting visibility, restricting access, or public communication - play an important role in reducing ongoing impact.

Overall, sanctions-related cases illustrate that the existence of legal instruments alone is insufficient. Effective response depends on the **timely alignment of evidence, institutional competence, and procedural pathways**, which the Framework helps to structure.

Table 4. Sanctions workflow overview

Phase	What this typically involves in Bulgaria	Main practitioner focus	Relevant Framework Measures
PREPARE	Evidence is gathered linking activity, channels, or infrastructure to a sanctioned entity, with emphasis on legal robustness and traceability	Build legally usable evidence and demonstrate link to sanctioned entity	1.1 Find and Collect Publicly Available Content; 2.1 Observable List; 2.2 Online Archiving; 2.4 Hash Evidence; 3.1 Analyse Content; 3.2 Identify Links Between Actor and Threat Actor; 4.2 Legality; 4.3 Attribution
PREPARE → DISRUPT	The case is assessed to determine the appropriate enforcement pathway (regulatory, financial, diplomatic, or legal), depending on available evidence and institutional competence	Identify correct authority and align evidence to required legal threshold	4.2 Legality; 4.3 Attribution; 5.2 Send Alert; 5.4 Briefing
DISRUPT	Action is implemented through competent authorities or external actors (platforms, service providers), depending on the pathway (e.g. infrastructure, platform, financial, sanctions enforcement)	Use the most effective available disruption vector and ensure coordinated escalation	6.1 Hosting; 6.2 Domain; 6.3 Revoke SSL Certificates; 6.4 Content Delivery Network; 7.1 Report Content; 7.2 Report Channel; 8.1 Demonetise Operation Assets; 9.1 DSA; 9.2 EU Sanctions; 10.2 Ministry of Foreign Affairs
MITIGATE	Where enforcement is delayed or incomplete, additional measures are used to reduce visibility, access, or impact, including public communication and stakeholder engagement	Limit ongoing harm and maintain pressure on relevant actors	11.1 Engage Political Actor; 11.2 Engage Advocacy Actors; 12.1 Media Exposure; 12.2 Expose Actor and Intentions

For Bulgarian practitioners, sanctions-related cases show the importance of linking evidence-building to the correct implementation pathway early enough in the process. The Framework helps by structuring that progression and by clarifying that effective response depends not only on the existence of legal instruments, but on the timely sequencing and coordinated use of them.

11. Minimum Operational Readiness

To apply the Toolkit effectively, institutions and practitioners should ensure the availability of basic coordination capabilities, alongside clear actions that operationalise them.

Table 5. Minimum Readiness Capability

Capability	Description	Operational actions (what actors can do)
Signal intake	Mechanism for receiving and reviewing alerts	Receive alerts from CSOs; screen incoming signals; prioritise cases based on risk (e.g. imminent harm, elections, national security relevance); acknowledge receipt and trigger initial review
Case tracking	Basic documentation of cases	Open a case file; assign responsible focal point; log key information (source, content, actor, timeline); update case status (open / under review / escalated / closed); maintain evidence repository
Routing clarity	Understanding of institutional competences	Identify competent authority (e.g. regulator, law enforcement, ministry); route cases to appropriate body; escalate high-risk cases; avoid duplication by clarifying roles across institutions
Evidence standards	Consistent approach to documentation	Collect and preserve evidence (screenshots, URLs, metadata); apply hashing where needed; ensure documentation meets legal thresholds; structure evidence to support reporting, sanctions, or prosecution
Coordination channels	Ability to engage relevant actors	Contact relevant stakeholders (platforms, regulators, government bodies, CSOs); convene coordination calls if needed; share information securely; align actions across actors (e.g. reporting + public communication)
Communication capacity	Preparedness for public messaging	Prepare factual statements, briefings, or alerts; decide whether to communicate publicly; engage media or publish fact-checks; ensure messaging is timely, accurate, and coordinated
Learning mechanisms	Ability to capture lessons learned	Conduct post-case review; identify what worked / gaps; update internal procedures; share lessons with partners; feed insights into training and preparedness activities

These elements support the Framework's role as a coordination standard and operational reference.

12. Conclusion

The Bulgarian institutional landscape includes a wide range of competences relevant to addressing influence operations. The primary challenge lies not in the absence of capability, but in the timing, sequencing, and coordination of action across institutions.

The DISRUPT Framework provides a structured approach to this challenge by introducing a shared lifecycle model, linking evidence development to proportionate intervention, and supporting cooperation across a whole-of-society system. Its localisation to Bulgaria demonstrates how coordination can be strengthened without altering legal mandates or institutional structures.

By clarifying workflows, aligning expectations, and enabling earlier and more predictable engagement, this Toolkit supports a more effective and resilient response to influence operations in Bulgaria.

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 Bulgaria

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; Purchase Data; Interview; Freedom of information request
PREPARE	Data Collection and Documentation	Document	Screenshots *(hashing required for legal certainty)*; Offline Archiving; Online Archiving; Hash Evidence
PREPARE	Data Collection and Documentation	Monitoring	Monitor and Track Operation Activity; Narrative Monitoring *(relies on CSOs in Bulgaria)*; Account Monitoring; Behavioural Monitoring; Crowdsourced Monitoring
PREPARE	Analysis and Assessment	Analyse	Actor Mapping; CIB Detection; Manual CIB Detection; CIB Algorithm; Analyse Content; Identify Deepfake; Identify AI-re-writen Content; Identify Identical Content; Identify Source of Content
PREPARE	Analysis and Assessment	Assessment	**Legality** *(Criminal Code; Electoral Code; GDPR; Digital Services Act; Law on Radio and Television; Measures Against Money Laundering Act)*; **Attribution** *(Ministry of Foreign Affairs; Security Services – SANS, SIA)*; **Imminent Risk** *(GDCOC Cybercrime Department; Security Council)*; **Foreign Interference** *(Criminal Code Art. 103, 105, 108, 108a; Prosecutor's Office)*; Identify Illegal Content; Identify links between actor and threat actor; Identify Funding *(FIU – FID-SANS)*; Identify Ownership Structure (UBO); Identify Personnel Affiliations; Identify Partnerships, Clients, and Service Providers; Identify Amplification; Identify Pattern of Behaviour; Check Sanctions Status *(EU/UN sanctions; LMFT)*
PREPARE	Analysis and Assessment	Infrastructure Analysis	Identify Infrastructure; Domain Analysis; URL Analysis; IP Analysis; Software Components Analysis; Services; Identify AI Generation Tool *(AI Act – pending national authority)*

DISRUPT	Inform	Inform	Send Alert; Send Email; Briefing; Publish Report *(critical due to limited institutional monitoring capacity in Bulgaria)*
DISRUPT	Report Through Established Mechanisms	Platform & Content Reporting	Report Content; Reporting T/S Abuse; DSA Notice & Action Mechanism *(CRC as Digital Services Coordinator)*; Report Illegal Content; Report Copyright Infringement *(Bulgarian Copyright Law)*; Reporting NCII T/S Abuse; Report as Spam; Report Coordinated Inauthentic Behaviour
DISRUPT	Report Through Established Mechanisms	Legal / Harm Categories	Incitement to Violence *(Criminal Code; Constitution Art. 39)*; Hate Speech *(Art. 162, 164)*; Terrorist Content *(Art. 108a)*; Intellectual Property Infringement; Privacy & Data Protection Violations *(GDPR; Commission for Personal Data Protection)*; Defamation *(Art. 146–148)*; Impersonation; Fraudulent Registration Information; Domain Sanctions Violations; Sanctioned content; Unlabelled Political Ads *(Election Code)*; Holocaust Denial *(covered under hate speech provisions)*
DISRUPT	Report Through Established Mechanisms	DSA & Regulatory Mechanisms	DSA; DSA Out-of-court Dispute Settlement *(ACE; ADR Center; ADR Point)*; Leveraging DSA Systemic Risk Obligations (Article 34-35 Reporting); DSA Trusted Flagger Mechanism *(not yet developed in Bulgaria)*; Digital Service Coordinator Oversight *(CRC; CEM; Data Protection Commission)*
DISRUPT	Cyber Infrastructure	Cyber Infrastructure	Hosting; Domain; Website Components; Content Delivery Network; Web Application Firewall; Remove Search Engine Results; The Right to be Forgotten *(GDPR)*; Revoke SSL Certificates
DISRUPT	Social Media Companies	Social Media Companies	Direct Platform Engagement; Contact Platform Representatives
DISRUPT	Financial Actions	Financial Actions	Demonetise Operation Assets; Ad Network; Ad Buyer; Advertising; Monetisation; Financial Services; Freeze Banking Services *(FIU – FID-SANS; AML framework)*; Investor; Payment Provider; Crypto Exchange and Wallet

DISRUPT	Regulatory Action	Regulatory Action	EU Sanctions for De-Platforming and Financial Disruption; Utilise Existing Sanctions Legislation *(EU/UN sanctions; LMFT)*; Propose new sanctions *(Ministry of Foreign Affairs → Council of Ministers)*; Invocation of Foreign Interference Legislation *(Criminal Code)*; Foreign Finance Legislation *(Political Parties Law; Election Code)*; GDPR *(Commission for Personal Data Protection)*
DISRUPT	Government Engagement	Government Collaboration	Counter FIMI Agency *(not present in Bulgaria)*; Ministry of Foreign Affairs; Security Services (SANS, SIA); Financial Intelligence Units (FID-SANS); Interior Ministry (GDCOC/GDBOP); Audio-Visual Regulator (CEM); Prosecutor's Office; Police; Military / Ministry of Defence (Information Center); Electoral Authorities (CEC); Election Management Body; Digital Service Coordinator (CRC); EU Institutions; National Institutes for Cyber Security; Ombudsman office; Data Protection Regulator; Consumer Protection Regulator
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 Private Sector; Engage Interest Group; Engage Company; Engage Journalist; Written question to institutions (officially); Media Exposure; Name and Shame; Behavioural Exposure; Expose Actor and Intentions; Open Letter; Civil Society Joint Letter; Online Petition *(important due to reliance on CSOs in Bulgaria)*
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 *(e.g. Diplomatic Institute training)*; Influencer Partnerships; Youth-focused messaging; Flood the information space with positive narratives