DISRUPT FRAMEWORK

CZECHIA

TOOLKIT

Alliance 4Europe

Prague Security Studies Institute

AMO.CZ

TABLE OF CONTENTS

Foreword

Czechia operates within an increasingly complex information environment shaped by persistent **foreign information manipulation and interference (FIMI), coordinated inauthentic behaviour (CIB)**, and broader hybrid threats. As a Member State of the European Union and NATO, and as a country with recent experience in electoral integrity challenges, Czechia faces sustained pressure on democratic processes, public trust, and institutional credibility.

This pressure has become more pronounced in the context of political developments following the October 2025 elections in Czechia, which introduced a more volatile alignment in the national political landscape. In this environment, influence operations do not occur in isolation, but intersect with domestic political dynamics, public debate, and regulatory positioning - particularly in relation to EU digital frameworks such as the Digital Services Act (DSA). This creates additional complexity for institutional response, as operational action may be affected by shifting national political priorities or levels of political support.

Beyond their immediate informational impact, influence operations contribute to polarisation, undermine trust in public institutions, and can weaken social cohesion over time. Electoral periods remain particularly sensitive, but influence activity is continuous and adaptive, requiring sustained attention beyond crisis moments.

Czechia benefits from a diverse response ecosystem, however with limited direct disruption capabilities, comprising state institutions, civil society organisations, academic institutions, media actors, and international partners. This network includes a particularly strong concentration of civil society and academic actors, which provide analytical capacity, methodological validation, and operational continuity.

In the current context, this broad ecosystem plays a critical stabilising role. By embedding the Framework within a wide network of non-governmental and academic partners, it contributes to creating a resilience layer that can sustain counter-influence efforts independently of short-term political shifts. At the same time, continued engagement with technical and professional actors within state institutions- particularly in security and hybrid threat domains - ensures alignment with the Czech Republic's long-term security architecture.

However, effective disruption depends not only on the availability of actors, but on how these actors are connected. While Czechia demonstrates strong capabilities across monitoring, analysis, and communication, coordination remains largely informal and case-specific. As highlighted in the national consultation, no single actor is responsible for linking detection, disruption, and mitigation into a continuous operational process, and response timing is often affected by unclear escalation thresholds and fragmented workflows.

The DISRUPT Toolkit is designed to support this coordination. By introducing a shared operational logic and common vocabulary, the Toolkit aims to support practitioners across sectors in understanding *what actions are available, when they can be applied, and how coordination can be initiated more predictably*. It is intended as a practical resource to strengthen cooperation across the Czech response ecosystem, improve response timing, and enhance overall resilience.

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

Saman Nazari , Alliance4Europe **Kristína Šefčíková, PSSI** **Pavel Havlicek, AMO**

1. Introduction

Influence operations present a sustained challenge to democratic processes, public trust, and national security. These activities evolve rapidly, often peak within short timeframes, and operate across institutional and sectoral boundaries, making coordinated response inherently complex.

In Czechia, the response landscape is characterised by a **broad but distributed ecosystem**, where responsibilities are divided across ministries, regulators, law enforcement bodies, intelligence services, cybersecurity authorities, and communication structures, as well as a large number of civil society, academic, and media actors. This distribution enables specialised expertise, but also means that response depends on how effectively these actors coordinate across mandates.

The Czech Republic has developed practical experience in election security, crisis communication, and hybrid threat awareness, and maintains strong monitoring and analytical capabilities. However, national stakeholders across government, security and intelligence services, electoral bodies, regulators, and civil society and media organisations recognise that current response mechanisms rely heavily on informal, ad hoc coordination, which can be effective in familiar or crisis-driven scenarios, but struggles to keep pace with fast-moving influence operations outside declared emergencies.

A key challenge lies in the **transition from detection to action**. While monitoring and analysis are well developed, disruption pathways are more limited, particularly in cases that do not meet criminal thresholds or fall outside clearly defined legal frameworks. As a result, response is often delayed, sequential, or dependent on case-by-case escalation, rather than driven by predefined operational triggers.

This toolkit presents a national localisation of the DISRUPT Framework, drawing on the DISRUPT Toolkit White Paper and on multi-stakeholder consultations conducted in the Czech Republic. 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 the roles of different actors across society and how their efforts can be coordinated. By standardising how measures are combined and sequenced, it reduces the burden on individuals and organisations, making the fight against disinformation more practical and manageable.

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, measures, templates, workflows, and 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 **DISRUPT** 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.

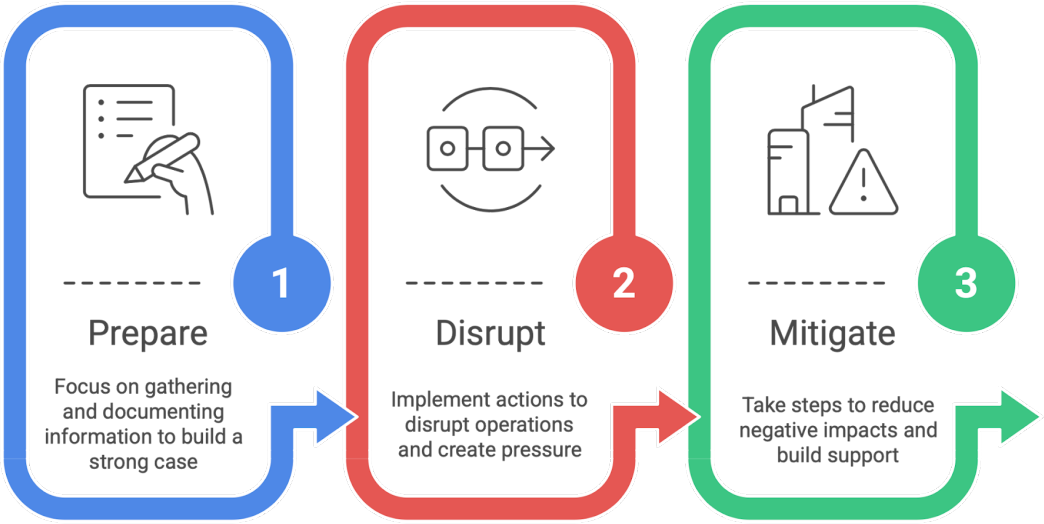
A central feature of the Framework is the use of decision points that help determine when a case has developed sufficiently to move from preparation into disruption, and when mitigation needs to be activated because disruption is delayed or insufficient. In this way, the Framework helps counter disinformation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

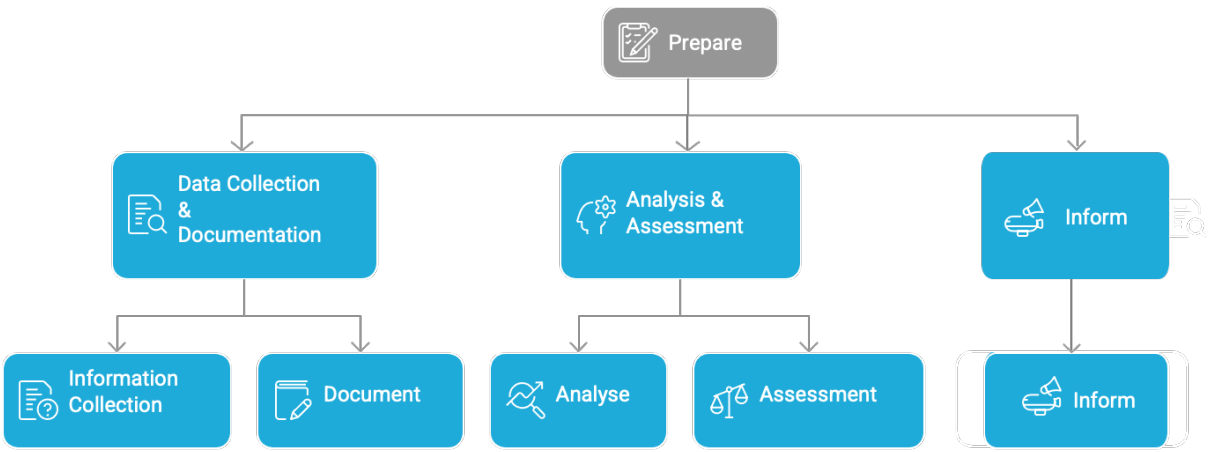
3.1 PREPARE

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:

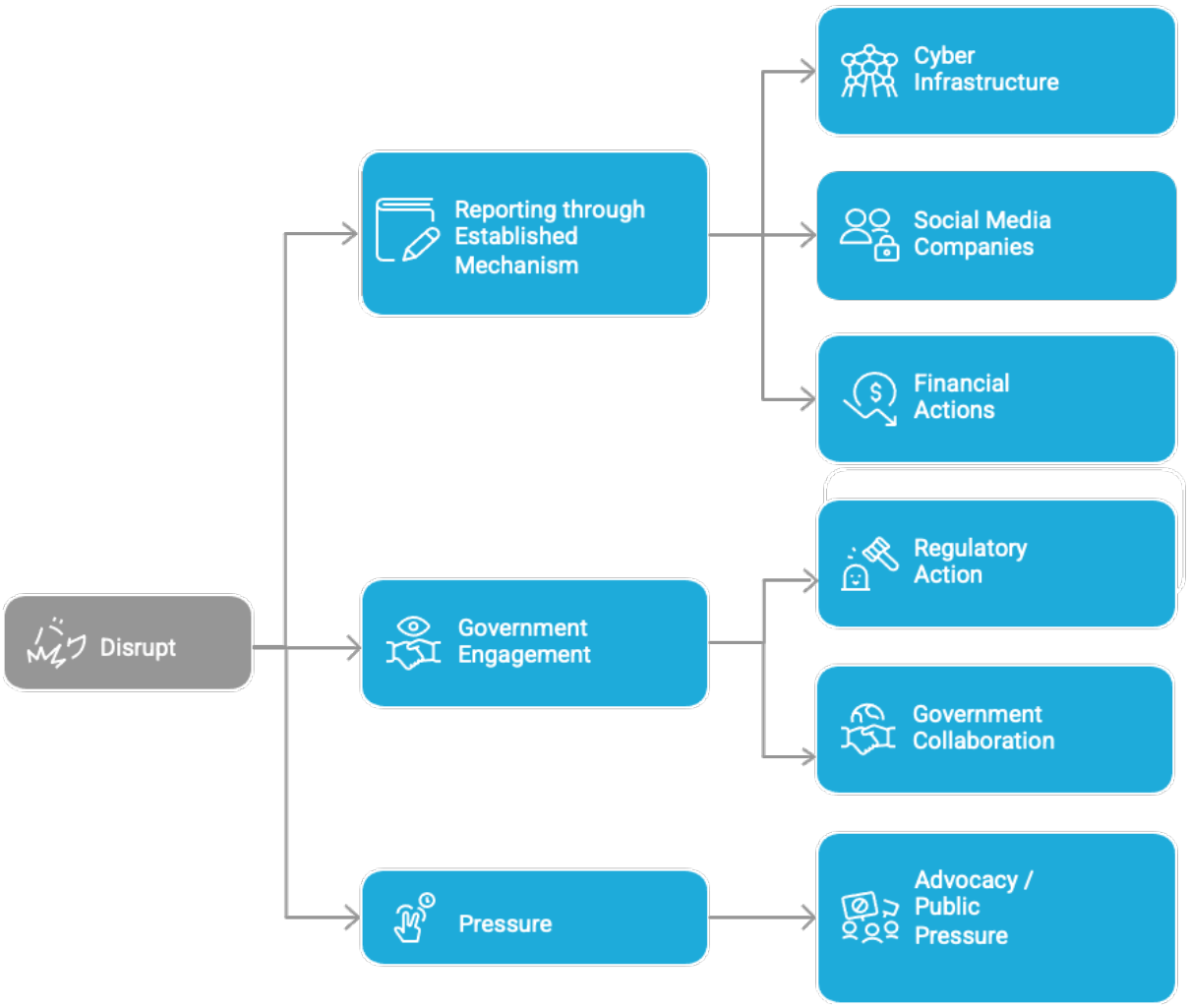
- regulatory or administrative measures;
- law enforcement or judicial processes where applicable;
- platform-related actions;
- diplomatic or coordination measures.

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.

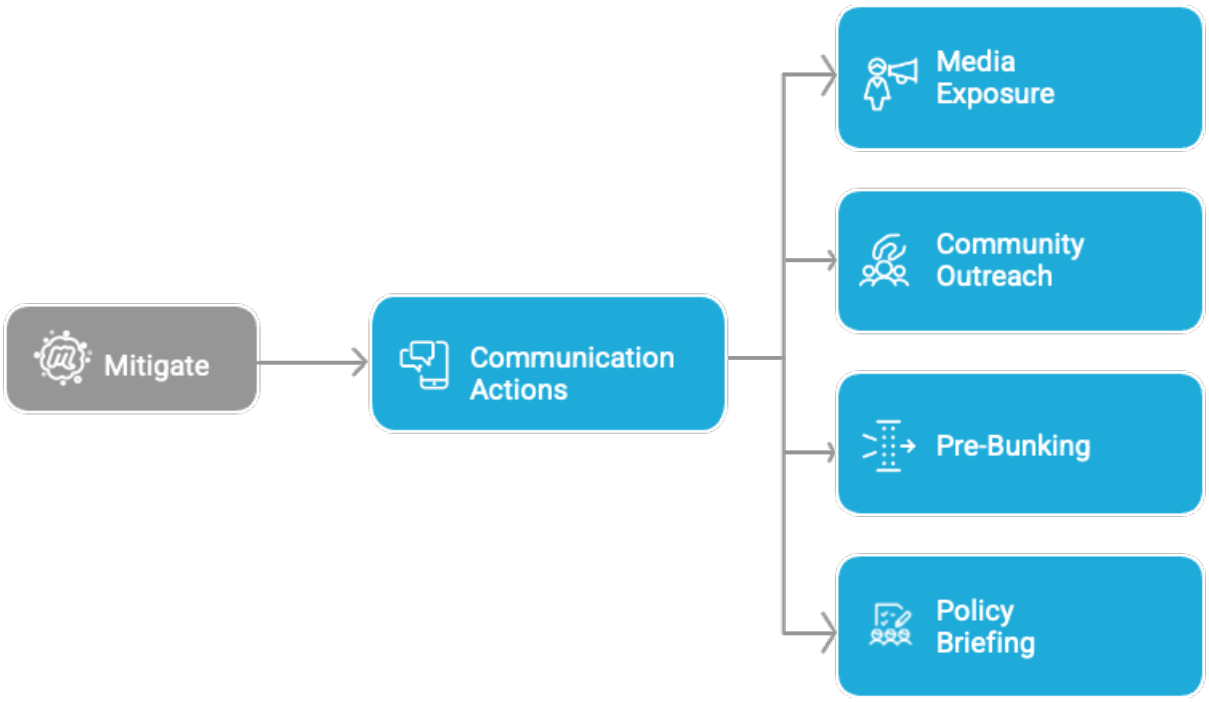
3.3 MITIGATE

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 Czechia 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 provides a shared operational layer intended to improve coordination, sequencing, and response timing.

6. National Response Structure in Czechia

6.1 Sectoral Breakdown of the Response Ecosystem

The Czech response ecosystem for influence operations is characterised by a **broad and highly diversified network of actors**, spanning public institutions, civil society, academia, media, and international partners. This distribution reflects a "whole-of-society" model, in which analytical, operational, regulatory, and communication functions are not concentrated within a single institutional structure, but distributed across multiple sectors. While this enables a high level of expertise and resilience, it also means that effective response depends on coordination between actors rather than a single operational chain.

- **Government and regulatory authorities**
  Includes national security, regulatory and ministerial actors, such as ČTÚ, and relevant departments within ministries (e.g. Interior, Defence). While political turnover has affected strategic communication functions at the executive level, the framework remains anchored in the permanent technical and security apparatus. This ensures continuity of expertise and alignment with the Czech Republic's long-term security architecture, particularly for PREPARE (analysis) and DISRUPT (legal and security pathways).
- **Civil society organisations**
  The largest and most operationally active cohort, forming the backbone of the ecosystem. Organisations such as the Association for International Affairs (AMO), Prague Security Studies Institute (PSSI), and the Center for Informed Society contribute to monitoring, analysis, policy development, and practical disruption support. Their role is particularly significant in sustaining operational continuity, supporting PREPARE activities, and enabling MITIGATE functions through public communication, advocacy, and exposure.
- **Academic institutions**
  Provides methodological validation, technical expertise, and analytical depth. Institutions such as Charles University (FSV), Masaryk University, and the Central European Digital Media Observatory (CEDMO) hub bridge research and practice, supporting evidence-based assessment, detection methodologies, and evaluation of disruption approaches. This sector strengthens the analytical rigour of the PREPARE phase and contributes to long-term capacity building.
- **Media and journalism actors**
  Includes public broadcasters (e.g. Czech Television, Czech Radio) and investigative outlets (e.g. Investigace.cz). This sector plays a critical role in validating findings, exposing influence operations, and amplifying mitigation efforts. Media actors are central to the MITIGATE phase, particularly in public communication, narrative clarification, and accountability.

Taken together, these sectors are functionally distinct but operationally interdependent. The overall ecosystem reflects a whole-of-society approach in which detection, assessment, disruption, and mitigation are distributed across actors. This distribution highlights both the scale and diversity of the network, as well as the feasibility of a multi-stakeholder response model grounded in a broad and resilient ecosystem.

6.2 Differentiation Within Civil Society

Civil society organisations in Czechia do not operate as a single, homogeneous group. Instead, they fulfil a range of distinct but complementary functions across the lifecycle of influence operations, particularly in the PREPARE and MITIGATE phases, and to a more limited extent in DISRUPT through platform engagement and public exposure.

The Czech ecosystem is characterised by a **high concentration and diversity of civil society actors**, which form the largest and most operationally active component of the national network. These organisations contribute not only to detection and analysis, but also to communication, advocacy, and public accountability, making them central to the overall response model.

Several functional groupings can be identified within this sector:

- **Analytical and monitoring organisations** focus on identifying emerging narratives, tracking coordinated behaviour, and documenting influence operations. These actors contribute to social listening, narrative monitoring, and evidence collection, often working in close alignment with academic partners.
- **Research and methodology-focused organisations** support the development and validation of analytical approaches, including detection methodologies, attribution practices, and evaluation frameworks. Their role is particularly important in ensuring that assessments are evidence-based and methodologically robust.
- **Advocacy and policy organisations** engage in shaping public debate, raising awareness of influence operations, and promoting policy responses at national and European levels. These actors contribute to maintaining visibility of the issue and sustaining pressure on institutions and platforms.
- **Fact-checking and investigative organisations** play a key role in verifying claims, exposing manipulation techniques, and providing publicly accessible evidence of influence activity. Their work supports both detection and mitigation by translating complex analytical findings into accessible formats.
- **Communication and public engagement actors** contribute to awareness campaigns, media collaboration, and public education initiatives. These activities are central to mitigation efforts, particularly in addressing the impact of influence operations once they become visible.

Across these functions, civil society organisations frequently operate in **close collaboration with academic institutions and media actors**, forming interconnected clusters of expertise that support both analysis and communication. This integration strengthens the overall ecosystem by linking technical assessment with public dissemination and accountability.

In the Czech context, the scale and diversity of civil society involvement also serve a strategic function. Given the current political environment and the potential variability in institutional engagement, this

sector provides a form of **operational continuity and resilience**, ensuring that monitoring, analysis, and public communication can be sustained independently of shifts in political priorities.

At the same time, civil society actors generally lack formal enforcement powers, and their ability to contribute to disruption depends on indirect mechanisms, such as platform reporting, public exposure, and advocacy-driven pressure. As a result, their role is strongest in early-stage detection and later-stage mitigation, while their impact on disruption is mediated through engagement with platforms, regulators, and public authorities.

Overall, **the differentiation within civil society highlights a sector that is both highly specialised and structurally central to the Czech response ecosystem**. Its effectiveness lies not only in individual organisational capacity, but in the ability to connect analytical, communicative, and advocacy functions across the broader network.

6.3 Regulatory and Institutional Context

Regulatory and institutional actors in Czechia play an important role in the DISRUPT phase, but their ability to intervene is shaped by legal thresholds, formal competences, and a fragmented distribution of mandates. Czechia does not have a single authority that connects the PREPARE, DISRUPT, and MITIGATE phases into a continuous operational process. Instead, institutions operate within specialised roles across the response ecosystem.

Analytical and monitoring functions are primarily carried out by actors such as the Ministry of the Interior's Centre Against Hybrid Threats (CHH), alongside civil society and academic partners. Law enforcement bodies, including specialised police units and prosecutors, intervene when activity meets criminal thresholds, particularly in cases involving fraud, incitement, or national security concerns. Security services operate in parallel through intelligence and counter-intelligence channels, focusing on foreign-linked threats but with limited public-facing engagement.

Administrative and regulatory functions are distributed across sectoral authorities. The Czech Telecommunication Office (ČTÚ) holds responsibilities linked to the implementation of the Digital Services Act, including coordination and escalation of platform-related cases, but its role remains limited in practice due to incomplete implementation and constrained enforcement powers. Financial disruption pathways are available through the Financial Analytical Office (FAÚ), particularly in relation to anti-money laundering and sanctions enforcement, although these require strong evidentiary grounding and often operate on longer timelines.

Other regulatory instruments, including sanctions legislation, anti-money laundering frameworks, and foreign investment screening mechanisms (see table 1), provide additional avenues for disruption, particularly in cases involving financial flows or sanctioned entities. These pathways enable measures such as asset freezing, financial investigation, and reporting obligations, typically coordinated through bodies such as the Financial Analytical Office. However, these measures are evidence-intensive and often require cross-sectoral coordination to be effective.

Electoral legislation provides a separate, time-bound set of instruments applicable during election periods. Oversight bodies such as the Office for the Supervision of the Financial Management of

Political Parties and Political Movements (UDHPSH) can act on campaign financing, political advertising transparency, and specific violations within the electoral framework. These mechanisms can enable relatively rapid intervention in defined contexts, but do not extend to broader influence operations outside electoral periods.

Across the system, communication and mitigation functions are distributed among government communication units, civil society, and media actors, and are typically activated once an issue becomes publicly visible or requires clarification. There is no central authority responsible for linking communication with earlier stages of detection and disruption.

Overall, the Czech regulatory and institutional landscape reflects a model in which disruption is not driven by operational urgency alone, but by the availability of a qualifying legal or regulatory pathway. While a wide range of instruments exists, their application depends on case classification, evidentiary thresholds, and institutional mandates. As a result, response pathways can be fragmented, and the transition from detection to action is not consistently structured.

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

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

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 (Articles 34–35 Reporting); Digital Service Coordinator Oversight	Czech Telecommunication Office (ČTÚ) as DSC; European Commission in relevant cases; platforms	The DSA has not yet been fully operationalised in Czechia. ČTÚ's role is focused on escalation and liaison rather than strong independent enforcement, which limits speed and direct intervention.
DSA out-of-court dispute settlement	Structured review of disputes concerning platform decisions under the DSA	DSA Out-of-court Dispute Settlement	Relevant out-of-court dispute settlement bodies; platforms; users	This is a structured redress mechanism rather than a rapid disruption tool. It may support escalation, but usually does not produce immediate results.
DSA systemic risk obligations	Structural escalation where platform failures in handling illegal or manipulative	Leveraging DSA Systemic Risk Obligations (Articles 34–35 Reporting)	European Commission; ČTÚ in coordination role	Useful for sustained or repeated failures by platforms, but slow and not

	content may indicate systemic risk			suitable for rapid-response disruption in fast-moving cases.
Czech DSA implementation / DSC framework	National coordination for DSA-related cooperation and liaison with EU structures	Digital Service Coordinator Oversight; forwarding platform-related cases; coordination with EU mechanisms	ČTÚ	The current Czech framework reflects a coordination role rather than a strong enforcement model. Missing implementing arrangements weaken the practical impact of this pathway.
Law No. 69/2006 Coll. on the implementation of international sanctions	Disruption of activities linked to sanctioned individuals, entities, or content originating from sanctioned actors	Utilise Existing Sanctions Legislation; EU Sanctions for De-Platforming and Financial Disruption; sanctions-related escalation to platforms and providers	Police; Financial Analytical Office (FAÚ); Ministry of Foreign Affairs in external dimension	Provides a clearer legal pathway than general CIB cases, but enforcement remains evidence-heavy and operational practice appears limited.
Law No. 1/2023 Coll. on restrictive measures against certain serious conduct applied in international relations	Additional sanctions-related framework for restrictive measures and related enforcement	Utilise Existing Sanctions Legislation; sanctions-related reporting and escalation	Relevant government authorities; FAÚ; Police	Legally relevant, but practical disruption still depends on attribution, evidence, and coordination across institutions.
Anti-Money Laundering Act (Act No. 253/2008 Coll.)	Financial tracing, suspicious transaction reporting, identification of illicit flows, and sanctions-related financial disruption	Freeze Banking Services; Payment Provider; Crypto Exchange and Wallet; Identify Funding	FAÚ; obligated entities such as banks and financial institutions	Particularly relevant for sanctions and financial influence activity, but less useful for broader non-financial influence operations.
Central Register of Accounts Act (Act No. 300/2016 Coll.)	Support for tracing bank account information and financial structures in serious cases	Financial tracing; Identify Funding; ownership and account-link analysis	FAÚ and other competent state authorities	Useful in structured financial investigations, but not a standalone counter-influence mechanism.
Act No. 37/2021 Coll. on registration of beneficial owners	Identification of beneficial ownership and hidden control structures	Identify Ownership Structure (UBO); financial and entity mapping	Courts / registry framework; competent state authorities	Useful for attribution and network mapping, but slower and supportive rather

				than directly disruptive.
Foreign Direct Investment Screening Act (Act No. 34/2021 Coll.)	Screening of certain foreign investments affecting national security or public order	Foreign Finance Legislation; ownership and foreign-link assessment	Ministry of Industry and Trade	Relevant only in specific investment-related cases; not a general-purpose disruption tool for most IO cases.
Criminal Code (Act No. 40/2009 Coll.) – general criminal thresholds	Criminal investigation and prosecution of unlawful conduct linked to influence operations	Prosecutorial action; Police reporting; criminal investigation	Police; Prosecutor's Office; courts	Most IO activity does not meet criminal thresholds, making this pathway important but limited in scope.
Criminal Code – Section 184 (defamation)	Legal action in cases involving serious reputational harm and false statements	Defamation actions; complaint-based proceedings	Courts; complainants; prosecutors in relevant cases	Defamation exists as a legal pathway, but it is not a central state-led disruption mechanism and is often pursued through civil or complaint-based routes.
Criminal Code – Section 318a ("Unauthorised activity for a foreign power")	Foreign interference and collaboration with foreign power activities affecting Czech interests	Invocation of Foreign Interference Legislation; Collaboration with Foreign Intelligence Services Legislation	Police; Prosecutor's Office, Intelligence services	The law is new and operational practice remains limited. It is potentially important, but still relatively untested.
Criminal law provisions on hate speech / incitement / extremist content	Disruption of illegal hate speech, incitement to violence, Holocaust denial, and related extremist content	Hate Speech; Incitement to Violence; Report Illegal Content; Police reporting	Police; Prosecutor's Office; courts	Requires content to cross criminal thresholds. Many influence incidents remain below that threshold and therefore do not trigger rapid intervention.
Terrorism-related provisions under the Criminal Code	Disruption of terrorist content or terrorist-linked material	Terrorist Content; Report Illegal Content; legal escalation	Police; Prosecutor's Office; relevant security bodies	Narrow scope, relevant only where content or actors meet terrorism-related legal definitions.
GDPR (EU) and Act No. 110/2019 Coll. on personal data processing	Data misuse, privacy violations, impersonation, unlawful profiling, and	Privacy & Data Protection Violations; GDPR complaints; The Right to be Forgotten	Data protection authority and courts; relevant platforms/search engines	Useful where personal data misuse is central to the case, but not a general anti-

	search delisting requests			disinformation instrument.
Copyright Act (Act No. 121/2000 Coll.)	Disruption of copied, manipulated, or reused protected content	Copyright takedown; Report Copyright Infringement	Rights holders; courts; platforms	Useful in specific cases involving protected content, but narrow and dependent on ownership rights and legal classification.
Intellectual property legislation (including Act No. 206/2000 Coll., Act No. 441/2003 Coll., Act No. 527/1990 Coll.)	Disruption of trademark misuse, counterfeit branding, and related IP violations	Intellectual Property Infringement	Rights holders; Police economic crime units; courts; prosecutors in relevant cases	Narrow and case-specific. Can support disruption where branding or protected assets are misused, but is not a general IO response pathway.
Electoral legislation – campaign and campaign finance rules	Election-period restrictions and oversight of campaign conduct, financing, and transparency	Political Advertisement Transparency Legislation; election-related reporting; campaign finance scrutiny	Office for the Supervision of the Financial Management of Political Parties and Political Movements (UDHPSH)	Relevant mainly in electoral periods and campaign contexts. It is time-bound and focused on electoral compliance rather than broader IO response.
Law No. 234/2025 Coll. – election-period restrictions	Limited restrictions related to late-stage campaign conduct, polling publication, and agitation near polling locations	Silence Period-related enforcement; election-related reporting	UDHPSH and relevant authorities specified by law	No general electoral silence period; a limited pre-election 3 day moratorium applies.
Political advertising transparency / third-party campaign rules	Oversight of transparency in campaign spending and third-party political advertising	Political Advertisement Transparency Legislation; oversight of third-party campaign actors	UDHPSH	Useful where covert or unlawful campaign financing or political advertising can be shown. Enforcement speed varies depending on context.
Electronic Communications Act / telecom regulatory framework	Sectoral intervention where telecoms, domains, or service-provider relationships are relevant	Domain-related escalation; provider contact within regulatory scope	ČTÚ	Relevant mainly in technical or provider-facing cases. Does not create a general pathway for content-level disruption.
Audio-visual / media regulatory framework	Limited sectoral relevance where broadcast or regulated media	Sectoral escalation in relevant regulated media contexts	Relevant media regulator / sectoral authority	Czechia does not rely on a broad audiovisual regulator as a core

	rules are engaged			IO disruption actor. Relevance is narrower than in some other national contexts.
European Media Freedom Act (EMFA)	Structural media-governance relevance in the media environment	Regulatory escalation; media-governance related engagement	Relevant Czech authorities / EU framework	More relevant to structural media governance than to rapid-response disruption.
EU AI Act	Potential future relevance for harmful AI-enabled content and systems	AI-related regulatory escalation in relevant cases	Competent authorities as designated	Not yet a primary operational disruption tool in Czech practice.
Secret service / intelligence laws	Classified security-sector activity in cases involving state-sponsored threats, foreign influence, or national security risks	Security-sector escalation; intelligence handling	Intelligence services within mandate	These tools may be operationally significant, but their use is not generally visible and does not form part of a transparent public workflow.

These instruments do not form a single counter-influence regime. Instead, they provide a set of partial pathways that can be activated depending on whether a case falls within criminal, regulatory, financial, electoral, or platform-related competence. In practice, disruption depends less on the existence of instruments in the abstract, and more on whether a case can be qualified in a way that enables a competent authority to act.

6.5 Cross-Sector Interaction Across the Framework

The DISRUPT Framework is particularly relevant in the Czech context because it helps make visible how a highly distributed set of actors interacts across the three phases of Prepare, Disrupt, and Mitigate. While Czechia has a large and capable ecosystem - spanning government, civil society, academia, and media - these actors operate within distinct mandates and are not systematically connected through a single operational workflow. The framework therefore provides a structure for understanding how actions can be sequenced and combined across sectors.

6.5.1 PREPARE

In Czechia, PREPARE-phase activities are primarily analytical, research-driven, and distributed across both governmental and non-governmental actors. Measures such as information collection, social listening, narrative monitoring, behavioural analysis, content archiving, and evidence preservation are carried out by a combination of ministries, intelligence services, civil society organisations, academic institutions, and investigative journalists.

Government actors such as CHH contribute to monitoring and threat assessment, particularly in areas linked to national security and foreign influence. However, much of the observable and publicly

actionable analysis is produced by civil society organisations, think tanks, and academic partners, including actors such as AMO, PSSI, CEDMO, and university-based researchers. Media actors also play a key role in identifying and documenting emerging narratives.

The objective at this stage is to move from initial observation to structured assessment and attribution. However, as inputs are generated across a wide network of actors and no single institution is responsible for consolidating them into an operational trigger, early-stage coordination remains largely informal and informational rather than procedural.

6.5.2 DISRUPT

The DISRUPT phase in Czechia is led by whichever authority holds competence over the qualified case, resulting in a fragmented but functionally diverse response landscape. Depending on the nature of the influence operations, this may involve law enforcement bodies, prosecutors, financial intelligence authorities, regulatory actors, security services, or platform-facing mechanisms.

Relevant measures include reporting content or accounts to platforms, engaging infrastructure providers (such as hosting or domain services), invoking DSA-related procedures, activating sanctions or anti-money laundering frameworks, involving security services in cases of foreign interference, or pursuing criminal or administrative action where thresholds are met.

In practice, this phase is strongly conditioned by legal qualification. Most institutions can act only when an activity clearly falls within their formal mandate, such as criminal offences, financial violations, or sanctions breaches. As a result, many influence operations - particularly those involving coordinated inauthentic behaviour without a clear legal violation - do not trigger direct intervention.

This creates a structural gap between detection and disruption. Even where high-quality analytical outputs exist, the absence of a clear legal or regulatory entry point can delay or prevent operational response. In addition, the limited enforcement capacity of regulatory actors, particularly in relation to platform governance under the Digital Services Act, further constrains rapid disruption.

6.5.3 MITIGATE

Mitigation in Czechia is more consistently applied than disruption and is largely driven by civil society, media, and analytical actors, with selective involvement from government communication structures. Measures such as fact-checking, media reporting, public exposure, narrative clarification, and awareness-raising are widely used across the ecosystem.

Fact-checking organisations (such as Demagog.cz), investigative journalists, and independent media outlets play a central role in countering false or manipulative narratives. Civil society organisations contribute through public reporting, advocacy, and educational initiatives, including media literacy and pre-bunking efforts.

Government communication capacity has shrunk recently due to strategic communications units ending their operation. Their agenda has formally been returned to press and communications

departments Broader mitigation of influence operations outside acute crises relies heavily on non-governmental actors.

As a result, mitigation often functions as the primary practical response in cases where legal or regulatory disruption is not available or is delayed. Public explanation and exposure therefore become key tools, even though they typically occur later in the lifecycle and do not directly disrupt the underlying operational infrastructure of influence activities.

6.6 Fragmentation and Coordination

Both the institutional and non-governmental response landscape in Czechia are structurally fragmented. Expertise, authority, and access are distributed across a large number of actors, reflecting a mature but decentralised ecosystem. However, the mechanisms linking these actors remain weakly formalised and often depend on informal networks, personal relationships, and case-by-case coordination.

Several recurrent coordination gaps can be identified:

- no shared incident definition across actors and sectors;
- no common escalation thresholds linking analytical outputs to operational response;
- no predefined routing sequence between institutions;
- limited structured fallback mechanisms from disruption to mitigation;
- and limited systematic integration of lessons learned into future operational practice.

This fragmentation does not imply a lack of capacity. On the contrary, Czechia demonstrates an extensive multi-stakeholder ecosystem, with strong analytical, research, and media capabilities, and a significant network of civil society and academic actors. These actors provide resilience, continuity, and a degree of independence from political cycles.

However, the absence of shared operational triggers and structured workflows means that these capacities are not consistently connected. As a result, response timing can be uneven, cases may stall between detection and action, and mitigation measures often compensate for delayed or unavailable disruption.

The DISRUPT 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 across sectors;
- linking analytical outputs to institutional escalation pathways.

In the Czech context, effectiveness depends not on reducing fragmentation, but on coordinating across it. The framework provides a practical structure for doing so, while preserving the strengths of a decentralised, whole-of-society response model.

6.7 Operational Implication

In Czechia,

- **PREPARE measures** are extensive and distributed across a wide network of civil society, academic, media, and specialised government actors, providing strong analytical and monitoring capacity.
- **DISRUPT measures** are available but highly dependent on legal qualification, institutional mandates, and case-specific routing, with limited direct enforcement capacity in platform and regulatory pathways.
- **MITIGATE measures** are consistently applied, largely driven by civil society, media, and fact-checking actors, and often serve as the primary response where disruption is delayed or unavailable

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 Czechia

Consultation findings indicate that the response to influence operations in Czechia develops through a highly distributed, multi-actor process, rather than through a unified or linear institutional workflow. While a wide range of activities exists across the PREPARE, DISRUPT, and MITIGATE phases, these are not consistently connected through shared operational sequencing. Instead, actions are primarily triggered by institutional mandates, legal thresholds, and sector-specific competences, rather than by a coordinated lifecycle approach.

In practice, detection, assessment, disruption, and communication are carried out by different actors operating across civil society, academia, media, and state institutions. Analytical and monitoring functions are widely distributed, with a particularly strong role played by non-governmental and research actors, while disruption depends on whether a case can be qualified within legal, regulatory, financial, or security frameworks.

The transition between phases is therefore conditional rather than automatic. Cases move from PREPARE to DISRUPT only when a competent authority can act within its mandate. Where this qualification is unclear, not met, or delayed, cases may stall or shift directly into mitigation measures such as public communication, media exposure, or fact-checking.

This results in a response model where sequencing is not predefined, and where mitigation often compensates for limitations in enforcement or regulatory intervention.

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; Monitoring by CHH, ČTÚ (within mandates); Inputs from civil society (e.g. AMO, PSSI), academia (CEDMO, universities), and media	Initial signal detection and analytical observations
PREPARE	Analysis & Assessment	Document; Create Evidence Repository; Actor Mapping; Identify Pattern of Behaviour; CIB Detection (primarily by civil society and researchers); Attribution (where possible); Legality assessment	Analytical qualification of the case
PREPARE → DISRUPT	Inform	Send Alert; Briefing; Direct outreach to authorities (e.g. Police, FAÚ, ČTÚ) or platforms; informal coordination between actors	Case routed to competent authority, platform, or relevant stakeholder
DISRUPT	Competence Qualification	Determining whether the case fits criminal (Police / Prosecutor), financial (FAÚ), security (Police, MoI), regulatory (ČTÚ), or platform pathway	Decision on whether disruption is possible within existing mandates

DISRUPT	Enforcement / Action	Report Content; Report Channel; Platform engagement; DSA escalation (via ČTÚ or EU level); Criminal investigation (Police / Prosecutor); Financial investigation (FAÚ); Security-service involvement; limited sanctions-related action	Enforcement action, referral, or platform response (where applicable)
MITIGATE	Communication Actions	Public communication; Media exposure; Fact-checking (Demagog.cz, CEDMO); Investigative reporting; Narrative clarification; Awareness campaigns; civil society advocacy	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.
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) represents one of the most operationally complex and resource-intensive types of influence activity in Czechia. Unlike clearly illegal content, CIB typically operates in a grey zone, where disruption depends less on direct legal intervention and more on platform enforcement, analytical attribution, and sustained monitoring.

The Czech ecosystem demonstrates strong capabilities in detection and analysis, primarily driven by civil society, research organisations, and independent analysts, with partial involvement from state actors such analytical units within the Ministry of the Interior. Actors such as PSSI, the Association for International Affairs, Investigace.cz, and Voxpot play a key role in identifying behavioural patterns, mapping networks, and documenting coordinated activity.
However, the transition from analysis to disruption remains inconsistent. Many disruption pathways depend on:

- platform responsiveness and willingness to act on reported CIB;
- the ability to attribute activity to hostile foreign, coordinated, or state-linked actors;
- whether the case meets legal, regulatory, or policy thresholds for intervention within Czech law and EU frameworks.

As a result, disruption is often indirect, delayed, or reliant on external actors (particularly platforms and EU-level mechanisms), while mitigation - especially through communication, exposure, and public awareness - remains a consistently applied response.

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

Table 3. CIB workflow overview

Phase	What this typically involves in Czechia	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through social listening, narrative monitoring, behavioural tracking, and collection of publicly available content. Detection is largely	Preserve evidence, document coordinated behaviour systematically, and	1.1 Find and Collect Publicly Available Content, 1.2 Narrative Monitoring, 1.3 Account Monitoring, 1.4 Behavioural Monitoring, 2.1 Observable list,

	driven by civil society, investigative journalists, and academic actors, with partial input from state bodies such as CHH and the Ministry of the Interior. Cases are documented through observable lists, scraping, and archiving.	establish patterns (accounts, narratives, infrastructure) before assets are removed or altered.	2.2 Offline Archiving, 2.3 Online Archiving, 2.4 Hash Evidence
PREPARE → DISRUPT	Cases are assessed for inauthentic behaviour, harm, attribution, and possible legal or platform-based intervention. In Czechia, this includes identifying infrastructure, ownership, amplification networks, and potential foreign links. Legal qualification is often limited unless content violates specific provisions (e.g. hate speech, defamation, sanctions).	Determine whether the case meets thresholds for action and identify viable escalation routes-primarily platform-based, but also regulatory, financial, or security-related where applicable.	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 a combination of platform reporting, infrastructure targeting, financial disruption, and limited governmental engagement. In Czechia, disruption frequently relies on platform enforcement, DSA-related escalation to the European Commission, and selective involvement of institutions such as police, or regulators. Direct state-led disruption remains limited.	Use the most effective available pathway—primarily platform and infrastructure-based—while combining regulatory, financial, and institutional measures where feasible.	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 Political Advertising Rules, 10.2 Ministry of Foreign Affairs, 10.3 Security Services, 10.4 Interior Ministry, 10.5 Prosecutor
MITIGATE	Where disruption is limited or delayed, mitigation is carried out through public reporting, media exposure, advocacy, and awareness campaigns. Czech media, investigative outlets, and civil society play a central role in exposing networks and	Reduce impact through transparency, strengthen public resilience, and apply reputational pressure on platforms and enabling actors.	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

	explaining manipulation techniques.		

11. Application to Sanctions-Related Cases

Sanctions-related influence operations in Czechia represent a distinct category of cases where legal frameworks are more clearly applicable than in other types of information manipulation. Unlike CIB, sanctions circumvention involves the dissemination, amplification, or monetisation of content originating from sanctioned entities, which is prohibited under EU law. This creates stronger legal grounds for disruption, but operationalisation remains complex and resource-intensive.

The Czech ecosystem demonstrates particularly strong capabilities in **detection, documentation, and analytical validation**, driven by a dense network of civil society organisations, academic institutions, and investigative journalists. Actors such as AMO, PSSI, Investigace.cz, and CEDMO contribute significantly to identifying republication patterns, tracing content provenance, and linking proxy actors to sanctioned entities. Technical expertise is further supported by cybersecurity actors and independent analysts.

Detection typically relies on:

- tracing content origin and republication chains;
- identifying coordinated amplification patterns;
- linking actors, infrastructure, or funding streams to sanctioned entities;
- building legally robust evidence through archiving, hashing, and comparative analysis.

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

- the ability to **prove origin and attribution** to a sanctioned entity;
- the **availability and responsiveness of platforms and service providers**;
- the identification of **intermediary infrastructure** (hosting, domains, payment systems);
- engagement with **competent national authorities** (e.g. FAÚ, Police) or EU-level mechanisms.

Disruption pathways in Czechia are legally grounded but institutionally fragmented. Available measures include:

- reporting sanctioned content and channels to platforms;
- targeting infrastructure providers (hosting, domain registrars, CDN, SSL);
- disrupting monetisation through ad networks, payment providers, and financial institutions;
- invoking EU-level mechanisms such as the Digital Services Act (DSA), including out-of-court dispute settlement;
- engaging financial intelligence mechanisms (FAÚ) and anti-money laundering frameworks;
- escalating cases to security services or law enforcement where thresholds are met.

However, **government engagement is less centralised and less operationalised**. Czechia does not have a dedicated counter-FIMI authority, and ministries have limited direct operational roles in disruption. Security actors contribute primarily within their mandates (counter-intelligence and cybersecurity), and their outputs are often non-public.

As a result, coordination between non-governmental actors and state institutions remains largely **informal, case-dependent, and non-systematised**.

Despite stronger legal grounding, disruption is not always immediate. Many measures - particularly those involving financial investigation, sanctions enforcement, or regulatory escalation - require:

- high evidentiary thresholds;
- formal procedures;
- extended timeframes.

Where enforcement is delayed or unavailable, **mitigation becomes a central operational pathway**. Civil society, media, and academic actors play a critical role in:

- publishing investigative reports;
- conducting fact-checking;
- exposing influence operations;
- applying reputational and public pressure on platforms and service providers.

Overall, sanctions-related cases in Czechia demonstrate a **high-capacity detection and mitigation environment**, but a **less consolidated and slower disruption layer**, with effectiveness dependent on cross-sector coordination, platform compliance, and the ability to translate analytical findings into legally actionable evidence.

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

Table 4. Sanctions workflow overview

Phase	What this typically involves in Czechia	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through monitoring of content suspected to originate from sanctioned entities. Civil society, researchers, and media trace republication patterns, identify proxy actors, and document links between sanctioned sources and local amplifiers. Evidence is preserved through archiving and hashing.	Establish verifiable links between content, actors, and sanctioned entities, ensuring evidence meets legal and platform standards.	1.1 Find and Collect Publicly Available Content, Social Listening, Scraping, 2.1 Observable List, 2.2 Online Archiving, 2.3 Offline Archiving, 2.4 Hash Evidence
PREPARE → DISRUPT	Cases are assessed for sanctions relevance, including attribution,	Determine whether the activity	3.1 Analyse Content, Identify Source, Identify Funding,

	ownership, funding, or infrastructural links. Legal qualification is required to determine whether disruption pathways are available.	constitutes sanctions circumvention and identify viable disruption vectors (platform, infrastructure, financial, regulatory).	Identify Infrastructure, 4.2 Legality, 4.3 Attribution, Foreign Interference
DISRUPT	Action is taken through available legal and technical mechanisms. Practitioners engage platforms, infrastructure providers, and financial intermediaries. Escalation to authorities (FAÚ, Police, ČTÚ) occurs where thresholds are met, while EU-level mechanisms may be used where national enforcement is limited.	Apply disruption measures across infrastructure, financial flows, and platforms, while navigating fragmented institutional mandates.	6.1 Hosting, 6.2 Report Content, 6.3 Contact Platform Representatives, 7.2 Report Channel, 8.1 Demonetise Assets, 8.3 Freeze Banking Services, 9.1 DSA, 9.2 Sanctions Enforcement, 9.3 AML / Foreign Finance, 10.3 Security Services, 10.4 Financial Intelligence Units, 10.8 Police
MITIGATE	Where disruption is delayed or partial, actors rely on exposure and awareness. Media, NGOs, and academic actors publish findings, conduct fact-checking, and mobilise public and political attention to increase pressure on platforms and institutions.	Increase transparency, build public awareness, and apply reputational pressure to compensate for limited enforcement speed.	4.1 Publish Report, 4.3 Briefing, 11.1 Engage Political Actor, 11.2 Engage Advocacy Actors, 11.5 Engage Journalist, 12.1 Media Exposure

12. Minimum Operational Readiness

To apply the Toolkit effectively in Czechia, institutions and practitioners should ensure the availability of basic coordination capabilities, alongside clear actions that operationalise them within an already distributed and largely decentralised response ecosystem.

In the Czech context, minimum operational readiness is particularly important because relevant capabilities exist across civil society, research organisations, media actors, and selected state institutions, but they are not consistently connected through predefined triggers, workflows, or escalation mechanisms. Unlike more centralised systems, Czechia relies on a mixed ecosystem where analytical detection is often non-governmental, while enforcement capacities sit within state institutions.

Readiness therefore depends not only on institutional capacity in isolation, but on the ability to receive signals, document cases, route them appropriately, coordinate across mandates, and activate communication or mitigation where disruption is delayed, platform-dependent, or legally constrained.

Table 5. Minimum Readiness Capability

Capability	Description	Operational actions (what actors can do)
Signal intake	Mechanism for receiving and reviewing alerts	Receive alerts from civil society organisations, researchers, investigative journalists, platforms, or international partners; where relevant inputs may also come from the Ministry of the Interior; screen incoming signals; prioritise cases based on risk (elections, foreign interference, sanctions relevance, public harm); acknowledge receipt and initiate initial review.
Case tracking	Basic documentation of cases	Open a case file; record key information (source, content, actors, platforms, timelines, possible legal relevance); maintain structured documentation and evidence repositories; track case progression; document referrals between civil society, media, and institutional actors.
Routing clarity	Understanding of institutional competences	Identify competent actors depending on case type: Ministry of the Interior (incl. Centre Against Hybrid Threats) for disinformation monitoring; Police or prosecutors for criminal thresholds; Financial Analytical Office for financial/sanctions-related aspects; Czech Telecommunications Office as Digital Services Coordinator; NUKIB for cybersecurity-related analysis; platforms for CIB and content moderation; route cases accordingly.
Evidence standards	Consistent approach to documentation	Collect and preserve evidence (URLs, screenshots, metadata, archived content); apply hashing where needed for legal robustness; structure evidence to support platform reporting, regulatory escalation, or potential legal proceedings; ensure traceability and verifiability of findings.
Coordination channels	Ability to engage relevant actors	Engage relevant stakeholders (platforms, regulators, ministries, civil society, media); organise coordination calls where needed; share information securely; align actions across actors (e.g. platform reporting combined with media exposure or regulatory escalation); compensate for lack of formal coordination mechanisms through ad hoc collaboration.
Communication capacity	Preparedness for public messaging	Prepare reports, alerts, and briefings; determine when to escalate to public communication; engage journalists, investigative outlets, and civil society initiatives; where appropriate, coordinate messaging with government actors; ensure communication is timely, evidence-based, and clearly explains manipulation techniques.

Learning mechanisms	Ability to capture lessons learned	Conduct post-case reviews across participating actors; identify coordination gaps and effective practices; update internal workflows; share lessons informally across networks; integrate insights into future monitoring, training, and preparedness activities.

These elements support the Framework's role as a coordination standard and operational reference. In Czechia, they are particularly important because the main operational challenge is not the absence of relevant actors, but the absence of structured coordination between them. Minimum readiness therefore means ensuring that decentralised capacities - across civil society, media, and state institutions - can be connected quickly enough to enable timely, proportionate, and context-appropriate responses across the lifecycle of influence operations.

13. Conclusion

The application of the DISRUPT Framework in Czechia highlights a response ecosystem that is functionally capable but structurally decentralised. Detection, analysis, disruption, and communication capacities are all present, but they are distributed across civil society, media, and state institutions without a consistently shared operational sequence.

This creates a system that is adaptable and analytically strong, but uneven in its ability to translate findings into timely and coordinated action. In particular, disruption remains dependent on external actors - especially platforms and EU-level mechanisms - while legal and institutional pathways are applied selectively and often require high evidentiary thresholds.

Within this context, the Framework provides value not by introducing new capacities, but by connecting existing ones. It enables practitioners to move from isolated actions toward a more structured approach by:

- linking detection to actionable pathways;
- clarifying when and how escalation is possible;
- supporting parallel use of platform, regulatory, and communication measures;
- and identifying where mitigation should be activated early when disruption is constrained.

For Czechia, effectiveness does not depend on centralisation, but on coordination across a distributed landscape. Strengthening shared triggers, improving routing clarity, and enabling faster alignment between actors are therefore more critical than institutional expansion.

In practice, the Framework serves as a common operational logic that allows diverse actors - ranging from civil society and investigative media to institutions such as the Ministry of the Interior - to act in a more connected and predictable way across the lifecycle of influence operations.

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 Czechia

Phase	Function	Measure	Sub-measures
PREPARE	Data Collection and Documentation	Information Collection	Find and Collect Publicly Available Content; Social Listening (LetsData, Evidence Ninja, Alliance4Europe access); Scraping (Czech OSINT researchers); Threat Intelligence Monitoring Tool (Gerulata); Agent-based Crawling; Gain Proprietary Intelligence / Infiltration (journalistic, legally constrained); Purchase Data; Interview (investigative journalism); Freedom of Information Request
PREPARE	Data Collection and Documentation	Document	Observable List; Create Evidence Repository; Offline Archiving; Online Archiving; Screenshots (hashed for legal robustness); 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 (PSSI, AMO, CIS, Voxpot, Investigace.cz, academia); CIB Algorithm; Actor Mapping; Analyse Content; Identify Deepfake; Identify AI-rewritten Content; Identify Identical Content; Identify Source of Content; Identify Illegal Content (Czech Criminal Code, GDPR, sanctions law)
PREPARE	Analysis and Assessment	Assessment	Inauthentic Behaviour; Legality (Criminal Code, copyright, GDPR, sanctions); 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 (NUKIB, independent experts); URL Analysis; IP Analysis; Software Components Analysis; Services; Identify AI Generation Tool; Fact-check (Demagog.cz, Ověřovna, CEDMO); 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 (mostly civil enforcement in Czechia); 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 (Financial Analytical Office – FAÚ); Payment Provider; Crypto Exchange and Wallet
DISRUPT	Report Through Established Mechanisms	Regulatory Action	DSA; DSA Out-of-court Dispute Settlement (ACE, Central European Appeals Hub); Leveraging DSA Systemic Risk Obligations (Art. 34–35, via EC); DSA Trusted Flagger (limited implementation); Digital Service Coordinator Oversight (ČTÚ – limited mandate); EU Sanctions for De-platforming and Financial Disruption; Propose New Sanctions (via EU/EEAS); Utilise Existing Sanctions Legislation (Law 69/2006 Sb., 1/2023 Sb.); Invocation of Foreign Interference Legislation (§318a Criminal Code); Foreign Finance Legislation (AML Act, FDI Screening Act); Collaboration with Foreign Intelligence Services Legislation; Foreign Agent Legislation (emerging, untested); Silence Period (limited electoral restrictions, UDHPSH); Political Advertisement Transparency Legislation (UDHPSH); GDPR; Defamation; Intellectual Property Infringement; Terrorism Laws
DISRUPT	Government Engagement	Government Collaboration	Counter FIMI Agency (no dedicated body); Ministry of Foreign Affairs (limited IO role); Security Services; Interior Ministry (Centre Against Hybrid Threats – CHH); Audio-Visual Regulator / Digital Service Coordinator (ČTÚ); Prosecutor (Státní zastupitelství); Police (NCTEKK); Military (limited role); Electoral Authorities (UDHPSH); Digital Service Coordinator (ČTÚ); EU Institutions (European Commission, EEAS); National Cyber Authority (NÚKIB); Ombudsman; Data Protection Authority (UOOU); Consumer Protection Bodies
DISRUPT	Pressure	Public Pressure	Engage Political Actor; Engage MEP; Engage MP; Engage Political Party (e.g. TOP09, STAN, Piráti); Engage Council / Minister; Engage Advocacy Actors (Odolné Česko, Demokratické pojistky, etc.); Engage Advocacy Network; Engage Activist Group; Engage Public; Engage Private Sector; Engage Interest Group; Engage Company; Engage Journalist (Seznam, Voxpot, Investigace.cz, Deník N, etc.); Written Question to Institutions; 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 (Demagog.cz, Ověřovna, CEDMO, Manipulátoři.cz); 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