Module 5: Disinformation and Information Manipulation

Training material to be shared with trainers only

CONTENTS

TRAINER OVERVIEW 2

PREPARATION AND ROUTE SELECTION 3

CORE MESSAGES THAT SHOULD REMAIN CONSTANT 5

CONCEPTS AND SAFEGUARDS 6

NARRATIVES, ACTORS AND HARMS 7

BEHAVIOUR AND AMPLIFICATION 8

GENERATIVE AI AND SYNTHETIC MEDIA 9

FROM DETECTION TO ASSESSMENT 10

VERIFICATION AND ANALYTICAL WRITING 12

PROPORTIONATE RESPONSE 12

RECENT ELECTION CASES 14

CHECKING LEARNING AND NEXT STEPS 15

TRAINING OF TRAINERS' GUIDANCE AND ASSESSMENT 16

AUDIENCE ADAPTATION 16

SOURCES AND FURTHER READING 17

This module helps participants recognise and assess disinformation and information manipulation during elections without treating contested political speech as an automatic violation. It shifts attention from isolated posts to narratives, actors, behaviour, distribution and potential democratic harm. The module also connects detection with a proportionate response based on mandate, evidence and urgency.

Use the separate participant workbook for activities. Keep the worked answers, case outcomes and debrief guidance in this trainer document until exercises are complete. The activities can be delivered with printed materials and do not require access to social-media accounts or specialist software.

The module addresses domestic information manipulation as well as foreign information manipulation and interference. The term FIMI should be used only when evidence supports a foreign dimension. Where attribution remains uncertain, describe the observed behaviour and use a provisional hypothesis.

Trainer overview

Module objective

Enable participants to distinguish inaccurate information from intentional and coordinated manipulation; analyse narratives and distribution behaviour; assess electoral harm and urgency; and select responses that protect both electoral integrity and freedom of expression.

Learning outcomes

- Distinguish misinformation, disinformation, malinformation, propaganda, hate speech and FIMI, while recognising overlaps and legal differences.
- Analyse a suspected incident through content, narrative, actor, behaviour, distribution, target and harm.
- Identify indicators of coordinated or inauthentic amplification without declaring accounts to be bots, trolls or foreign proxies on insufficient evidence.
- Assess synthetic media and generative-AI content through provenance, context, distribution and harm rather than visual intuition alone.
- Apply a documented verification and escalation process that separates observations, analytical judgments and attribution.
- Choose a timely and proportionate response within the mandate of the responsible actor and explain why non-response may sometimes be preferable.

Session techniques and methods

Concept sorting; narrative and harm mapping; individual evidence coding followed by group comparison; simulated election incident room; response drafting; peer review; short case comparison; individual exit task. Provide printed scenarios, large text and seated roles where needed. Warn participants before material involving harassment or identity-based attacks and allow them to work with a neutral alternative.

Duration

Standard route: 120 minutes. Condensed route: 90 minutes. Extended route: 180 minutes. The timing includes instructions, group work, reports and debriefs but excludes breaks, translation and preparation. The standard route uses the Slovakia case as the main simulation. The extended route adds Romania and Moldova and a second response round.

Standards and scope

CM/Rec(2022)12 is the principal Council of Europe reference for electoral communication in the digital environment. It addresses disinformation campaigns, abusive use of bots and algorithms, platform transparency and safeguards for freedom of expression. Read it together with Article 10 of

the European Convention on Human Rights and Article 3 of Protocol No. 1. Restrictions on expression must have a legal basis, pursue a legitimate aim and be necessary and proportionate. Measures should be transparent, non-discriminatory and use the least restrictive effective means. [1–4]

FIMI is a behaviour-centred analytical concept used by the European External Action Service. It usually concerns intentional and coordinated manipulative behaviour that threatens political processes and may remain lawful in itself. The label is not a substitute for evidence of attribution, illegality or impact. [5–7]

Module 4 supplies the monitoring discipline on which this module builds. Platform governance and political-advertising obligations belong in Module 6, protection and inclusion in Module 7, and wider violations, remedies and resilience in Modules 8 and 9.

Preparation and route selection

Trainer checklist

- Review the national legal framework, electoral calendar, silence period, institutional mandates and emergency communication arrangements. Do not assume that an EMB, regulator, police service, platform or fact-checker can take the same action.
- Map the information environment: major broadcasters and online outlets, platforms, messaging services, languages, regional audiences, influential creators and trusted community intermediaries.
- Consult media, journalists' associations, civil society organisations, fact-checkers, election observers, regulators and EMBs. Treat allegations as leads until independently verified.
- Print Sheets 1–6. Keep the case outcomes and suggested responses in this guidance. The fictional material is for training and makes no allegation about a real actor.
- Prepare an escalation contact list and a simple incident log. For a national adaptation, verify all names, dates and legal powers against primary sources.
- Avoid live searches for harmful content during training. Use archived and redacted examples. Do not expose personal data or ask participants to enter closed groups.
- Agree how participants will distinguish public-interest documentation from amplification. Repeating a false claim in a correction can increase its visibility.
- Assign roles before the simulation and rotate the spokesperson. Let participants analyse individually first so professional hierarchy does not determine the group's initial judgment.

Route table

Session	90 min	120 min	180 min
1 Concepts and safeguards	5	10	15
2 Narratives, actors and harms	10	15	20
3 Behaviour and amplification	15	20	30
4 Generative AI	15	20	30

Session	90 min	120 min	180 min
5 Detection and assessment	15	20	30
6 Proportionate response	15	20	30
7 Recent cases	10	10	15
8 Learning check	5	5	10

For 90 minutes, provide the definitions before the session, use only Items A–C in Sheet 1 and one role in the Slovakia simulation. For 120 minutes, complete all core sheets and compare two professional responses. For 180 minutes, add a second incident, cross-role coordination and a revised response after peer review. Do not remove the safeguards or evidence debrief to save time.

Core messages that should remain constant

- False information and manipulation are related but different problems. Falsity concerns content; manipulation analysis also asks who acted, how, with what coordination, distribution method and apparent purpose.
- Not every inaccurate statement is disinformation. Error, satire, parody, opinion and good-faith reporting require different treatment.
- Harmful content can be authentic and factually accurate. Selective disclosure, decontextualisation, impersonation and coordinated amplification may manipulate the information environment without inventing a fact.
- Repetition, identical wording, new accounts or unusual timing are indicators for inquiry, not proof of bots, foreign control or platform complicity.
- Attribution requires stronger evidence than detection. State what is observed, what is assessed with a confidence level and what remains unknown.
- Electoral harm includes more than persuasion. Manipulation can confuse voters about procedures, suppress participation, intimidate candidates or officials, distort equal opportunities, erode trust and crowd out reliable information.
- Responses should reduce harm without unnecessarily amplifying the claim. Correct the information gap, identify the trusted messenger, preserve evidence and choose the least restrictive effective measure.
- Speed matters, but accuracy and legitimacy matter too. Pre-agreed roles and escalation thresholds allow institutions to respond quickly without improvising powers during a crisis.
- Resilience begins before an incident through transparent election information, independent journalism, media literacy, secure institutions and trusted channels across different communities.

Concepts and safeguards

SESSION METHOD Concept sorting using Sheet 1 | TIME 5, 10 or 15 minutes

Working distinctions

Term	Practical meaning for this module
Misinformation	False or inaccurate information shared without established intent to deceive. Correction may be needed, but intent should not be invented.
Disinformation	Verifiably false, inaccurate or misleading information deliberately created or disseminated to cause harm or obtain political or economic gain by deceiving the public. [1]
Malinformation	Genuine information used or disclosed in a way intended to cause harm, for example through deceptive framing or an invasion of privacy. The term does not itself determine legality.
Propaganda	Communication designed to shape attitudes or action in favour of a political cause or actor. It may contain facts, opinions, omissions or falsehoods and is not automatically unlawful.
Hate speech	Expression covered by the applicable Council of Europe definition and national law; assess its content, context, speaker, intent, reach and likely harm. Do not use “disinformation” as a substitute label. [8]
Information manipulation	Intentional conduct that distorts the information environment through content, deceptive behaviour, distribution or interference. The analysis may include lawful acts and must preserve Article 10 safeguards.
FIMI	A mostly non-illegal, intentional and coordinated pattern of manipulative behaviour involving state or non-state actors or proxies across borders or territories and capable of harming values or political processes. A foreign link must be evidenced, not assumed. [5–7]

Guidance for trainers

Ask participants to classify the Sheet 1 items, then identify what further evidence could change the classification. Accept more than one defensible answer where intent or context is missing. Emphasise that professional action can begin before attribution: an EMB may correct a false polling-place claim while investigators continue to examine its origin.

Freedom-of-expression check

Political speech receives strong protection. A response based on content must distinguish unlawful expression from lawful but harmful or misleading communication. Before recommending removal, blocking, sanctions or compulsory correction, ask: What rule applies? Who has authority? What evidence establishes the threshold? Is the measure necessary? Could labelling, authoritative information, reduced amplification, transparency or a right of reply address the harm with less interference?

Narratives, actors and harms

SESSION METHOD Narrative and harm map | TIME 10, 15 or 20 minutes

From a post to a narrative

A post is one observable item. A claim is a factual proposition that can often be checked. A narrative is a recurring interpretive frame that connects events, actors and emotions, such as “the election is already stolen” or “institutions serve outsiders”. Narratives may combine accurate facts, opinions and false claims. Track them without treating criticism of institutions as manipulation merely because it is uncomfortable.

Analytical map

Dimension	Questions
Message	What is claimed, implied or omitted? What image, audio, label or emotional cue carries the message?
Narrative	Which wider story does the item reinforce? Is the narrative established before the election or attached to a new incident?
Actor and source	Who created, first published, endorsed and amplified it? Which identities are verified, concealed or impersonated?
Target and audience	Which institution, contestant, community or procedure is targeted? Which language, grievance or vulnerability shapes reception?
Behaviour	Is there evidence of coordination, deception, automation, paid distribution, account recycling or cross-platform seeding?
Distribution	Through which outlets, accounts, groups, influencers, advertisements or recommender systems did it travel? What is known about reach?
Harm	Could it mislead voters about how to vote, suppress turnout, intimidate participation, damage safety, distort competition or erode confidence?
Evidence and confidence	Which observations are preserved? Which conclusion is low, medium or high confidence, and what would raise or lower it?

Guidance for trainers

Use Sheet 2. Ask one group to focus on electoral-process harm, another on candidates and participation, and another on affected communities. The same narrative can produce different harms. Gendered or identity-based manipulation may aim not only to discredit one person but to increase the cost of public participation for a wider group.

Sheet 2 adapts a field-tested foreign-influence narrative exercise previously used with civil society and election observers. The crucial distinction is between a domestic claim that institutions, media or civil society are “controlled from abroad” and evidence that a foreign actor actually created, coordinated or financed the campaign. Ask groups what would establish that foreign dimension and what wording remains defensible when attribution is unknown.

Do not infer impact from engagement counts alone. Public reactions can show circulation or attention but not unique exposure, belief or voting behaviour. Ask what additional audience research, surveys or platform data would be needed.

Behaviour and amplification

SESSION METHOD Evidence ladder using Sheet 3 | TIME 15, 20 or 30 minutes

Observable indicators

Possible indicators include near-simultaneous posting, identical or translated wording, repeated links to the same low-credibility domain, clusters of recently created accounts, copied profile material, sudden changes in account topic, systematic replies under unrelated news, coordinated hashtags, undisclosed paid promotion and cross-platform sequencing.

Each indicator has benign explanations. Campaign volunteers may use approved text; activists may mobilise quickly; news events can create real spikes; and new users may join during an election. Analyse combinations, persistence and context rather than treating a single signal as proof.

Evidence ladder

Level	What can be stated
Observation	Describe the captured posts, times, wording, account metadata and public interaction pattern without assigning intent or identity.
Analytical indicator	Explain why the pattern is unusual under a declared rule and identify plausible alternative explanations.
Coordinated behaviour assessment	Support with repeated temporal, linguistic, network or operational connections and record the confidence level.
Inauthentic or automated behaviour	Require evidence that identities or activity misrepresent who controls the accounts or how they operate. High posting volume alone is insufficient.
Attribution	Link the activity to an organisation, campaign, state or proxy only through corroborated technical, financial, documentary, platform or investigative evidence.
Electoral impact	Establish through evidence of reach, audience response, institutional disruption or other effects; do not infer a change in votes from content analysis alone.

Bots, trolls and coordinated inauthentic behaviour

A bot is an automated account or process. A troll usually describes a person or account that provokes or disrupts discussion, but the term is imprecise and should not replace an operational finding. Coordinated inauthentic behaviour concerns deceptive coordination about the identity or origin of actors and their behaviour; the exact platform definition may differ. Report the observable pattern and applicable definition.

Behaviour exercise debrief

Suggested assessment for Sheet 3

The identical wording, narrow eight-minute window, common anonymous link and concentration of new accounts support a hypothesis of coordination. They do not establish automation, payment, common control, foreign attribution or falsity of the underlying claim. The established activist accounts should not be added automatically to the suspected network because later sharing can reflect organic uptake.

The team should preserve URLs, post identifiers, public timestamps, screenshots or lawful archives, account creation dates and the collection method. It should verify the ballot-scanner claim with competent sources, search for earlier or cross-platform versions, examine public network connections and seek platform or investigative assistance where lawful. A preliminary finding should use language such as “a coordinated posting pattern is suspected with medium confidence” and state the basis and limits.

Common analytical errors

- Starting with a preferred label and collecting only evidence that confirms it.
- Treating correlation in timing as proof of common control.
- Calling all anonymous, pseudonymous or recently created accounts fake.
- Equating high interactions with reach, agreement or electoral influence.
- Naming a foreign actor because the narrative aligns with its interests.
- Publishing account lists before completing verification and risk assessment.

Trainer prompt

Ask what evidence would falsify the group’s hypothesis. A credible method looks for disconfirming evidence and updates confidence when new information appears. Record alternative explanations in the incident log rather than mentioning them only after a conclusion is challenged.

Generative AI and synthetic media

SESSION METHOD Synthetic-media triage and scenario | TIME 15, 20 or 30 minutes

What changes and what does not

Generative AI lowers the cost and time needed to produce convincing text, images, audio and video, personalise messages and create many variations. It can facilitate impersonation, fabricated evidence and harassment at scale. It can also support translation, accessibility, journalism and voter information. The analytical task remains to establish authenticity, context, distribution and harm.

Do not rely on visual or auditory intuition, a single detector or the absence of an obvious artefact. Detectors can produce false positives and false negatives. Preserve the original file where lawfully available, record provenance and publication history, compare with verified sources, consult the person or institution depicted, examine contextual inconsistencies and seek specialist analysis when consequences are serious.

Rapid triage

1. Preserve the item, URL, timestamp and account context without redistributing it unnecessarily.

2. Identify the precise claim and the decision voters are being asked to make.

3. Check authoritative sources and contact the impersonated actor where appropriate.

4. Assess circulation, timing, vulnerable audiences and whether a correction would amplify the content.

5. Mark what is verified, likely, uncertain and false. Do not call content AI-generated unless evidence supports that statement.

6. Escalate according to the incident protocol and prepare accurate public information that closes the information gap.

Slovakia 2023 simulation

Shortly before the 30 September parliamentary election and during the campaign moratorium, manipulated audio circulated purporting to capture a discussion about electoral manipulation between a political leader and a journalist. ODIHR reported multiple deepfake audio clips and wider disinformation concerns in the campaign. The timing constrained ordinary political rebuttal and increased the importance of prepared coordination among election authorities, media, civil society and platforms. Use Sheet 4 for the incident-room exercise. [9]

From detection to assessment

SESSION METHOD Incident-room analysis using Sheet 4 | TIME 15, 20 or 30 minutes

Minimum incident record

Field	Record
Incident	Unique identifier, first observation, election phase, analyst and status.
Content and narrative	Exact claim, format, language, wider narrative and known variations.
Source and spread	First known public source, amplifiers, platforms, timing and observed metrics with definitions.
Target and harm	Procedure, institution, person or community targeted; plausible and observed harms.
Verification	Sources consulted, evidence preserved, unresolved questions and contradictions.
Behaviour	Coordination or inauthenticity indicators and alternative explanations.
Attribution	Evidence, confidence and whether the foreign dimension is established, suspected or unknown.
Legal and policy status	Potentially unlawful content or conduct, relevant rule, competent authority and safeguards.
Response	Decision, responsible actor, message, channel, escalation and review time.

Risk and urgency matrix

Assess at least four factors: potential harm, observed circulation, time sensitivity and confidence in the underlying facts. A low-reach false claim about a candidate's policy may require monitoring or journalism. A rapidly spreading false polling-place instruction can justify immediate authoritative correction even if its author remains unknown. A credible threat or doxxing requires a safety response and possible law-enforcement referral.

Do not collapse these factors into a number that hides judgment. Record why an incident falls into the selected response tier and when it will be reassessed.

Verification and analytical writing

Three layers

Observation: “Twelve public accounts posted identical wording and the same link between 20:00 and 20:08.”

Assessment: “The temporal and textual similarity supports a medium-confidence hypothesis of coordination; common campaign messaging remains an alternative explanation.”

Attribution: “No public evidence identifies common control, automation, funding or a foreign actor.”

Keep these layers separate in internal records and public communication. Use confidence language consistently and update it as evidence changes.

Minimum verification questions

- Can the factual claim be checked against a primary source or independent evidence?
- Is the source authentic, and does the material preserve its original context?
- Who first published it, and what is known rather than assumed about that actor?
- Does the circulation pattern differ from normal activity under a documented baseline?
- Is paid promotion, influencer support or cross-platform seeding visible?
- Which affected actor has been offered a fair opportunity to comment?
- What evidence is missing because of privacy, access or platform limitations?

Data protection and safety

Collect only information necessary for the purpose. Use public data lawfully, restrict access, protect investigators and affected people, and avoid publishing personal information that facilitates harassment. Closed or encrypted spaces require particular legal, ethical and methodological care. Election observers should normally rely on public content and credible specialist reporting rather than infiltrating private groups.

Trainer debrief

Good monitoring identifies a decision point. It should tell the responsible actor what is known, how urgent it is, which harm is plausible, what remains uncertain and when to review the assessment. A large archive without an escalation route is detection without response.

Proportionate response

SESSION METHOD Response selection and drafting using Sheet 5 | TIME 15, 20 or 30 minutes

Response options

Option	Appropriate use and safeguards
Monitor and preserve	Use where evidence or circulation is limited. Set a review trigger and avoid indefinite passive monitoring.
Fill the information gap	Publish clear election facts through trusted and accessible channels. Address the correct procedure without repeating sensational falsehoods unnecessarily.
Prebunk	Explain a foreseeable manipulation technique or recurring false narrative before it peaks. Avoid implying that legitimate criticism is illegitimate.

Option	Appropriate use and safeguards
Debunk or correct	Lead with accurate information, identify the evidence and provide an action voters can take. Consider whether repeating the claim will amplify it.
Journalistic response	Verify, contextualise and report the operation or public-interest issue. Avoid embedding harmful material merely for illustration.
Platform escalation	Use an established channel and identify the applicable service rule or legal duty. Preserve evidence and record response times and outcomes.
Regulatory or legal action	Use only within legal powers and with due process, independence, necessity, proportionality and effective review. Distinguish illegal content from lawful but manipulative behaviour.
Safety and security response	Address threats, doxxing, account compromise or cyber incidents through the appropriate protection and law-enforcement pathway.
Strategic and diplomatic action	Where attribution is sufficiently supported, consider public attribution, sanctions or diplomatic measures through competent authorities.

Communication principles

Lead with verified information and the practical action voters should take. Use a messenger trusted by the affected audience and provide accessible formats and relevant languages. State uncertainty honestly. Coordinate facts and roles, not political messaging. Review whether the response reduced confusion, reached the intended audience or unintentionally amplified the manipulation.

Roles and coordination

Actor	Primary contribution
Election management body	Provide rapid, authoritative procedural information; monitor threats to election administration; maintain a correction page and escalation protocol.
Media regulator or supervisory authority	Apply the law independently; monitor relevant services within its mandate; request information or impose remedies only where legally authorised and proportionate.
Courts and judges	Review legality, evidence, procedural fairness and proportionality; provide effective and timely remedy.
Lawyers	Test the legal basis and evidence, protect rights, advise affected actors and frame proportionate remedies.

Actor	Primary contribution
Policymakers	Establish clear mandates, safeguards, transparency duties and resources before elections; avoid last-minute rules tailored to a speaker or viewpoint.
Journalists and media	Verify claims, investigate networks, explain uncertainty, protect sources and avoid becoming an amplification channel.
Civil society and fact-checkers	Detect narratives, verify content, reach communities, document harms and provide independent scrutiny.
Election observers	Assess the environment and institutional response; distinguish observed incidents from proven impact and attribution.
Platforms	Enforce clear rules consistently, preserve evidence, provide transparency and researcher access, address systemic risk and offer redress.
Political actors and influencers	Avoid deceptive practices, disclose sponsorship and synthetic content where required, correct their own false claims and refrain from coordinated harassment.

Coordination protocol

Before the campaign, agree contact points, severity thresholds, evidence fields, secure communication channels and who may speak publicly. During an incident, share verified facts and avoid circulating unnecessary personal data. After action, record what each actor did, whether the response arrived in time and what should change. Institutional cooperation must respect independence: an EMB should not direct editorial decisions, and political authorities should not control fact-checking or enforcement outcomes.

Suggested Sheet 5 debrief

A strong response to the false election-day suspension claim confirms that voting continues, gives the official polling-place lookup method, names the responsible EMB, uses local languages and accessible formats, and asks media and platforms to direct users to the authoritative source. It does not need to accuse a foreign actor before attribution. For the Slovakia audio, a response can state that the recording is manipulated once verification supports that conclusion, explain how voters can check official election information and avoid replaying the audio.

Recent election cases

SESSION METHOD Case comparison using Sheet 6 | TIME 10 or 15 minutes

Romania presidential election 2024

Romania's Constitutional Court annulled the first-round result on 6 December 2024 after finding that essential principles of free democratic elections had been breached. Declassified material indicated a mass online influence operation and undisclosed promotion benefiting a candidate. The European Commission had issued a TikTok data-retention order and later opened formal Digital Services Act proceedings concerning systemic electoral risks. Treat the case as an example of the difficulty of

obtaining a graduated remedy before fast-moving online harm affects an election, not as a template for cancelling results. [10–12]

Moldova presidential election and referendum 2024

ODIHR concluded that both rounds were well managed and contestants could campaign freely overall, while the environment was affected by interference from abroad and active disinformation. The case allows participants to examine how coordinated institutional action can coexist with safeguards, contested attributions and concerns about equal opportunity. [13]

Slovakia parliamentary election 2023

ODIHR reported deepfake audio, manipulative content attributed to foreign sources and domestic politicians, and limited timely remedies for some media complaints. The case highlights moratorium timing, domestic amplification and the need to prepare verification and communication channels before election day. [9]

Guidance for trainers

Do not rank countries or treat one incident as proof of electoral impact. Ask participants to identify the verified fact, the institutional decision, the evidence still required and the safeguard that prevents an overbroad response. Use the full primary report when adapting a case nationally.

Checking learning and next steps

SESSION METHOD Exit task and action commitment | TIME 5 or 10 minutes

Exit task

Give participants this observation: “Ten accounts publish the same false polling-place address within five minutes. Three are new; two are verified party accounts; the others are unknown.” Ask them to write four sentences: one observation, one analytical assessment with confidence, one unsupported conclusion to avoid, and one immediate response.

Expected elements

The observation should preserve facts and source limits. The assessment may identify suspected coordination while recognising campaign messaging or organic copying as alternatives. Participants should avoid claiming bots, common control, foreign interference or changed votes. The immediate response should provide accurate voting information through the EMB and trusted intermediaries, preserve evidence and trigger further review.

Learning check

- Can the participant separate falsity, intent, coordination and foreign attribution?
- Can they identify the narrative and democratic harm without treating criticism as manipulation?
- Can they state what observed indicators do and do not prove?
- Can they select a response within their professional mandate and apply freedom-of-expression safeguards?
- Can they name the missing evidence and a review point?

Follow-up task

Within one month, participants should map their organisation’s contact points and draft one incident protocol covering collection, verification, severity, escalation, public communication, data protection and post-incident review. A tabletop test before the next election should expose gaps while there is still time to fix them.

Training of trainers' guidance and assessment

Module-specific facilitation

Create distance between emotionally powerful content and analytical judgment. Begin with classification and evidence, then move to narratives, behaviour, attribution and response. Common mistakes include using disinformation as a label for any false statement, inferring coordination from similarity, identifying a foreign actor because a narrative aligns with its interests, and treating synthetic content as harmful by definition. Use fictionalised or safely redacted material where displaying real abuse would reproduce harm.

Audience-specific application

Regulators and lawyers should focus on authority, evidence thresholds and safeguards. EMBs should analyse procedural narratives and corrective communication. Journalists should practise verification and reporting without amplification. Civil society and observers should map narratives and behaviour while stating confidence levels. Policymakers should examine structural gaps without drafting content-based powers too broadly.

Assessment and evaluation

Use the concept-sorting task as the entry diagnostic. Assess whether participants separate observation, analytical assessment and attribution; follow the evidence ladder; identify the targeted audience and electoral harm; and select a proportionate response. Use the three-layer writing exercise and final learning check as the exit assessment.

Evidence of learning and trainer reflection

Participants meet the objective when they classify content cautiously, describe amplification without unsupported claims about bots or coordination, state attribution at the level supported by evidence, and propose a response that protects expression. Ask each participant to underline the strongest and weakest clause in their analytical finding. Trainers should note emotional or safeguarding issues that require adaptation.

Audience adaptation

One analytical framework, different professional tasks

Audience	Emphasis	Suitable technique and output
Regulators and supervisory authorities	Mandate, evidence thresholds, platform liaison, due process and proportionate remedy.	Complaint triage and simulated decision with reasons, safeguards and review route.
Election management bodies	Procedural rumours, authoritative information, incident escalation and trusted public communication.	Election incident room and a two-sentence correction in multiple audience formats.

Audience	Emphasis	Suitable technique and output
Judges and legal professionals	Attribution evidence, legality, necessity, proportionality, procedural safeguards and effective remedy.	Structured hearing using an evidence bundle; reasoned decision separating illegal content from lawful manipulation.
Policymakers	Institutional design, independence, resources, transparency and election-period coordination.	Gap analysis and protocol drafting; avoid writing content-based emergency powers around one case.
Journalists and media practitioners	Verification, provenance, network reporting, source protection and avoiding amplification.	Editorial conference deciding whether, when and how to report a synthetic-media incident.
Civil society, fact-checkers and observers	Narrative monitoring, community harm, credible documentation, referrals and limits on impact claims.	Evidence-ladder analysis and public finding with confidence and methodological caveats.

Mixed groups should analyse the same incident from different mandates, then negotiate a coordination plan. Do not ask every group for the same product. A regulator gives a reasoned legal response; an EMB closes an information gap; journalists decide how to report; civil society documents patterns; observers assess the overall environment.

Accessibility and inclusion

Adapt examples to languages and media habits of affected communities. Do not expose participants to repeated abusive content where a neutral description teaches the same skill. Provide content warnings, anonymise targets and allow alternative roles. Ask whose trust is needed and whether the chosen messenger can reach people with disabilities, minority-language audiences and voters with limited connectivity.

Sources and further reading

1. Council of Europe, Recommendation CM/Rec(2022)12 on electoral communication and media coverage of election campaigns. Open source

2. European Convention on Human Rights, Article 10, and Protocol No. 1, Article 3. Open source

3. Council of Europe, Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries. Open source

4. Council of Europe, Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression. Open source

5. EEAS, Information Integrity and Countering Foreign Information Manipulation and Interference. Open source

6. EEAS, 2nd Report on FIMI Threats and Response Framework, 2024. Available through the EEAS FIMI page.

7. EEAS, 3rd Report on FIMI Threats, 2025, and 4th Report, 2026. Available through the EEAS FIMI page.

8. Council of Europe, Recommendation CM/Rec(2022)16 on combating hate speech. Open source

9. OSCE/ODIHR, Slovak Republic Early Parliamentary Elections 30 September 2023, Final Report, 29 February 2024. Open source

10. Constitutional Court of Romania, Decision No. 32 of 6 December 2024, as summarised in Council of Europe Parliamentary Assembly materials on foreign interference.

11. European Commission, TikTok election-risk data-retention order, 5 December 2024. Open source

12. European Commission, formal proceedings against TikTok concerning election risks, 17 December 2024. Open source

13. OSCE/ODIHR, Republic of Moldova Presidential Election and Constitutional Referendum 20 October and 3 November 2024, Final Report, 24 March 2025. Open source

14. Venice Commission, Interpretative Declaration to the Code of Good Practice in Electoral Matters on Digital Technologies and Artificial Intelligence, CDL-AD(2024)044. Open source

15. Council of Europe, Disinformation and electoral campaigns, legal and technical challenges. Open source

16. Council of Europe, Guidance note on the implications of generative artificial intelligence for freedom of expression, 2026.

Verify national law, current platform rules and institutional contact details before delivery. Where a case summary depends on an official decision or election report, use the full primary text rather than this training summary.

Training material to be shared with participants

Work from the evidence supplied. Separate what you observe from what you assess and what you cannot establish. Do not label accounts as bots, trolls or foreign proxies without sufficient evidence. For each proposed response, identify the responsible actor, legal or policy basis, urgency and freedom-of-expression safeguard.

Sheet 1 Classify the information problem

INDIVIDUAL AND GROUP TASK Concept sorting | SESSION TIME 5, 10 or 15 minutes

Items

A. A local newspaper publishes the wrong deadline for postal voting after misreading an official notice. It corrects the article when the EMB contacts it. No evidence of deliberate deception is available.

B. On election morning, a campaign team knowingly publishes a fabricated notice using the EMB's logo. It falsely claims that voting has been suspended in opposition strongholds and tells those voters to stay home until further notice.

C. A satirical account posts an obviously exaggerated video of every candidate dancing. The account and post are clearly labelled satire.

D. An anonymous channel publishes authentic private medical information about a candidate with a misleading headline two hours before voting begins.

E. Thirty accounts conceal their common operator and coordinate the same false claim about ballot counting. The available evidence does not identify whether the operator is domestic or foreign.

F. A foreign state-linked network and local proxies coordinate deceptive accounts and paid creators to undermine confidence in the electoral register.

Task

For each item, select the most useful working category: misinformation, disinformation, malinformation, satire, information manipulation, possible FIMI or another precisely defined category. More than one category may apply. Explain what is known and what remains uncertain.

Item	Working classification	Evidence and uncertainty	Appropriate first action
A			
B			
C			
D			
E			
F			

Questions

1. Which classification depends on evidence of intent?
2. Which classification requires evidence of a foreign link?
3. Which items may be harmful but remain protected expression?
4. What response can occur before attribution is complete?

Sheet 2 Map a narrative and possible harm

GROUP TASK Narrative and harm mapping | SESSION TIME 10, 15 or 20 minutes

Fictional material

Over three weeks, posts and short videos repeat these messages: “The register is controlled from abroad”; “media and civil society take orders from outsiders”; “real citizens will be erased”; and “the result has already been decided”. Some posts cite genuine administrative delays or accurately identify foreign grants received by independent organisations. Others falsely claim that an overseas software supplier can secretly remove names. The material appears in two minority languages as well as the majority language. No evidence supplied for the exercise establishes who coordinated or financed the posts.

Task

Distinguish individual claims from the wider narrative. Do not assume that every person who criticises the register belongs to a manipulation campaign.

Dimension	Group analysis
Message and verifiable claims	
Wider narrative and emotional cues	
Known creators and amplifiers	
Targeted institution, groups and audiences	
Distribution channels and observed circulation	
Plausible electoral harms	
Evidence needed to assess intent or coordination	

Dimension	Group analysis
Evidence needed to assess exposure or impact	

Questions

1. Which part should the EMB correct, and which part requires journalism or investigation?
2. Could an accurate fact still support a manipulative narrative? Explain.
3. Does a narrative alleging foreign control establish FIMI? What evidence would be required before making that attribution?
4. Which community messenger may be more trusted than a national institution?
5. How would you report the narrative without repeating it so prominently that you amplify it?

Sheet 3 Analyse behaviour and evidence

INDIVIDUAL AND PAIRED TASK Evidence ladder | SESSION TIME 15, 20 or 30 minutes

Fictional observations

During one evening, 12 public accounts post the claim “Ballot scanners discard every third opposition vote” and link to the same anonymous page. The posts appear between 20:00 and 20:08 and use identical wording. Eight accounts were created during the previous seven days and use generic profile images.

Within the next 20 minutes, bursts of comments repeat two identical slogans under three news articles about election technology. Four long-established activist accounts share the claim later, adding their own comments and different images.

The team has public posts, account creation dates and timestamps. It lacks platform data on account control, devices, location, automation, payment or recommendations. It has not yet verified the scanner claim.

Evidence ladder

Level	What the evidence supports
Observation	
Indicator and alternative explanation	
Coordination assessment and confidence	
Inauthentic or automated behaviour	
Attribution	

Level	What the evidence supports
Electoral impact	

Questions

1. Which facts may indicate coordination? Which genuine behaviour could look similar?
2. Can the accounts be called bots or trolls? What evidence would be needed?
3. Should established activists be grouped automatically with the early accounts?
4. Can the content be called disinformation before the scanner claim and intent are checked?
5. What evidence would disconfirm your preferred hypothesis?
6. What public evidence should be preserved, and what personal data should not be published?

Preliminary wording

Observed pattern: .....

Assessment and confidence: .....

Unsupported conclusion to avoid: .....

Next verification step: .....

Sheet 4 Synthetic-media incident room

ROLE SIMULATION Slovakia-inspired scenario | SESSION TIME 15, 20 or 30 minutes

Scenario

At 18:00, two days before an election and after the campaign moratorium begins, an anonymous account posts audio that appears to capture a leading candidate and a journalist discussing how to manipulate the election. The candidate says it is fabricated. The journalist cannot be reached immediately.

At 18:20, six political accounts share the clip. At 18:40, a large news account reports that "audio alleging election fraud is spreading" and embeds it. By 19:00, edited versions with subtitles circulate on three platforms and in a messaging service. One synthetic-media detector returns 72 per cent "likely generated"; another returns "inconclusive". The EMB has no information that election systems are compromised.

Assigned role

Election management body / regulator / judge or lawyer / journalist / civil society and fact-checker / platform team

First 15 minutes

1. What will you preserve?
2. What exact claim must be checked?
3. Who will you contact, and through which pre-agreed channel?
4. What can your role lawfully and practically do now?
5. What will you avoid saying or doing?

Incident assessment

Factor	Assessment and evidence
Potential harm	
Observed circulation	
Time sensitivity	
Confidence in authenticity assessment	
Coordination indicators	
Legal or policy threshold	
Immediate action and review time	

Sheet 4 Continued

Update at 19:15

The journalist confirms that the conversation never occurred and provides an original recording from which several words appear to have been taken. A forensic specialist says the circulated audio shows strong signs of manipulation but needs more time to determine the method. An official election-information page is available in three languages. The platform has acknowledged the urgent escalation but has not acted.

Task

Revise the assessment. Prepare a short internal note and a public response of no more than three sentences. Lead with verified information and practical voter guidance. Decide whether reproducing or linking to the audio is necessary.

Internal note

Observation: .....

Assessment and confidence: .....

Remaining uncertainty: .....

Action, responsible actor and review time: .....

Public response

.....

.....

.....

Coordination check

What do you need from the other professional roles?

.....

What must remain independent rather than coordinated?

.....

Sheet 5 Select and draft a response

GROUP TASK Proportionate response | SESSION TIME 15, 20 or 30 minutes

Incident options

Choose one: the false election-day voting-suspension notice from Sheet 1; the foreign-influence and register narrative from Sheet 2; the suspected coordinated scanner claim from Sheet 3; or the manipulated audio from Sheet 4.

Response menu

Monitor and preserve; fill the information gap; prebunk; correct or debunk; investigate and report; escalate to a platform; regulatory or legal action; safety response; strategic action after supported attribution.

Response plan

Decision	Group answer
Harm to reduce	
Evidence and confidence	
Target audience and trusted messenger	
Selected response and responsible actor	
Legal or policy basis	
Less restrictive alternative considered	
Amplification and safety risk	
Accessibility and language	
Review time and success indicator	

Draft public message

Write no more than three sentences. State what is verified, what voters should do and where authoritative information is available. Do not speculate about attribution.

.....

.....

.....

Peer review

Is the message timely, accurate and understandable? Does it close the information gap without repeating harmful material unnecessarily? Is the action within the actor's mandate and proportionate to the evidence?

Sheet 6 Compare recent election cases

OPTIONAL GROUP TASK Evidence and safeguards | SESSION TIME 10 or 15 minutes

Case A Slovakia parliamentary election 2023

Shortly before the 30 September election and during the campaign moratorium, manipulated audio circulated purporting to capture a discussion about electoral manipulation between a political leader and a journalist. ODIHR reported multiple deepfake audio clips and wider concerns about manipulative content from foreign and domestic actors.

Source: OSCE/ODIHR, Slovak Republic Early Parliamentary Elections, Final Report, 29 February 2024. Open source

Questions: Why did timing matter? What could actors prepare before a moratorium begins? Which conclusions about electoral impact would require more evidence?

Case B Romania presidential election 2024

Romania's Constitutional Court annulled the first-round result on 6 December 2024 after finding breaches of essential principles of free democratic elections. Declassified information indicated a mass online influence operation and undisclosed promotion benefiting a candidate. The European Commission used Digital Services Act powers to preserve platform data and later opened formal proceedings concerning systemic election risks.

Sources: Romanian Constitutional Court Decision No. 32 of 6 December 2024; European Commission actions of 5 and 17 December 2024.

Questions: Which parts concern content, campaign transparency, platform systems and election remedies? Why should annulment not be treated as an ordinary or automatic response to online manipulation?

Sheet 6 Continued

Case C Moldova presidential election and referendum 2024

ODIHR concluded that both rounds were well managed and contestants could campaign freely overall, while the campaign environment was affected by interference from abroad and active disinformation. The case involved institutional measures as well as continuing questions about illicit finance, online enforcement and equal opportunity.

Source: OSCE/ODIHR, Republic of Moldova Presidential Election and Constitutional Referendum, Final Report, 24 March 2025. Open source

Questions: How can institutions respond actively while preserving pluralism and legal safeguards? What should observers assess beyond the number of incidents?

Group comparison

Select one case and complete the record.

Question	Group answer
Verified fact from the source	
Behaviour or narrative at issue	
Responsible institutional actors	
Evidence still needed	
Response used or available	
Freedom-of-expression or due-process safeguard	
Unsupported claim to avoid	

Transfer question

Which lesson can be adapted to your context, and which feature is too country-specific to transfer directly?

.....

Reusable incident record

PRACTICE FORM One record per incident and version every update

Incident ID, analyst and date: .....

Election phase and urgency: .....

First known public observation: .....

Content and narrative

Exact claim and format: .....

Wider narrative and language variants: .....

Targeted procedure, person, institution or community: .....

Source and distribution

First known source and known amplifiers: .....

Platforms or channels and collection times: .....

Observed metrics with definitions: .....

Possible paid, coordinated or inauthentic behaviour: .....

Alternative explanations: .....

Verification and assessment

Evidence preserved and sources consulted: .....

Verified facts: .....

Assessment and confidence: .....

Attribution status and basis: .....

Potential or observed harm: .....

Missing evidence and data limitations: .....

Decision

Applicable rule or policy and competent actor: .....

Response, message and channel: .....

Less restrictive alternative considered: .....

Data protection and safety steps: .....

Escalation contact and time: .....

Review time, outcome and next action: .....

Retain the original record when the assessment changes. Store evidence securely, collect only necessary personal data and distinguish a public-interest finding from an allegation that still requires verification.

COUNCIL OF EUROPE

HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW



DROITS DE L'HOMME, DÉMOCRATIE ET ÉTAT DE DROIT

CONSEIL DE L'EUROPE

MODULE 5
DISINFORMATION AND INFORMATION MANIPULATION

Purpose and learning outcomes

- Distinguish inaccurate information from intentional manipulation
- Analyse narratives, actors, behaviour, distribution and harm
- Use indicators without prematurely labelling bots or foreign proxies
- Assess synthetic media through provenance, context and circulation
- Separate observations, analytical judgments and attribution
- Choose a timely response that protects freedom of expression

90, 120 AND 180 MINUTE ROUTES

The analytical focus

CONTENT	BEHAVIOUR	HARM
What is claimed, implied, altered or omitted?	Who acts, how they coordinate and how content spreads	What electoral process, person or community may be affected

Attribution and impact require stronger evidence than detection.

Core safeguards

- Political speech receives strong protection
- Criticism of institutions does not become manipulation merely because it is uncomfortable
- Restrictions require a legal basis, legitimate aim, necessity and proportionality
- Transparent and non-discriminatory procedures protect against selective enforcement
- The least restrictive effective response should address the identified harm

Working distinctions

MISINFORMATION	False or inaccurate information without established deceptive intent	**DISINFORMATION**	False, inaccurate or misleading information deliberately used to deceive and cause harm or gain
MALINFORMATION	Genuine information disclosed or used with intent to cause harm	**PROPAGANDA**	Communication designed to shape political attitudes or action
HATE SPEECH	Expression assessed under the applicable definition and law	**INFORMATION MANIPULATION**	Intentional conduct that distorts the information environment

CONCEPT SORTING | SHEET 1 | 5–15 MINUTES

Intent changes the classification

ERROR

A newspaper misreads an official deadline and promptly corrects it

DECEPTION

A campaign knowingly fabricates an EMB notice to suppress turnout

Professional action can begin while intent and origin remain under investigation.

FIMI requires a supported foreign dimension

OBSERVED PATTERN

Intentional and coordinated manipulative behaviour may be assessed before origin is known

FIMI ATTRIBUTION

Evidence must support cross-border actors, state links or proxies

Narrative alignment with foreign interests does not establish attribution.

From item to narrative

POST — One observable item

CLAIM — A proposition that can often be checked

NARRATIVE — A recurring frame that connects events, actors and emotions

Narratives may mix facts, opinions and false claims.

Narrative and harm map

MESSAGE	Claim, implication, omission and emotional cue	**ACTOR**	Creator, first publisher, endorser and amplifier
TARGET	Procedure, institution, contestant or community	**BEHAVIOUR**	Coordination, deception, automation or account recycling
DISTRIBUTION	Channels, creators, advertising and recommendation	**HARM**	Confusion, suppression, intimidation or distorted opportunity

GROUP MAP | SHEET 2 | 10–20 MINUTES

Foreign control narrative

"The register is controlled from abroad. Media and civil society take orders from outsiders."

- Some posts cite genuine delays or foreign grants
- Other posts falsely claim that an overseas supplier can erase names
- The material appears in majority and minority languages
- No supplied evidence identifies who coordinated or financed it

Electoral harm extends beyond persuasion

PROCEDURE	Confuse voters about registration, polling or counting
PARTICIPATION	Suppress turnout or deter candidacy
SAFETY	Intimidate candidates, officials, journalists or communities
COMPETITION	Distort equal opportunities and access
TRUST	Erode confidence and crowd out reliable information

Behavioural indicators

- Near-simultaneous posting or repeated wording
- Shared links to low-credibility domains
- Clusters of new accounts or copied profile material
- Sudden changes in account topic or systematic replies
- Coordinated hashtags, paid promotion or cross-platform seeding
- Combinations and persistence matter more than one signal

Evidence ladder

OBSERVATION	Captured posts, times, wording and public metadata
INDICATOR	An unusual pattern with plausible alternatives
COORDINATION	Repeated temporal, linguistic or network connections
INAUTHENTIC OR AUTOMATED	Evidence of deceptive identity or automated operation
ATTRIBUTION	Corroborated links to an organisation, campaign, state or proxy
ELECTORAL IMPACT	Evidence of exposure, response or institutional disruption

EVIDENCE LADDER | SHEET 3 | 15–30 MINUTES

Bots, trolls and inauthentic behaviour

BOT	An automated account or process
TROLL	An imprecise label for provocative or disruptive activity
COORDINATED INAUTHENTIC BEHAVIOUR	Deceptive coordination about actor identity or origin

High posting volume alone supports none of these labels.

Ballot scanner scenario

Twelve accounts post the same claim and link within eight minutes.

- Eight accounts are less than seven days old
- Bursts of identical comments appear under three news stories
- Four established activists share the claim later with their own comments
- No platform data establish control, devices, automation, payment or recommendation

Behaviour exercise debrief

SUPPORTED	A medium-confidence hypothesis of coordination
NOT ESTABLISHED	Automation, payment, common control, foreign origin or falsity
DO NOT MERGE AUTOMATICALLY	Later organic sharing by established activists
NEXT EVIDENCE	Claim verification, archives, public links and lawful specialist support

Generative AI changes scale and speed

RISKS	USES
Impersonation	Translation
Fabricated evidence	Accessibility
Personalised harassment	Journalistic production
Rapid variations	Voter information

The assessment still requires authenticity, context, distribution and harm.

Synthetic media triage

PRESERVE	Original item, URL, timestamp and account context
DEFINE	The precise claim and voter decision at issue
VERIFY	Authoritative sources and the depicted person or institution
ASSESS	Circulation, timing, vulnerable audiences and amplification risk
LABEL CAREFULLY	Verified, likely, uncertain or false
ESCALATE	Use the incident protocol and fill the information gap

Slovakia 2023 incident room

Two days before polling, during the moratorium, manipulated audio appears to capture a candidate and journalist discussing electoral manipulation.

- The candidate says it is fabricated
- Political accounts, news accounts and edited versions amplify it
- Two detectors return different assessments
- The EMB has no evidence that election systems are compromised

The incident update

19:15 UPDATE

- The journalist confirms that the conversation never occurred
- An original recording appears to contain source fragments
- A specialist finds strong signs of manipulation but needs more time
- The platform acknowledges the urgent escalation but has not acted
- Official election information is available in three languages

Minimum incident record

INCIDENT	Identifier, first observation, phase and status	**CONTENT**	Exact claim, format, language and narrative
SPREAD	Source, amplifiers, platforms, timing and metrics	**HARM**	Target, plausible harm and observed harm
EVIDENCE	Preserved material, sources and contradictions	**DECISION**	Responsible actor, response, channel and review time

Risk and urgency

POTENTIAL HARM

What could happen if the claim spreads?

CIRCULATION

What public evidence shows spread or reach?

TIME

How soon could the harm become irreversible?

CONFIDENCE

Which underlying facts have been verified?

Three layers of analytical writing

OBSERVATION

Twelve accounts posted identical wording and the same link within eight minutes.

ASSESSMENT

The similarity supports a medium-confidence coordination hypothesis.

ATTRIBUTION

No public evidence identifies control, automation, funding or a foreign actor.

WRITE EACH LAYER SEPARATELY

Minimum verification questions

- Can a primary source or independent evidence check the claim?
- Is the source authentic and in its original context?
- Who first published it, and what is known about that actor?
- Does the pattern differ from a documented baseline?
- Is paid promotion or cross-platform seeding visible?
- What evidence remains unavailable because of privacy or platform limits?

Response options

MONITOR AND PRESERVE	Limited evidence or circulation with a review trigger
FILL THE INFORMATION GAP	Clear facts through trusted and accessible channels
PREBUNK OR CORRECT	Explain a foreseeable technique or lead with verified information
INVESTIGATE AND REPORT	Verify the operation without unnecessary reproduction
PLATFORM ESCALATION	Use an established channel and applicable rule
LEGAL OR SAFETY RESPONSE	Act within authority, due process and proportionality

RESPONSE PLAN | SHEET 5 | 15–30 MINUTES

Public communication principles

- Lead with verified information and the action voters should take
- Use a messenger trusted by the affected audience
- Provide accessible formats and relevant languages
- State uncertainty honestly
- Coordinate facts and roles rather than political messaging
- Review whether the response reduced confusion or amplified the claim

Recent election cases

OPTIONAL OR EXTENDED

SLOVAKIA 2023	Manipulated audio, moratorium timing and limited response time
ROMANIA 2024	Mass online influence, undisclosed promotion and exceptional judicial remedy
MOLDOVA 2024	Foreign interference, active disinformation and coordinated institutional response

Romania 2024

ELECTION REMEDY

The Constitutional Court annulled the first-round result on 6 December 2024

PLATFORM SUPERVISION

The European Commission preserved data and opened DSA proceedings on systemic election risks

The case illustrates the difficulty of obtaining a graduated remedy before fast-moving harm affects an election.

One incident, different professional tasks

REGULATORS	Triage a complaint and give reasons for a proportionate response	**EMBs**	**OPTIONAL OR EXTENDED** Close a procedural information gap and activate escalation
LAWYERS / JUDGES	Test evidence, legality, safeguards and remedy	**POLICYMAKERS**	Design mandates and protocols before the campaign
JOURNALISTS	Decide whether, when and how to report	**CIVIL SOCIETY / OBSERVERS**	Document narratives and publish a scoped finding

Learning check

Ten accounts publish the same false polling-place address within five minutes.

- Write one observation
- Write one assessment with confidence
- Name one unsupported conclusion to avoid
- State one immediate response and responsible actor

EXIT TASK | 5–10 MINUTES

Key messages

- Not every inaccurate statement is disinformation
- Manipulation analysis examines actors, behaviour, distribution and purpose
- Indicators justify inquiry but do not prove bots or foreign control
- Attribution requires stronger evidence than detection
- Electoral harm includes procedural confusion, intimidation and suppressed participation
- Effective responses reduce harm while protecting lawful expression

END OF MODULE 5