DISRUPT FRAMEWORK

POLAND

TOOLKIT

Alliance 4Europe

CEE Digital Democracy Watch

TABLE OF CONTENTS

FOREWORD 3
1. INTRODUCTION 4
2. THE DISRUPT FRAMEWORK 5
3. THE THREE PHASES OF THE DISRUPT FRAMEWORK 5
3.1 PREPARE 6
3.2 DISRUPT 7
3.3 MITIGATE 8
3.4 RELATIONSHIP BETWEEN THE PHASES 9
4. HOW TO USE THIS TOOLKIT 9
5. PURPOSE AND SCOPE 10
6. NATIONAL RESPONSE STRUCTURE IN POLAND 10
6.1 SECTORAL BREAKDOWN OF THE RESPONSE ECOSYSTEM 10
6.2 DIFFERENTIATION WITHIN CIVIL SOCIETY 11
6.3 TECHNOLOGY AND OSINT AS A CORE OPERATIONAL LAYER 12
6.4 REGULATORY AND INSTITUTIONAL CONTEXT 12
6.5 CROSS-SECTOR INTERACTION ACROSS THE FRAMEWORK 16
6.5.1 PREPARE 16
6.5.2 DISRUPT 16
6.5.3 MITIGATE 16
6.6 FRAGMENTATION AND COORDINATION 17
6.7 OPERATIONAL IMPLICATION 17
7. CURRENT OPERATIONAL PATTERN IN POLAND 18
8. STANDARD NATIONAL WORKFLOW 19
9. APPLICATION TO COORDINATED INAUTHENTIC BEHAVIOUR 20
10. APPLICATION TO SANCTIONS-RELATED CASES 23
11. MINIMUM OPERATIONAL READINESS 25
12. CONCLUSION 26
Annex 1: Minimum Questions for Initial Case Handling 29
ANNEX 2: OVERVIEW OF THE DISRUPT FRAMEWORK IN POLAND 30

Foreword

Poland occupies a central position in the current European security environment. As a frontline state in the context of Russia's war against Ukraine, and as a key political, logistical, and humanitarian hub, it is exposed to sustained and evolving influence operations. These activities are not limited to electoral periods but form part of a broader landscape of hybrid threats, often intersecting with sanctions circumvention, economic pressure, and information manipulation targeting public trust and social cohesion.

Beyond their immediate informational impact, such operations contribute to polarisation, undermine trust in institutions, and can weaken Poland's social cohesion over time. This context makes the question of operational response both timely and critical, not only as a matter of security but also as a question of democratic resilience.

In Poland, civil society organisations play a particularly important role in this landscape. They are often at the forefront of detection, analysis, and early warning, identifying emerging narratives, documenting cases, and initiating response processes. Their work complements that of public institutions and independent experts, and forms a critical part of the national response ecosystem.

At the same time, effective disruption depends on how these efforts connect with the broader system. Influence operations routinely span platforms, jurisdictions, and sectors, requiring coordination between civil society, public authorities, technology companies, regulators, and financial actors. While Poland has developed strong capabilities across these domains, coordination mechanisms – such as the Resilience Council under the Ministry of Foreign Affairs of Poland – provide an important basis for aligning responses across stakeholders. However, the effectiveness of response ultimately depends on how these efforts are operationalised in practice.

The DISRUPT Toolkit is designed to support this coordination. It does not introduce new mandates or institutional reforms, but provides a structured way to organise existing capabilities, clarify roles, and sequence actions across the lifecycle of a case – from early detection to disruption and mitigation. By organising available measures into a shared operational logic, and by introducing a common vocabulary and repeatable workflows, the Toolkit aims to help practitioners understand *what can be done, when it can be done, and who can act*. It is intended as a practical resource to support cooperation across sectors, improve predictability in responses, and strengthen the overall resilience of the system.

This national adaptation draws on multi-stakeholder engagement in Poland and reflects the specific operational challenges identified by practitioners. By offering a shared Framework, it aims to support more predictable, timely, and coordinated responses to influence operations, while reinforcing the contributions of civil society and enabling stronger collaboration across sectors.

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

Saman Nazari, Alliance4Europe **Jakub Szymik, CEE Digital Democracy Watch**

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 Poland, this challenge is shaped by the country's geopolitical position as a frontline state in the context of Russia's war against Ukraine. Poland has been a primary target of pro-Kremlin information manipulation, while also serving as a key political, military, and humanitarian hub in support of Ukraine. As a result, influence operations are persistent, multi-layered, and often closely linked to broader hybrid threats, including sanctions evasion, financial flows, and infrastructure dependencies.

In practice, detection, analysis, and early response are often driven by civil society organisations, independent researchers, and media actors, while key points of disruption are distributed across platforms, infrastructure providers, financial and regulatory actors, and public authorities, rather than concentrated within a single sector. Public authorities play an essential role in legal enforcement, attribution, and coordination, but effective response depends on how these actors operate together.

The Polish ecosystem demonstrates strong analytical and monitoring capabilities, developed through sustained exposure to high-volume influence operations – linked in part to Poland's role as a frontline state in the context of Russia's war against Ukraine – as well as through election-related response and international cooperation. Despite this extensive operational experience, competences remain distributed across multiple institutions, and responses are often triggered only once legal or procedural thresholds are met. Coordination typically occurs on a case-by-case basis, rather than through structured, pre-defined workflows, creating a gap between detection and operational disruption- particularly in cases that fall outside clearly defined legal categories.

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

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

2. The DISRUPT Framework

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

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

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

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

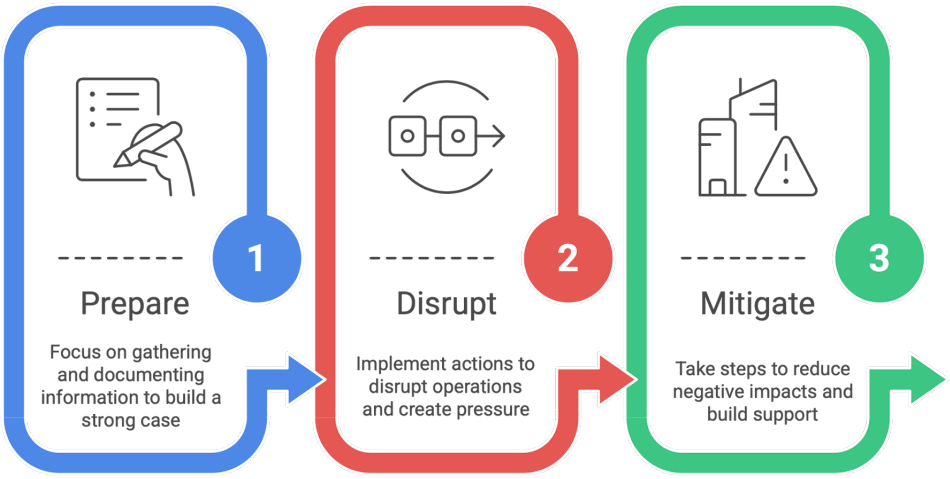
A central feature of the Framework is the use of decision points that help determine when a case has developed sufficiently to move from preparation into disruption, and when mitigation needs to be activated because disruption is delayed or insufficient. In this way, the Framework helps practitioners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

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

This Toolkit adapts that general framework to the Polish 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.

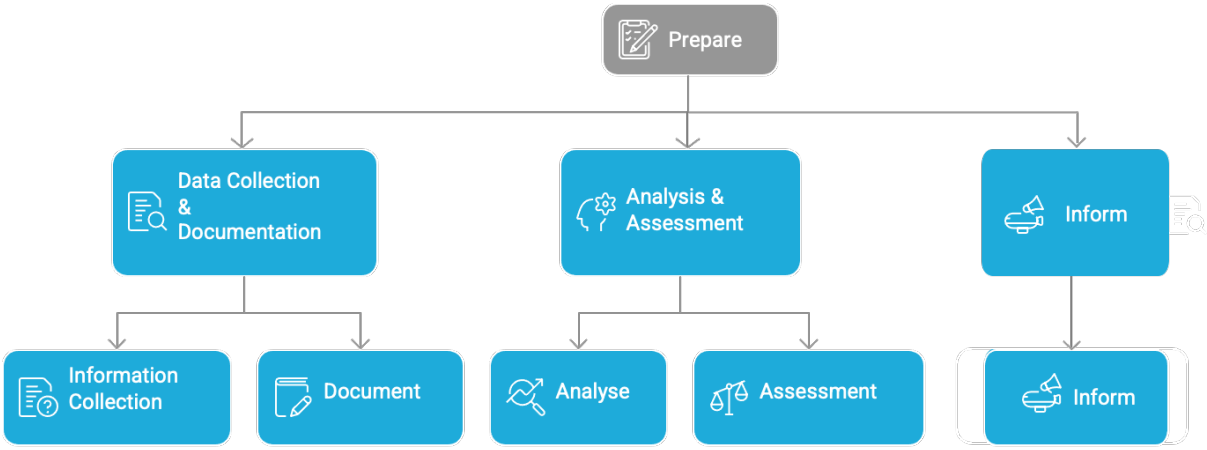
3.1 PREPARE

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**.



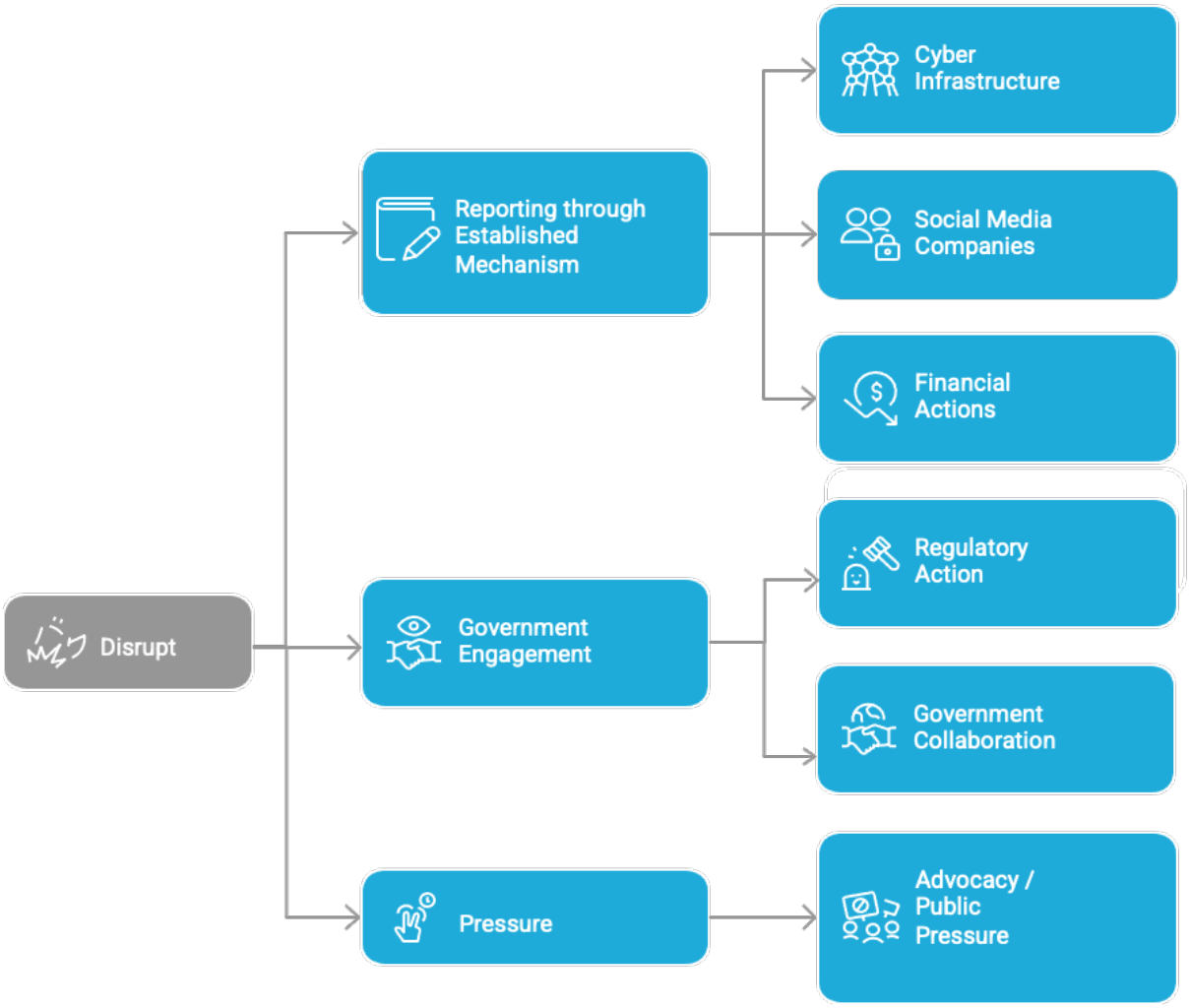
Outputs of the PREPARE phase typically include:

- 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**.

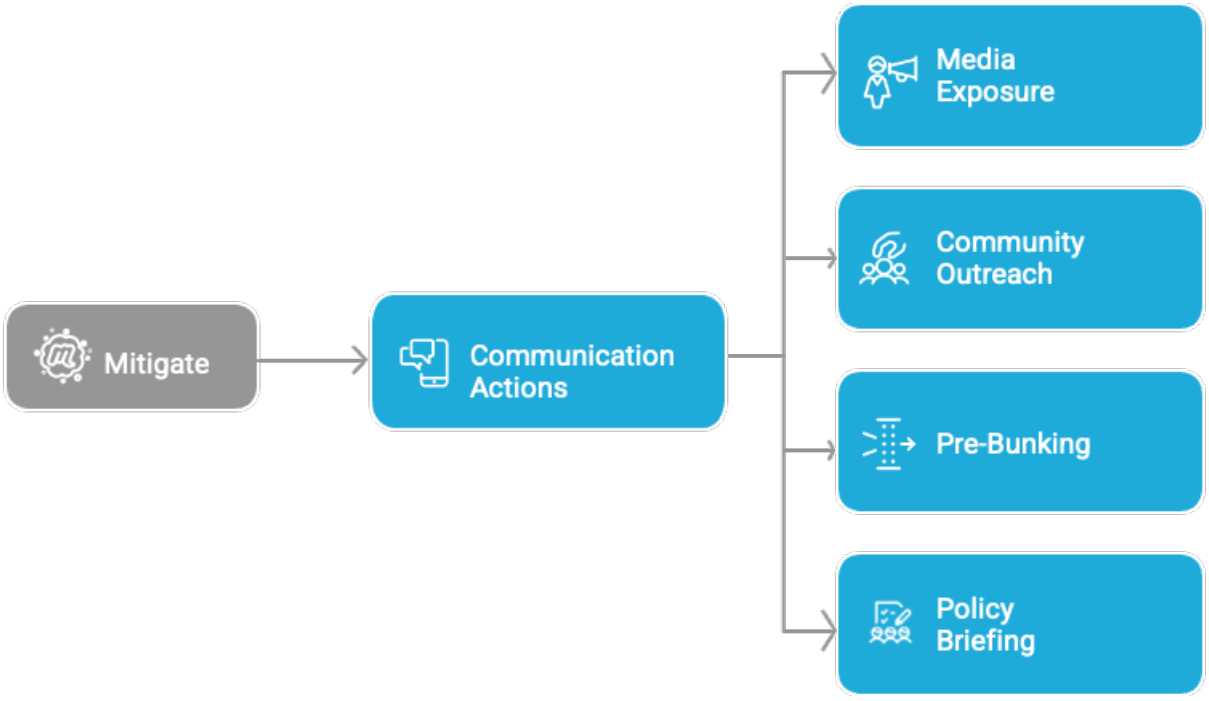
The selection of measures depends on:

- 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 Poland 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 Poland

Poland's response to influence operations is characterised by **a highly diversified, multi-sectoral ecosystem, combining public institutions, civil society, academia and media actors**.

Competences are formally distributed across government bodies, including analytical monitoring (NASK), law enforcement, diplomatic actors (MFA), and sectoral regulators. However, **operational response remains fragmented**, with institutions acting within narrow legal mandates and coordination occurring on a case-by-case basis rather than through a unified workflow.

At the same time, core inputs in the PREPARE phase – detection, monitoring, and documentation – are largely generated by NASK but also civil society, researchers, and media actors, while disruption sits with regulators, and government authorities.

As a result, effective response depends on linking distributed detection capacity to institutional intervention pathways, rather than centralising functions.

6.1 Sectoral Breakdown of the Response Ecosystem

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

- **Government and regulatory authorities**
  Provide the principal pathways for formal disruption, enforcement, diplomatic response, and regulatory action. This includes actors such as NASK, the Ministry of Foreign Affairs, the

Ministry of Interior and Administration, the Office for Electronic Communications, and other sectoral or enforcement bodies. Their relevance lies primarily in the DISRUPT phase, where legal authority and institutional legitimacy are required to act.

- **Civil society organisations**
  Form the largest mapped cohort in the ecosystem. Their size and diversity are operationally significant because they provide much of the monitoring, documentation, analysis, fact-checking, and advocacy capacity that feeds into the PREPARE phase. They also contribute to mitigation by supporting public awareness, public pressure, and structured engagement with institutions and platforms. The range of actors within this category helps ensure that ethical, legal, technical, and human-rights perspectives are represented in the response model.
- **Academic institutions**
  Contribute methodological validation and analytical expertise including institutions such as University of Warsaw and Kozminski University. Their role is particularly relevant in refining assessment methods, supporting research-based analysis, and helping translate emerging findings on influence operations into operationally useful frameworks.
- **Media and journalism actors**
  Provide both verification, exposure and public pressure functions. They support investigation, fact-checking, public reporting, and narrative clarification, and are therefore relevant both to preparation and to mitigation. In practice, media actors can also help create pressure when institutional disruption pathways are weak or delayed.

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. The strategic sectoral mapping for Poland **identifies 19 government and regulatory actors, 36 civil society organisations, 14 academic actors, and 12 media and journalism actors,** highlighting both the breadth of the network and the feasibility of a multi-stakeholder response model.

6.2 Differentiation Within Civil Society

Poland has **distributed civil society capability**, but **institutional analytical authority is centralised in NASK.** Within this landscape civil society is not a single functional actor but a large and differentiated ecosystem whose organisations contribute in different ways across the Framework:

- **OSINT and investigative actors** uncover networks, attribution, and infrastructure;
- **Fact-checking organisations** verify narratives and debunk false content (e.g. verification, debunking);
- **Policy and research organisations** provide structured analysis and reporting;
- **Advocacy and legal organisations** support accountability, rights-based oversight, and escalation

Some organisations specialise in social listening, narrative monitoring, and fact-checking. Others contribute legal analysis, human rights expertise, public advocacy, or international coordination. Still

others are better positioned to support public communication, media engagement, or outreach to political and institutional actors.

This differentiation is operationally important because the PREPARE phase depends heavily on capacities that are often strongest outside government. Civil society actors help identify signals, preserve evidence, analyse narratives and behavioural patterns, and build the evidentiary foundation needed for escalation. In some cases they also help bridge gaps between institutional mandates by translating technical or investigative findings into forms that are more actionable for public authorities, journalists, or platform contacts.

At the same time, the diversity of civil society also reflects fragmentation. Expertise is distributed across multiple organisations, and cooperation with institutions is uneven rather than systematically embedded. This means that, while civil society significantly expands national response capacity, its contribution is not always connected to predictable institutional workflows.

6.3 Technology and OSINT as a Core Operational Layer

At the institutional level, analytical capability in Poland is organised around a central technical actor, with NASK serving as the primary hub for monitoring and analysis..

Capabilities include:

- detection of coordinated inauthentic behaviour (CIB);
- monitoring of narratives and information flows;
- analytical assessment and reporting;

However, there is a critical structural limitation:

- CIB detection methodologies are centralised in a single actor (NASK);
- Other institutions lack independent analytical capability;
- This creates a dependency bottleneck in the PREPARE phase.

This contrasts with more distributed OSINT ecosystems seen in other countries.

6.4 Regulatory and Institutional Context

Regulatory and institutional actors in Poland play an important role in the DISRUPT phase, but their **ability to intervene is shaped by legal thresholds, formal competences, and the fragmented distribution of mandates**. Poland has no single authority connecting the PREPARE, DISRUPT, and MITIGATE phases into a continuous operational process. Instead, institutions perform specialised roles: **NASK** monitors and assesses; law enforcement and prosecutors act when criminal thresholds are met; the **Ministry of Foreign Affairs** handles diplomatic attribution and external response, including coordination with initiatives such as the Polish Resilience Council, which brings together government and civil society actors to address international disinformation; the **Ministry of Interior**

and Administration has sanctions-related competences; and communication bodies respond once an issue becomes publicly visible.

This means that disruption is typically triggered not by operational urgency alone, but by whether an incident can be qualified within an existing legal, administrative, diplomatic, or regulatory framework. **Law enforcement bodies** intervene primarily when behaviour constitutes a criminal offence. Administrative measures apply where sanctions, sectoral rules, or other legal instruments are engaged. Diplomatic action is possible in cases of foreign-linked activity that fall within the remit of the Ministry of Foreign Affairs. Communication functions are activated largely after visibility increases or public clarification becomes necessary.

The **Office for Electronic Communications (UKE)** holds an **interim role linked to Digital Services Act coordination**, but its role is limited to liaison and participation in European structures rather than independent content enforcement. Likewise, regulatory and sectoral authorities can act within their formal scope, but do not provide a comprehensive national response pathway.

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

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

Legal / regulatory instrument	Main disruption relevance	Typical measures enabled	Main competent authority / authorities	Key limitation / operational note
Digital Services Act (DSA)	Platform-related disruption, illegal content handling, notice-and-action procedures, systemic risk escalation	Report Content; Reporting T/S Abuse; DSA Notice & Action Mechanism; Leveraging DSA Systemic Risk Obligations (Article 34-35 Reporting); Digital Service Coordinator Oversight	Office for Electronic Communications (UKE) as interim DSC; European Commission in relevant cases; platforms	Poland does not yet have a fully empowered DSC in operational terms. UKE's role remains limited and much action still depends on platform responsiveness rather than rapid national enforcement.
Polish DSA implementation / interim 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	Office for Electronic Communications (UKE); Ministry of Digital Affairs	The workshop findings indicate a coordination role rather than a strong independent enforcement function. This limits speed and direct intervention capacity.
Polish Electoral Code – Article 107 (electoral silence / *cisza wyborcza*)	Election-period restrictions on political communication	Silence Period enforcement; election-related reporting; reporting illegal	National Electoral Office (KBW); relevant electoral authorities; NASK for digital	Relevant mainly during election periods. It is a time-bound instrument rather than a

	and campaign activity	electoral content; platform escalation during election periods	enforcement support	general counter-influence tool.
Law on Political Parties – Article 25	Restriction of foreign financing of political actors	Foreign Finance Legislation; funding scrutiny; escalation where foreign financing supports influence activity	Relevant electoral / finance oversight authorities; potentially prosecutors where offences arise	Applies only where financial support to political actors can be demonstrated. It is narrow and evidence-heavy, not a broad information operation tool.
Polish Penal Code – Article 130	Collaboration with foreign intelligence services / foreign interference with national security implications	Invocation of Foreign Interference Legislation; Collaboration with Foreign Intelligence Services Legislation; prosecutorial and security-service action	Internal Security Agency (ABW); Prosecutor's Office	High evidentiary threshold. Used only where links to foreign intelligence or comparable national security threats can be supported.
Polish Penal Code – Article 212	Defamation, including media-related defamation	Defamation actions; complaint-based legal proceedings; possible deterrent against targeted reputational attacks	Courts; victim or representative; prosecutors only in limited circumstances	In Poland, defamation can be criminally prosecuted, but these cases are typically driven by the victim rather than as a standard state-led disruption pathway.
Polish Penal Code – Article 226	Insult of a public official in connection with official duties	Legal action in cases targeting public officials; possible escalation in impersonation or harassment cases	Prosecutor's Office; courts	Narrow scope. Relevant only where conduct fits the specific protected-status offence.
Criminal law provisions on hate speech / incitement / extremist content	Disruption of hate speech, incitement to violence, extremist propaganda, and related criminal content	Report Content; Hate Speech; Incitement to Violence; Terrorist Content; Police reporting; Prosecutorial action	Police; Central Bureau for Combating Cyber Crime (CBZC); Prosecutor's Office	These pathways depend on content crossing criminal thresholds. In practice, many influence incidents remain below that threshold and therefore do not trigger rapid intervention.
GDPR / national data protection framework	Data misuse, unlawful profiling, privacy violations, impersonation	Privacy & Data Protection Violations; GDPR complaints; Right	Personal Data Protection Office (UODO)	Useful where influence activity overlaps with data misuse, but it is not

	involving personal data, targeted manipulation using unlawfully processed data	to be Forgotten; regulatory escalation		a general anti-disinformation instrument. Effectiveness depends on proving unlawful processing or privacy harm.
Polish copyright law	Copyright- and trademark-based disruption of manipulated, copied, or falsely branded content	Copyright takedown; Report Copyright Infringement; Intellectual Property Infringement; possible civil or criminal action	Rights holders; courts; platforms; prosecutors in relevant cases	Useful where protected content is reused or manipulated, but applicability is narrow and depends on rights ownership and legal classification. The civil/criminal boundary may require case-specific assessment.
Audio-visual media legislation / AVMSD-related framework	Broadcast and audiovisual regulatory action, including some influencer and streamer oversight	Content removal or restriction; regulatory warnings; fines; obligations on media service providers and video-sharing platforms to address harmful content; cooperation with platforms under AVMSD rules	National Broadcasting Council (KRRiT); in some cases cooperation with EU-level regulators under AVMSD framework	Primarily applies to registered broadcasters and certain video-sharing platforms. Limited reach over decentralised social media content and foreign-based services. Enforcement can be slower and less effective for rapidly spreading online influence operations.

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

6.5 Cross-Sector Interaction Across the Framework

The DISRUPT Framework is useful in Poland precisely because it helps show how these actors interact across the three phases of Prepare, Disrupt, and Mitigate.

6.5.1 PREPARE

In Poland, PREPARE phase activities are primarily analytical and awareness-based. Measures such as information collection, social listening, narrative monitoring, behavioural monitoring, content collection, archiving, and evidence preservation are concentrated in analytical actors and supported by civil society, researchers, and journalists. NASK plays the central institutional role in this phase, while non-governmental actors often contribute monitoring, documentation, and analysis.

The objective at this stage is to move from initial observation to a structured assessment of the incident. However, while inputs are generated across multiple actors, institutional monitoring and detection capability is largely concentrated in NASK. In the absence of a single operational trigger for consolidation and with limited analytical capacity across other public institutions, early-stage coordination remains informational rather than procedural.

6.5.2 DISRUPT

The DISRUPT phase is led by whichever authority has competence over the qualified case. This can include law enforcement, prosecutors, sanctions-related authorities, diplomatic actors, regulators, or platforms. Relevant measures may include reporting content or channels, engaging platforms directly, using DSA mechanisms, triggering sanctions-related restrictions, involving security services, or pursuing administrative or criminal procedures.

In practice, this phase is constrained by the fact that most institutions can act only when activity clearly falls within their legal remit. Many influence operations do not meet intervention thresholds, especially where coordinated inauthentic behaviour is not directly linked to an offence. In such cases, the transition from PREPARE to DISRUPT remains uncertain or delayed.

6.5.3 MITIGATE

Mitigation in Poland is more consistently applied than disruption. Measures such as: public communication, fact-checking, media exposure, and awareness-raising are carried out by government communication actors, line ministries, media, and civil society. The **Government Information Centre** plays a central role in coordinating government communication, while sectoral ministries may provide subject-specific clarification once an issue becomes visible.

This means that mitigation often functions as the practical fallback where legal or administrative disruption is unavailable, delayed, or insufficient. Public explanation and narrative response therefore become central, even though they generally occur later in the lifecycle and do not directly stop the underlying influence operations.

6.6 Fragmentation and Coordination

Both the institutional and non-governmental response landscape in Poland are structurally fragmented. Expertise, authority, and access are distributed across multiple actors, but the mechanisms linking them remain weakly formalised. Several recurrent coordination gaps are identified:

- no shared incident definition,
- no common escalation threshold,
- no predefined workflows between institutions,
- and no structured fallback from disruption to mitigation.
- Lessons learned are also retained informally rather than systematically integrated into future practice.

This fragmentation does not mean Poland lacks response capacity. On the contrary, the national ecosystem contains a substantial number of relevant actors and capabilities. The problem is that these capacities are not consistently connected through shared triggers or a repeatable sequence of action. As a result, response timing becomes unpredictable, incidents may stall between assessment and intervention, and communication often begins only after visibility has increased.

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

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

Effectiveness depends on coordination across fragmentation, not its removal.

6.7 Operational Implication

In Poland,

- **PREPARE measures** are analytically significant but concentrated in a limited number of actors, especially NASK, and supplemented by civil society and research actors.
- **DISRUPT measures** are institutionally available but highly dependent on legal qualification and case-specific routing.
- **MITIGATE measures** are more flexible and consistently used, particularly through communication and awareness-based responses.

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 Poland

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

In practice, detection, assessment, disruption, and communication are carried out by different actors operating within their own domains. The transition between phases depends on whether an incident can be qualified within a specific legal, administrative, or diplomatic framework. Where this qualification is unclear or not met, cases may stall or shift directly into mitigation 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; Monitoring by NASK; Inputs from civil society and researchers	Initial signal detection and analytical observations
PREPARE	Analysis & Assessment	Document; Create Evidence Repository; Actor Mapping; Identify Pattern of Behaviour; CIB Detection (primarily by NASK and CSOs); Attribution (where possible); Legality assessment	Analytical qualification of the case
PREPARE → DISRUPT	Inform	Send Alert; Send Email; Briefing; Forwarding to relevant authority (PM Chancellery) or platform	Case routed to competent authority or platform
DISRUPT	Competence Qualification	Determining whether the case fits criminal, administrative, diplomatic, or platform pathway	Decision on whether disruption is possible
DISRUPT	Enforcement / Action	Report Content; Report Channel; Platform engagement; Criminal investigation (Police / Prosecutor); Diplomatic response (MFA); Sanctions-related action; Financial tracing	Enforcement action, referral, or platform response
MITIGATE	Communication Actions	Public communication; Media exposure; Fact-checking; Narrative clarification; Awareness campaigns; Government	Public response and impact mitigation

		messaging (Government Information Centre, ministries)	

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 represents one of the most operationally complex and resource-intensive types of influence activity in Poland. 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 Polish ecosystem demonstrates strong capabilities in detection and analysis, particularly through NASK and a network of civil society and research actors. These actors are able to identify behavioural patterns, map networks, and document coordinated activity using structured methodologies.

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 foreign, coordinated, or sanctioned actors;
- whether the case meets legal, regulatory, or policy thresholds for intervention.

As a result, disruption is often indirect, delayed, or reliant on external actors, while mitigation-particularly through communication, exposure, and public awareness – remains a consistently applied response.

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

Table 3. CIB workflow overview

Phase	What this typically involves in Poland	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through social listening, narrative monitoring, account tracking, behavioural monitoring, and collection of publicly available content. Cases are documented through observable lists and archiving, while initial network characteristics and patterns are identified.	Preserve evidence, document coordinated behaviour in a structured way, and build a defensible record of channels, accounts, content, and patterns before assets are removed or changed.	1.1 Find and Collect Publicly Available Content, 1.2 Narrative Monitoring, 1.3 Account Monitoring, 1.4Behavioural Monitoring, 2.1 Observable list, 2.2 Offline Archiving, 2.3 Online Archiving, 2.4 Hash Evidence

	In Poland, this phase is strongly supported by NASK, alongside civil society and research actors such as CEEDDW, FakeNews.pl.		
PREPARE → DISRUPT	The case is assessed for whether behaviour is inauthentic, whether it causes harm, whether attribution is possible, and whether legal, platform, or institutional routes are available. In Poland, this includes assessing foreign interference links, identifying infrastructure, ownership, amplification, funding, and links between the actor and possible threat actors.	Determine whether the case meets thresholds for action and identify viable escalation routes, especially platform, regulatory, security, or prosecutorial pathways.	3.1 CIB Detection Tree, 3.2 CIB Algorithm, 3.3Analyse Content, 3.4 Identify links between actor and threat actor, 3.5 Identify Infrastructure, 3.5 Behaviour Analysis (DISARM), 4.1 Inauthentic Behaviour, 4.2Legality, 4.3 Attribution, 4.4 Harm, 4.5 Imminent Risk, 4.6 Foreign Interference
DISRUPT	Action is taken depending on the available legal, technical, platform, financial, and governmental pathways. In Poland, this includes cyber infrastructure disruption, platform reporting, monetisation disruption, regulatory escalation under the DSA, sanctions-related escalation where applicable, and engagement with NASK, the MFA, ABW, prosecutors, police, and other authorities.	Use the strongest available disruption measure without assuming that formal enforcement will always be possible or fast. Combine platform, infrastructure, financial, legal, and institutional measures where possible.	6.1 Hosting, 6.2 Domain, 6.3 Revoke SSL certificates, 6.4 Content Delivery Network, 6.5 Web Application Firewall, 7.1 Report Content, 7.2 Report Channel, 7.3Report Coordinated Inauthentic Behaviour, 7.4Contact Platform Representatives, 7.5 CoC Rapid ResponseSystem, 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, 9.6Political Advertisement Transparency Legislation, 10.1 Counter FIMI Agency, 10.2 Ministry of Foreign Affairs, 10.3 Security Services, 10.4 Interior Ministry, 10.6 Prosecutor
MITIGATE	Where disruption is delayed, incomplete, or platform-dependent, communication and	Strengthen public resilience, expose manipulation techniques, and sustain pressure on	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

	awareness measures are used to reduce impact. In Poland, this includes public reporting, alerts, briefings, media collaboration, political engagement, advocacy mobilisation, and public exposure of the network's behaviour, affiliations, and manipulation techniques.	platforms, institutions, and enabling actors.	

In the Polish context, the operationalisation of CIB response is shaped by **3 structural factors**:

First**, analytical detection** is concentrated in a limited number of actors, especially NASK. NASK applies the main methodology for identifying coordinated inauthentic behaviour, while other institutions generally do not maintain independent CIB classification mechanisms. This makes the quality of detection and evidence preparation especially important in the PREPARE phase, but also creates dependence on a relatively narrow analytical layer.

Second, **the transition from PREPARE to DISRUPT** is weakly formalised. Once a case has been identified and analysed, there is no single escalation trigger that automatically routes it into action. Instead, institutions assess independently whether the case falls within their own competence. In practice, this means that many CIB cases rely primarily on platform reporting and related notice-and-action mechanisms, rather than on direct institutional intervention. Where the activity does not meet criminal, administrative, or security thresholds, disruption options remain limited.

Third, **mitigation** frequently substitutes for disruption. Because platform enforcement is discretionary and legal pathways are often unavailable or slow, the most consistent response to CIB in Poland is public communication, clarification, and awareness-raising. Government communication actors, ministries, media, and civil society organisations therefore play a central role in reducing impact, even where they cannot directly stop the operation itself.

For Polish practitioners, the main operational implication is that CIB response depends on the ability to move from strong analytical identification toward the most viable available response pathway, whether platform-based, regulatory, institutional, or communicative. The DISRUPT Framework is particularly useful in this context because it helps connect detection and documentation to proportionate intervention, while also making clear where disruption is likely to stall and where mitigation must be activated instead.

10. Application to Sanctions-Related Cases

Sanctions-related influence operations in Poland 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 Polish ecosystem demonstrates strong capabilities in detecting and documenting sanctions circumvention, particularly through actors such as NASK, civil society organisations, and investigative researchers. Detection typically relies on tracing content provenance, identifying republication patterns, and establishing links between proxy actors and sanctioned entities. This requires structured evidence collection, including archiving, hash verification, and comparative content analysis to demonstrate that content has been laundered from sanctioned sources.

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

- the ability to **prove origin and attribution** to a sanctioned entity;
- the willingness of **platforms and service providers** to enforce sanctions compliance;
- the identification of **intermediary infrastructure** (hosting, domains, payment providers);
- engagement with **competent national and EU authorities** responsible for sanctions enforcement.

Disruption pathways in sanctions cases are broader and more legally grounded than in CIB. They include:

- reporting sanctioned content and channels to platforms;
- targeting infrastructure providers (hosting, domain registrars);
- disrupting monetisation through ad networks, payment providers, and financial institutions;
- invoking regulatory frameworks such as the Digital Services Act (DSA) and EU sanctions regimes;
- escalating cases to government actors, including ministries and financial intelligence units.

In the Polish context, **government engagement plays a more central role than in CIB cases**. Institutions such as the Ministry of Foreign Affairs, security services, and financial intelligence bodies can contribute to attribution, enforcement, and escalation at the EU level. However, coordination between non-governmental actors and state authorities remains partially ad hoc, and formal escalation pathways are not always clearly defined.

Despite stronger legal grounding, disruption is not always immediate. Many measures – particularly those involving financial flows, sanctions enforcement, or regulatory escalation – require longer timeframes and substantial evidence thresholds. As a result, mitigation through communication and exposure remains an important complementary approach. Public reporting, media collaboration, and advocacy are frequently used to apply pressure on platforms and service providers, especially in cases where formal enforcement is delayed.

Overall, sanctions-related cases in Poland demonstrate a more mature and enforceable disruption environment compared to CIB. However, effectiveness still depends 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 can be operationalised in Poland for sanctions-related cases.

Table 4. Sanctions workflow overview

Phase	What this typically involves in Poland	Main practitioner focus	Key Framework measures
PREPARE	Signals emerge through monitoring of content suspected to originate from sanctioned entities. Practitioners trace republication patterns, identify proxy actors, and document links between sanctioned sources and local amplifiers. Evidence is preserved through archiving and hashing to support legal thresholds.	Establish verifiable links between content and sanctioned entities, ensuring evidence meets legal and platform enforcement standards.	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	Cases are assessed for sanctions relevance, including attribution to listed entities, financial or infrastructural links, and legal qualification under EU sanctions regimes. Analytical work focuses on proving origin, ownership, or amplification of sanctioned content.	Determine whether the activity constitutes sanctions circumvention and identify viable disruption pathways (platform, infrastructure, financial, or regulatory).	3.1 Analyse Content, 3.2 Identify Links Between Actor and Threat Actor, 3.3 Identify Infrastructure, 4.1 Legality, 4.2 Attribution, 4.3 Foreign Interference
DISRUPT	Action is taken through legally grounded mechanisms. Practitioners report sanctioned content to platforms, target hosting and domain providers, and disrupt monetisation via ad networks and financial intermediaries. Escalation to government actors enables enforcement, attribution, and potential sanctions expansion.	Use legally enforceable disruption measures, prioritising financial, infrastructural, and regulatory pressure points while coordinating with public authorities.	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 Contact Platform Representatives, 7.4 CoC Rapid Response System, 7.5 Advertising, 8.1 Demonetise Operation Assets, 8.2 Investor, 8.3 Freeze Banking Services, 8.4 Payment Providers, 9.1 DSA, 9.2 EU Sanctions for De-Platforming

			and Financial Disruption, 9.3 Invocation of Foreign Interference Legislation, 9.4 Intellectual Property Enforcement, 10.1 Counter FIMI Agency, 10.2 Ministry of Foreign Affairs, 10.3 Security Services, 10.4 Financial Intelligence Units, 10.5 Interior Ministry, 10.6 Prosecutor, 10.7 Audio-Visual Regulator, 10.8 Police
MITIGATE	Where disruption is delayed or partial, practitioners rely on exposure and awareness-building. Reports, media collaboration, and stakeholder engagement are used to highlight sanctions circumvention and pressure platforms and service providers to act.	Increase transparency around sanctions circumvention, mobilise stakeholders, and apply reputational pressure to accelerate enforcement.	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

11. Minimum Operational Readiness

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

In the Polish context, minimum operational readiness is especially important because relevant capabilities already exist across analytical actors, ministries, law enforcement, regulators, and civil society, but they are not consistently connected through predefined triggers or workflows. Readiness therefore depends not only on institutional capacity in isolation, but on the ability to receive signals, document cases, route them quickly, coordinate across mandates, and activate communication or mitigation where disruption is delayed or unavailable.

Table 5. Minimum Readiness Capability

Capability	Description	Operational actions (what actors can do)
Signal intake	Mechanism for receiving and reviewing alerts	Receive alerts from NASK, civil society organisations, researchers, media actors, or international partners; screen incoming signals; prioritise cases based on risk, including imminent harm, elections, sanctions relevance, foreign interference, or national security implications; acknowledge receipt and trigger initial review.

Case tracking	Basic documentation of cases	Open a case file; record key information such as source, content, actor, platform, timeline, and possible legal relevance; update case status; maintain an evidence repository and record referrals between institutions.
Routing clarity	Understanding of institutional competences	Identify the competent authority depending on case type, for example NASK for analytical assessment, prosecutor or police for criminal thresholds, MFA for diplomatic or sanctions-related pathways, ABW for national security concerns, UODO for data protection issues, or platform-facing channels for CIB and illegal content; route cases accordingly and clarify responsibilities early.
Evidence standards	Consistent approach to documentation	Collect and preserve evidence, including screenshots, URLs, metadata, archived copies, and platform identifiers; apply hashing where legal robustness is needed; structure evidence so that it can support platform reporting, sanctions enforcement, prosecutorial review, or security-sector escalation.
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, alerts, briefings, and explanatory material; determine when communication should remain internal and when public messaging is needed; engage the Government Information Centre, line ministries, journalists, or fact-checkers where appropriate; ensure communication 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. In Poland, they are particularly important because the main operational challenge is not the absence of relevant actors, but the absence of consistent sequencing between them. Minimum readiness therefore means ensuring that existing capacities can be connected quickly enough to support timely and proportionate action across the lifecycle of influence operations.

12. Conclusion

The application of the DISRUPT Framework in Poland demonstrates that the country possesses a comparatively strong ecosystem for detecting and analysing information manipulation, including coordinated inauthentic behaviour (CIB) and sanctions-related activities. Key actors –

particularly NASK, civil society organisations, and independent researchers – provide robust capabilities in monitoring, attribution support, and evidence collection.

However, the primary challenge is not detection, but the consistent translation of analytical findings into timely and effective disruption. In many cases, response pathways depend on external actors, such as platforms or EU-level mechanisms, or require high evidentiary thresholds before legal or regulatory measures can be applied. This creates a gap between identification and action, particularly in cases that fall into legal grey zones, such as CIB.

Sanctions-related cases demonstrate a more enforceable pathway, as they benefit from clearer legal grounding under EU law. These cases enable a broader range of disruption measures, including financial, infrastructural, and regulatory interventions, as well as more direct engagement with government authorities. However, even in these cases, effective disruption depends on coordination across multiple actors and on the ability to operationalise evidence in a legally actionable form.

Across both case types, the findings point to a structural issue: Poland has the necessary actors and capabilities, but lacks consistently applied coordination mechanisms, predefined escalation pathways, and shared operational standards. As a result, responses can be fragmented, delayed, or dependent on informal networks and individual initiative.

The DISRUPT Framework addresses this gap by providing a common structure for organising actions across the full lifecycle of an influence operation – from preparation and assessment to disruption and mitigation. Its value in the Polish context lies not in introducing new capabilities, but in connecting existing ones, clarifying roles, and enabling more predictable and coordinated responses.

Strengthening operational readiness in Poland will therefore depend on:

- improving clarity on institutional roles and escalation pathways;
- enhancing coordination between analytical, governmental, and platform-facing actors;
- ensuring that evidence collection is consistently aligned with legal and enforcement requirements;
- and reinforcing communication and mitigation strategies where disruption is delayed or not immediately feasible.

By embedding these elements, the Framework can support Poland in moving from a strong detection environment to a more consistently effective disruption ecosystem.

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 Poland

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

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