Crisis Communication and Combating Disinformation:

Playbook Template for Electoral Management Bodies

Updated January 2022

About this Document

To support preparedness in crisis communications planning, the International Foundation for Electoral Systems (IFES), in partnership with the Brunswick Group, has developed this playbook template, which outlines key approaches and considerations for establishing effective responses to threats of disinformation.

The template that follows outlines key components of a strategic communications plan that Electoral Management Bodies (EMBs) can build out, add as a module to existing plans, or tailor to the needs of their country with support from IFES. The sections of the template and their order are only suggestions and should be retained, amended, or deleted based on local needs. The content is in a template format, including bracketed text where the details relevant to each EMB and country can be filled in.

Note: This playbook template was updated in January 2022 by the Brunswick Group for IFES' use with EMBs. Any modifications or additions to the template and accompanying training materials are the responsibility of IFES and/or the EMBs. Responsibility for the accuracy and timeliness of the plan and subsequent updates also rest with the individual EMBs and approaches should be tailored to meet individual needs.

Table of Contents

Overview

In every phase of election administration, the importance of training, planning, and testing ahead of time is a critical component of Electoral Management Bodies' (EMBs) preparedness. In today's dynamic political and data environment, every EMB will likely have to respond to a misinformation or disinformation challenge at some point. Whether preparing for a disinformation incident or another type of crisis, this plan can assist the EMB to develop a well-thought-out plan and response that will better equip EMBs to maintain public trust and protect electoral integrity.

The top priority to counter any type of targeted disinformation event is to mitigate the impact of the disinformation and maintain public trust. The most effective way to achieve that goal is to be prepared, so you can respond confidently and quickly.

Key Definitions

- **Misinformation –** false, inaccurate, or incomplete information that is spread mistakenly or unintentionally
- **Disinformation –** false or inaccurate information that is spread deliberately, most often by adversaries. This includes technically factual information purposely presented in a misleading way and may include amplification by a bot or other inauthentic account
- **Stakeholder –** an internal or external individual, group, organization that needs to be informed about a disinformation incident even if their point of view may differ
- **Validator –** an external individual, group, or organization that can help provide accurate information to counter disinformation during an incident and/or help educate the public during "steady state"

Audiences

Each EMB will likely encounter multiple types of audiences in the general public, ranging from individuals who are strong advocates for free and fair elections to those who are highly distrustful and antagonistic towards government leaders and institutions. It is critical to keep in mind the broad spectrum of audiences the EMB will encounter. This will help enable effective prioritization when creating a strategy and drafting communications. Generally, audiences can be broken into four segments:

- **Advocates –** Individuals and groups who are favorable to EMBs and other organizations that are working to protect election integrity. They are willing to and be counted on or can be easily motivated to defend election integrity in public.
- **Persuadables –** Individuals and groups who have general awareness of efforts to protect election integrity and may be willing to more actively support this work if engaged appropriately.
- **Susceptibles –** Individuals and groups whose media literacy and awareness of measures to protect election integrity may be low; or have greater exposure to historical distrust and grievances. Often the key target of domestic or foreign misinformation and disinformation narratives.
- **Detractors –** Individuals and groups who are highly distrustful and antagonistic towards government leaders, public institutions, and efforts to protect election integrity. While

consideration should be given to engaging, the attitudes of this audience are very difficult to change and may not be worth the highest priority effort.

In today's divisive social and political environment, there is no single tactic or counter-narrative that can blunt the effect of misinformation and disinformation across all audiences. One way to strengthen resilience against misinformation and disinformation is by engaging in targeted reputation-building and educational activities towards persuadable and susceptible audiences. It can also be bolstered by educating advocates so they can deliver accurate messages about election integrity to multiple audiences. Altogether, building a strong base of support among local decisionmakers and influencers can build resilience in the general public conversation around election integrity.

Demonstrating Your Values

Demonstrating your values is the best way to protect your reputation in challenging circumstances. Discussing your institutional values publicly should inform your stakeholders about the workings of the EMB and build their resilience against false information.

Every EMB should consider: What are the guiding principles, values, professional standards, and ethical considerations that you want the wider public to know about your electoral system? Among these values and principles, which ones would make the public less likely to accept disinformation about the EMB? How can you display these values to the public in ways that are widely accessible and understood?

Principles should be inspiring and engaging, but also achievable and genuine. No system is perfect, and disinformation actors will exploit and sensationalize imperfections in the system. Therefore, humility and honesty are key. Acknowledging mistakes, and noting how checks and balances come into play, is important in building credibility and trust.

More robust civic and voter education can help equip citizens to withstand these disinformation narratives and EMBs need to play a role to ensure the public knows what the EMB stands for and how it operates. Values the public should know about your EMB and electoral process include:

- ____
- ____
- ____
- ____
- ____

Building Resilience to Combat Disinformation

Proactively educating your key stakeholders is one of the most effective tools to help build resilience to disinformation. It is, in effect, trying to inoculate the public against at least the most egregious disinformation attempts. Establishing a regular series of communications (online, on television, and in-person) with the media and the public will help establish credibility and increase public education about civics basics.

The first time they hear from you should not be when you are trying to combat disinformation.

There are several actions the EMB can take to build resilience, such as:

- Establish yourself as a credible source of information
- Use local events, such as school programs, youth organizations, or social or religious groups to connect with community members and raise awareness of the history and current processes related to elections
- Strengthen relationships with advocates and even find common ground with open-minded critics when possible

Each EMB should determine what types of outreach make the most sense in their community—especially, to reach advocates, persuadable and susceptible audiences. What is your EMB doing now? What more should be done moving forward?

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

What more should be done moving forward?

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

Additionally, how do outreach efforts reach different communities and respond to the experiences of different marginalized groups? What more could be done to reach different communities with messages intended to speak to their needs and experiences?

- ______________________________
- ______________________________
- ______________________________
- ______________________________
- ______________________________

Common Disinformation Themes

A goal of disinformation is to erode public faith in the values that uphold your country's electoral system. These attacks often seize on existing, and sometimes legitimate, critiques of the system and then grossly distort them to anger and mobilize skeptics. Below are three prevalent themes that are routinely used by foreign and domestic actors seeking to undercut faith in the electoral process.

- EMBs are a tool of the political elite and/or a certain political party
- EMBs tolerate, protect, and cover-up manipulation of the election process and results
- Security flaws in election technology, voting materials, and/or processes delegitimize election outcomes

Completing a Self-assessment of Your EMB's Vulnerabilities

Disinformation is most effective when there is some amount of believability. Developing this list requires an honest self-assessment of past issues, myths, controversies, and controversial decisions that have generated interest in the past.

What are some of the key narratives that are likely to be the source of disinformation related to the electoral system and process in your country?

- ____
- ____
- ____
- ____
- ____
- ____

Good Practices for Countering Disinformation

Every misinformation or disinformation scenario is different and requires creative thinking to counteract. However, several good practices for dealing with disinformation have emerged over time. These include:

- **Be accurate.** Disinformation related to the electoral system feeds off exploiting any inaccuracy or mistake to cast the EMB or a political party in the worst possible light. You need to ensure you are operating from a factual position, so check your facts with multiple sources before citing them publicly. Ask all appropriate questions and put in the work before you speak to ensure that you do not accidentally provide misleading information.
- **Lead with facts.** Avoid repeating misinformation or disinformation. Starting your rebuttal by repeating the false allegation or rumor can inadvertently reinforce that myth in the mind of your audience. Instead focus on providing accurate facts first and do not lead with or repeat false messages. For example, if a story on the local news misconstrues a quote from a spokesperson for the EMB in a misleading way, the response should focus on where accurate and verifiable information can be found, not on repeating the false information from the news story.
- **Develop a simple, accurate, short counter-message.** Avoid complex messages. Develop a clear statement that contains the facts. Speak plainly.
- **Be visual.** False information on social media is often compelling because it is paired with engaging images. When appropriate, getting your message out with your own compelling image or well-designed graphic can capture the public's attention. For example, vote counting procedures explained through an infographic or flow chart will be more accessible to the public than through technical jargon.
- **Establish your verified voice.** Use your social media platforms, like Facebook and Twitter, to regularly point to where voters can find reliable information on election processes and EMB values. Establish your channels as the go-to sites to find accurate information with key stakeholders so they go there first.
- **Respond quickly and consistently.** Disinformation can spread rapidly. Your counter-message should be ready to be disseminated as soon as possible. If you are still gathering facts say so, but always take the opportunity to direct your audience to where they can

find verified information online. Share your message consistently and repeatedly across platforms.

Guidelines for Communicating with the Media

- **Align with credible media sources and build relationships in advance.** Identify credible media sources that are committed to accurate journalism. Doing so will allow you to have a more open conversation in the middle of a crisis. Reporters that have a baseline understanding of how the EMB works are less likely to be deceived by clearly false information or rumors. If a credible journalist or outlet is not available, focus on direct outreach via social media and/or your website.
- **Accept that you cannot avoid media coverage.** Disinformation will frequently be picked up by a wide range of reporters. You will likely need to talk to the media to get an accurate narrative out widely. If you don't, you risk having others tell your story and it will likely be more hyperbolic and less factual than the actual story.
- **Avoid saying "no comment."** It leaves the impression you have something to hide. You can explain, if appropriate, why it would be irresponsible to speculate before having all the facts. You can also explain the reasons for EMB rules that may prevent you from commenting on a case. Speak about issues as directly as possible and avoid "wiggle words" like "so far as we know."
- **Work with journalists to counter misinformation.** Misinformation can easily spread from social media to traditional media outlets. Journalists may unknowingly re-post or quote messages that originated with fake accounts. By forming relationships with journalists before disinformation spreads, you can provide accurate information and encourage them to ignore misinformation.

Guidelines for Communicating with the Public

- **Make your communications about your most important stakeholder – the voter.** There will be a temptation to discuss the components of the incident or respond directly to the sources of disinformation. Instead, talk about what you are doing to address public needs or concerns in this specific situation.
- **Speak plainly and directly.** Heavy legal or technical jargon can be off-putting to nontechnical audiences. Use anecdotes and examples to demystify relevant issues whenever possible.

Building a Rapid Response Process

The first step in building preparedness to combat disinformation about the EMB and electoral processes is developing or updating your internal and external response processes.

Developing Your Process

The following steps will guide your development/updating of your response processes:

1. Create a disinformation response team (DRT). The DRT should determine when and how to convene and establish a decision-making process that will be used during an incident.
2. Map and analyze internal and external stakeholders that should be considered in a disinformation situation.
3. Set-up/refine processes to monitor for disinformation online.
4. Establish an escalation process to determine the severity of the incident.
5. Establish a drafting and approval process for key messages.
6. Establish a feedback loop.

A description of each of these steps in the process can be found below.

Establishing an Internal Disinformation Response Team (DRT)

Maintaining a coordinated process establishes effective and efficient communications planning and response procedures. The structure and organization of a DRT will depend on the hierarchical structure in each country. The DRT should include representation from your Public Relations Department, Strategic Communications Unit, or Public Outreach division, or equivalent. If possible, you can include in this team individuals across multiple departments to enable faster verification. For example, if there is a rumor that something has gone amiss at a polling station, having someone from the Election Operations side of the EMB can be useful to quickly verify. Additionally, members of the DRT should have enough seniority represented to ensure the DRT is able to make decisions quickly.

Depending on the structure of your EMB, it might make sense to create a stand-alone entity reporting directly to the Chief Elections Officer, EMB Spokesperson, or in some instances, the Chairperson's office to ensure the DRT is cross-cutting across the institution.

Below is a templated chart that should be adapted to your organizational structure and filled in. The team should be organized based on the title and role within the EMB, not the individual. The size of the DRT will depend on the structure of the EMB in your country. When building out your DRT, focus on making sure the right decision-makers are included, rather than the number of people that make up the team—and be sure to include a leader, who can drive the group to quick decisions. Additional roles that may make sense have been included in the templated chart below but should be tailored based on your structure.

Position	Designated individual and contact information	Designated back-up and contact information	Role on the DRT
			Leader
			Spokesperson
			Legal counsel
			IT / Cybersecurity
			Operations

Activating a DRT

Your DRT should be "activated" whenever notable disinformation is discovered that could interfere with the electoral process or its trust and integrity in the country. The activation process may vary but at a high-level should include the following activation steps:

1. DRT lead is made aware of disinformation.
2. DRT lead convenes team.
3. DRT uses the escalation protocol framework to determine severity of the incident and appropriate response plan.
4. DRT confirms roles and responsibilities during the incident.
5. DRT lead establishes regular cadence for DRT meetings until incident is de-escalates.

Early Warning Tools

Early warning tools can be used to help quickly identify narratives and get ahead of disinformation efforts. Digital media monitoring of the issues that are of the most relevance and biggest concern can help identify potential threats at the earliest possible stage. To use these tools effectively, EMB communicators need to understand what the biggest disinformation threats are in their context. Doing this due diligence upfront will allow you to come up with a series of search terms that can be programmed into social media tools to effectively warn you before disinformation runs rampant.

Depending on the EMB's size, this may be an effort that is most effective if coordinated with other entities such as intelligence services, communication ministries, and/or credible CSOs.

Potential Tools

Helpful social media tools, available at little or no cost, include:

- Google Alerts
- Google Trends
- Google Reverse Image Search

In recent years, a number of technology companies have also developed proprietary tools and services designed to help public and private sector organizations address the spread of online misinformation and disinformation. Many of these providers use artificial intelligence (AI) to track and identify potentially harmful content or emerging narratives across multiple social media platforms and online channels. These companies include:

- Logically
- Graphika
- ActiveFence
- Constella Intelligence
- Blackbird.ai
- Zignal Labs
- ZeroFox

Several of these companies have offerings to work with national and local government partners to monitor, detect, and counter harmful online content and activity related to election integrity.

While using AI-based technologies can complement the communications-driven activities described in this playbook, proprietary tools and services have varying costs and language coverage limits—and thereby may not be relevant for all EMBs.

First and foremost, an early warning tool can help identify potential threats quickly and provide more time for the DRT to be activated and a response plan to be formulated.

When tools are set up, you should familiarize yourself with how they work and establish protocols for contacting the social media platforms so the DRT can move quickly if they are requesting that disinformation about elections that could qualify as voter interference be taken down from a social media site. Please note there are no guarantees that information will be taken down as each platform has different standards for what violates their terms of service. The International Foundation for Electoral Systems (IFES) has working relationships with a point of contact at social media companies—including Facebook, Instagram, Twitter, Google, and YouTube—and can work as an intermediary if an EMB wishes to escalate and urgent concern.

The following are examples of types of coordination IFES may be able to facilitate between EMBs and social media platforms:

- Assistance with account issues, including taking down accounts imitating the EMB, restoring access to old accounts, and incident response in the case of compromised/hacked accounts.
- Support for local partners that are having difficulties with the Facebook/Instagram ad verification process or other difficulties placing ads intended to boost the visibility of civic content.
- Pre-electoral liaising between EMBs and social media companies. For example, to confirm election information such as voter registration or voting procedures that a platform may feature on or before Election day.

We recommend determining your best method for reaching key social media platforms before an incident occurs. Initiating a conversation with IFES on how best to facilitate communication with the platforms, if you do not already have a line of communication, may be a useful first step.

Stakeholder Outreach and Education

Before a crisis, it is critical to identify and establish relationships with key stakeholders. Key stakeholders may include civil society groups, local associations, media, social media companies, and the public. Working with these groups to listen to their concerns, be open about the procedures of the EMB, and share your values before a crisis increases the likelihood that they will vouch for you when misinformation/disinformation spreads.

Stakeholders should not only include groups with whom you are currently aligned. Building bridges with potentially adversarial yet respected civil society groups and members of the media may have more impact in a crisis. Support from unlikely allies can confound attempts by disinformation actors to sow discord between groups they want to place in opposition. At a minimum, having an open dialogue gives you options to address rumors directly with critics before they take an adversarial position. Relationships with respected legal experts and former government officials can help validate the work of the EMB because media will often reach out to these groups for independent comments on EMB activities. Having a dialogue with these figures will be helpful as they may be able to explain or comment on EMB procedures that you cannot.

Identifying key stakeholders ahead of time will ensure you can respond rapidly to activate this network when an incident occurs. What are the organizations in your country who have a vested interest in the independent electoral processes and whose opinions on your activities matter?

External Stakeholders

Stakeholder	Areas of Potential Assistance	Point of Contact
Council of Europe	Reports on combating disinformation based on analysis of key stakeholders.	
IFES	Technical assistance and social media engagement	dnorth@ifes.org
Academia (including law students)		
Media		
Advocacy group(s)		
Elected officials		

Internal Stakeholders

Internal stakeholders include other individuals, departments, or agencies within your government.

Stakeholder	Areas of Potential Assistance	Point of Contact

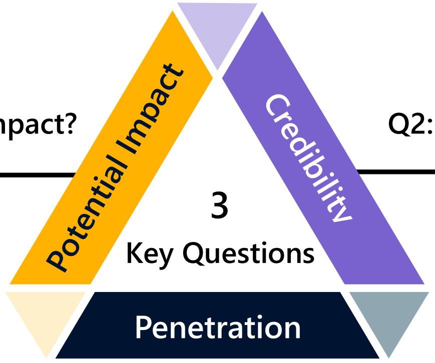
Escalation Protocol

An escalation protocol helps assess the severity of a disinformation incident. Not all disinformation requires the same level of response. Some disinformation—if it remains on the fringes and is already roundly rejected by key stakeholders—is best left monitored, as responding will only give the matter attention it does not deserve.

The three questions below provide a way to assess the level of risk that a disinformation narrative poses to the EMB. Using this structure, you can make decisions based on a consistent set of criteria to determine the level of risk.

Q1: What is the potential impact?

Could the narrative negatively impact the EMB's reputation or the integrity of the electoral system?



Q2: Is it credible to key audiences?

Is the narrative credible enough to cause concern among the EMB's key stakeholders?

Q3: What is the penetration of the narrative?

Is the content confined to online echo chambers or is it breaking through to mainstream audiences online?

The framework that follows is a starting point that you can tailor to meet your needs. These points in the framework should be considered during an incident, but all may not be necessary depending on the context of the situation. **It is usually easier to scale back an initial over-reaction than it is to catch up after you have insufficiently responded.**

SEVERITY: HIGH

A high severity incident occurs when disinformation is circulating in the public, on social media, or in local media that threatens to significantly undermine the EMB's credibility as an institution or credibility of election results for a prolonged period. It will likely have one or more of the following qualities:

- Prompts the public to question the credibility of your electoral process
- Damages confidence in the EMB
- Is currently or will result in inquiries from media (local, state, and potentially national), third-party groups, local and state officials, or political party officials
- Could lead to significant investigations into EMB personnel or department funding cuts

Key Considerations / Actions	**Potential Key Materials Checklist**
• Activate Disinformation Response Team (DRT). Identify disinformation narrative and establish ground-truth. • Reach out to relevant external stakeholders to educate, share key messages, and amplify fact-based information. • Develop a fact-based statement. If further investigation is required, deploy an interim statement. • Determine if broader public communication is appropriate. • Brief senior national or local officials. • Contact legislators, policymakers, or stakeholders as needed. • Reach out to third-party validators to vouch for the EMB with media. • Issue a follow-up statement once you have established the facts (if necessary). • Continue media and digital media monitoring and feedback loop. • Continue to push out fact-based statement across multiple channels, multiple times. • If applicable, consult law enforcement. • Alert national partners like IFES if additional support is needed and determine if it is appropriate to alert social media companies.	□ (Preferred) Fact-based statement deployed across multiple channels (EMB/agency website, social media, traditional media, shared with stakeholder groups). □ (If necessary) Interim statement to allow for more time to conduct an investigation. □ Key talking points taken from the statement. □ Peer communication/email. □ Develop/tailor clear, straightforward graphics, images, videos, or charts to provide correct information in a way that is visually appealing and easily digestible for your community. □ Email to social media contacts (if applicable). □ Website/social media materials. □ Visual infographics, charts, images, and videos as applicable. □ Media materials. □ Legislator/policymaker materials. □ Community leader / third-party validator materials or talking points (derived from key messages). □ Talking points for the EMB's spokesperson. □ Briefing for law enforcement. □ Follow-up media briefings.

SEVERITY: MEDIUM

The disinformation is circulating in the public, on social media, or in local media that has the potential to negatively affect the EMB's credibility and/or the integrity of the electoral process. The misleading information will likely spur questions from external stakeholders. It will likely have one or more of the following qualities:

- Prompts the public to question the credibility of your electoral process
- Is likely to result in inquiries from media (local, state, and potentially national), third-party groups, local and state officials, or political party officials

Key Considerations / Actions	**Potential Key Materials Checklist**
• Activate Disinformation Response Team (DRT). Identify disinformation narrative and establish ground truth. • Reach out to relevant external stakeholders to educate, share key messages, and amplify fact-based information. • Develop a fact-based statement. If further investigation is required, deploy an interim statement. • Determine if broader public communication is appropriate. • Issue follow-up statement once facts are established (if necessary). • Continue to push out fact-based statement across multiple channels, multiple times. • Continue media and digital monitoring and feedback loop. • Alert national partners like IFES if additional support is needed and determine if it is appropriate to alert social media companies.	□ (Preferred) Fact-based statement, deployed across channels (EMB/agency website, social media, traditional media, shared with stakeholder groups). □ (If necessary) Interim statement to allow more time to investigate. □ Peer communication/email. □ (If necessary) Develop/tailor clear, straightforward graphics, images, videos, or charts to communicate correct information in a way that is visually appealing and easily digestible. □ Email to social media contacts (if applicable). □ Website/social media materials. □ Visual infographics; charts; images; and video as applicable. □ Talking points for EMB spokesperson (if applicable). □ Community leader/third-party validator materials or talking points (derived from key messages).

SEVERITY: LOW

<table>
<tr><td colspan="2">The disinformation is circulating in fringe groups and has not reached mainstream conversation. At this stage, intervention is unnecessary because drawing attention to the information risks giving it more attention than it might otherwise receive. It will likely have one or more of the following qualities:
• Not receiving significant coverage
• Widely seen as implausible
• Poses a limited threat to the EMB’s credibility or the integrity of your electoral process</td></tr>
<tr><th>Key Considerations / Actions</th><th>Potential Key Materials Checklist</th></tr>
<tr><td>• Increase your dissemination of correct information in the places your community consumes news, like Twitter or Facebook.
• Prioritize traditional and digital media monitoring to continue to assess if the incident remains low severity.
• Reach out to relevant external stakeholders to educate, share key messages, and amplify fact-based information (if appropriate).</td><td>□ Draft communications to peer organizations, warning of the misleading information (if appropriate).
□ Email to social media contacts (if applicable).
□ Prepare contingency communications to be used if disinformation escalates to medium severity.</td></tr>
</table>

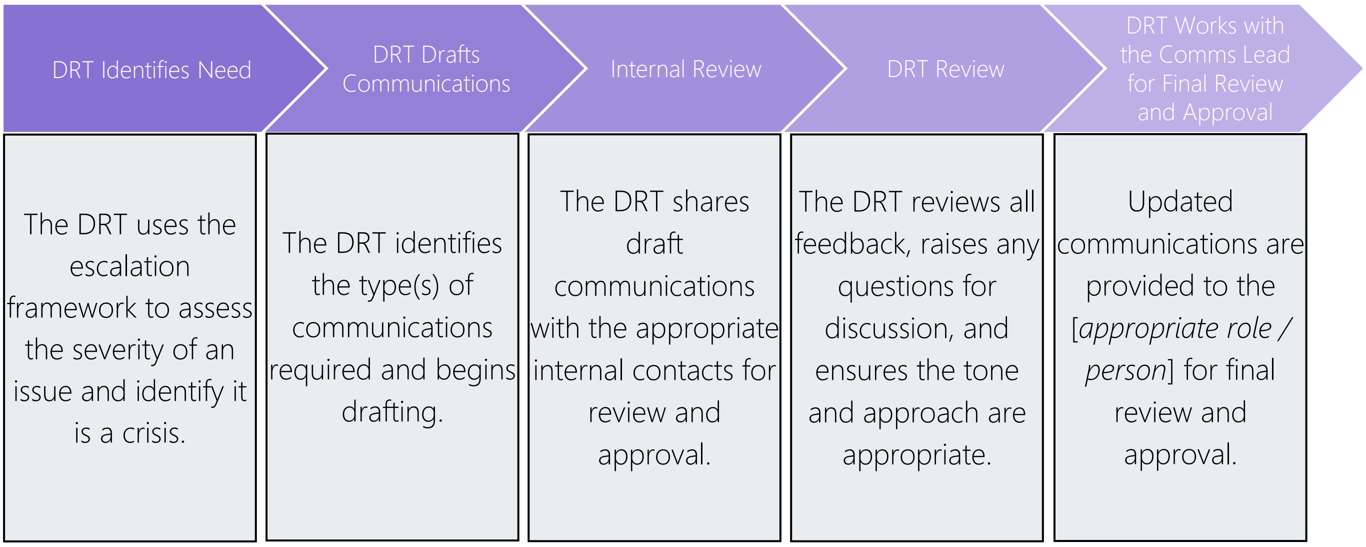
Activating Your Network

Once you have determined the severity of the disinformation (see Escalation Framework) it will be important to move quickly to activate your identified network of third-party validators who can amplify the counter-narrative as quickly as possible. In high and medium severity situations, aligning on the key messages and identifying the most important validators should happen right away. To make these decisions, the DRT should consider these key questions:

1. What are your objectives?
2. Who is your audience?
3. What disinformation are you trying to counter?
4. Who are the best people to validate and amplify your counter-narrative? (These individuals should be credible, trustworthy, and able to speak with authority and clarity on the issue).
5. How do you reach them?
6. Who should contact them?
7. What are you asking them to do?
8. Do you have contacts within the aggrieved audience that you could explain the situation to and ask them to convey accurate information to their stakeholders?

Content Drafting and Approval Process

The DRT will manage communications activities from the initial severity assessment to the drafting and dissemination of materials. The DRT will liaise with other internal stakeholders in the EMB during the process.



DRT Identifies Need	DRT Drafts Communications	Internal Review	DRT Review	DRT Works with the Comms Lead for Final Review and Approval
The DRT uses the escalation framework to assess the severity of an issue and identify it is a crisis.	The DRT identifies the type(s) of communications required and begins drafting.	The DRT shares draft communications with the appropriate internal contacts for review and approval.	The DRT reviews all feedback, raises any questions for discussion, and ensures the tone and approach are appropriate.	Updated communications are provided to the [*appropriate role / person*] for final review and approval.

Establishing a Feedback Loop

Establishing a means – both during and after an incident – to incorporate feedback from key stakeholders into your response is critical. During an incident, this work could take the form of media or social media monitoring and can be used to recalibrate messaging or approach. After an incident, you should write an after-action review and ensure lessons learned are incorporated into the Disinformation Response Plan Template.

Your after-action report should include:

- A summary of the incident (keeping in mind it could be subject to public disclosure)
- An overview of the operational response
- The communication objectives
- And an overview of the:
    - Incident
    - Outcome
    - Future recommendations

Incident Preparation and Rapid Response Checklist

What to do before the event

□ Establish a Disinformation Response Team (DRT) with contact information and back-up personnel as appropriate. Agree on roles and responsibilities

□ Map and analyze internal and external stakeholders

□ Establish a drafting and approval process for key messages

□ Discuss with IFES the possibility of establishing a direct line of communication with social media platforms

□ Decide what information can be communicated immediately and establish a feedback loop

□ Clarify the escalation protocol

□ Complete a self-assessment of the EMB's vulnerabilities

□ (Preferred) Set up early warning tools

□ Establish official voice with external stakeholders through ongoing proactive outreach and build public resistance through education

□ Regularly execute tabletop simulations to test the DRT and response process and develop additional scenarios

What to do during the event

Immediate actions (first 2 -3 hours)

□ Activate the DRT

□ Assess the disinformation severity using escalation protocol

□ Engage outside advisors, as necessary

□ Brief any necessary internal individuals/teams

□ Review and assess any legal obligations regarding disclosure or comment
First 24 hours
□ Confer with IFES on the viability of asking social media companies to take action, if necessary
□ Agree on internal roles and responsibilities for this incident, including spokesperson
□ Adjust and refine social media monitoring processes to track further dissemination of disinformation
□ Determine whether any pre-planned social content or media engagement should be put on hold/cancelled
□ Monitor traditional media for coverage
□ Draft a fact-based statement. If further investigation is required, draft an interim statement, leveraging pre-approved templates
□ Determine which channels to deploy fact-based statement or draft interim statement on and identify who will deploy the statement once approved
□ Receive approval for fact-based statement/interim statement
□ Deploy approved statement on pre-determined channel(s)
□ Conduct stakeholder assessment to determine most important audiences for this incident, leveraging pre-drafted stakeholder map
□ Draft appropriate core communications materials, leveraging templates, including: • Talking points • Press release • Q&A • Other materials as needed
□ Receive input on and approval of communications materials
□ Transmit approved materials, along with the instructions for distribution, to appropriate Communications Leads for transmission to assigned internal stakeholders
24 – 48 hours

□ Assess whether to launch a proactive digital strategy and determine protocol for when to directly engage with users on social media
□ Brief spokesperson(s) for any approved media engagements
□ Brief other relevant government officials for any approved media engagements
□ Conduct background/off the record media pre-briefing(s), if appropriate and necessary
□ Transmit approved materials, along with the instructions for distribution, to appropriate Communications Leads for transmission to assigned external stakeholders
□ Issue press release, if appropriate
72 hours and beyond
□ Field and triage media inquiries
□ Follow-up with key stakeholders (as appropriate) with any additional information/updates

What to do after the event
□ Record key learnings in an After-Action Report
□ Update playbook and template communications to reflect key learnings
□ Criminal, civil, regulatory action, if necessary and appropriate
□ Continue to monitor media and digital and, if applicable, update monitoring processes to reflect learnings from the incident
□ Continue reinforcing key messages and factual information at regular intervals
□ Re-engage external stakeholders to educate and build on existing relationships

Scenario Planning

Each EMB should engage in scenario planning and develop materials that can be adapted for use during an incident. To get started, we provide four examples that illustrate the range of issues for which each set of communications materials could be adapted. The scenarios have been drawn either from actual past events in one or multiple countries, or scenarios we anticipate being highly likely in the next few years. While no scenario is likely to fit your disinformation scenario exactly, the following possibilities reflect a range of incidents you may encounter based on the types of disinformation most likely to gain traction. You should adapt the scenarios to the issues you see as most likely and most challenging to respond to.

They are based on identified common themes, including:

- EMBs are a tool of the political elite and/or a certain political party
- EMBs tolerate, protect, and cover-up manipulation of the election process and results
- Security flaws in election technology, voting materials, and/or processes delegitimize election outcomes

Relevant scenarios that you need to prepare for include:

- ____
- ____
- ____
- ____
- ____

The following communications should be prepared for each scenario:

Interim Statement: The purpose of an interim statement is to allow officials time to gather information about the situation while remaining transparent about the existence of the incident – or an investigation into it. In some cases, an interim statement is useful in the event the media becomes quickly aware of an incident before officials intend to make the information public, to quickly address concerns and demonstrate grip of the situation.

Key Messages: The basis of all internal and external communications materials throughout an incident. This document is the only source of information from which your team should draft media statements, Q&A, website and social media copy, employee emails, and other communications materials. As new information becomes available, your team should update the key messages and circulate the most recent information to relevant officials.

Social Media Content: Facebook or Twitter posts that can be adapted for additional platforms.

Peer Communication: Communications developed to inform counterparts at the local, regional, and federal levels of the incident and provide guidance for any public communications they may issue.

Q&A: The Q&A materials should be used for those dealing with members of the media and other stakeholders. They should be updated and expanded as specific narratives or lines of questioning emerge, and as more information is known about the incident.

Images and Infographics: Your EMB may want to create and approve image templates and/or a bank of infographics in advance that can be adopted as needed. Good practice in disinformation response is to use straight-forward language and avoid jargon. Using infographics is a helpful way to communicate about complicated topics in a direct and eye-catching way. However, during an incident it might be challenging to set aside the necessary time to create these visuals. Creating a set of visuals in advance will ensure they can quickly be tailored to likely situations and shared more quickly alongside the other communications materials.

Scenario 1: Allegations by an opposition party that polling officials engaged in widespread fraud on Election Day

Scenario Summary

In the days before the presidential election, opinion polls consistently showed a lead in popular support for the opposition candidate. However, after the close of polls, a civil society organization announces exit poll results suggesting that the incumbent would be re-elected. Later that evening, the opposition candidate gives a press conference alleging widespread fraud by polling officials on Election Day, without providing any specifics, and calling for a new vote. Another civil society organization with ties to the opposition then announces that its exit polls show that the opposition candidate actually won by a large margin. It will take the EMB several days to finish counting the vote. Meanwhile, the allegations of fraud have spread quickly on social media, and the online space has become quickly flooded with speculation and misinformation. Some opposition supporters have begun to echo the opposition candidate's call for a revote or, perhaps, some kind of power-sharing arrangement.

Interim Statement

The [Electoral Management Body] is currently finalizing the vote count for the presidential election that took place on [date].

All election officials, including polling officials, go through extensive training before an election. Additionally, [appropriate organization or department within the government] oversees each election on site as an additional type of election oversight.

Anyone seeking an accurate overview of the processes in place to ensure a fair and unbiased election should visit [*our webpage – link to appropriate page/site*].

We encourage the public and all political parties to exercise caution when discussing the electoral process to avoid false or misleading information. As soon as the vote count is complete, we will release additional information.

Key Messages

- The election was conducted in full accordance with the law and no evidence of fraud at polling sites has been reported.
- Official sources of information about our electoral processes and the EMB's role can be found here [*insert relevant communications channels*].
- Online posts from unofficial accounts are not reliable sources of information and may be fake or peddling false information.
- The integrity of our electoral system is our top priority. There are established mechanisms to ensure elections have proper oversight and include appropriate checks and balances to eliminate fraud. More information about these oversight mechanisms can be found [*insert relevant webpage or communication channel*].
- Please exercise caution and verify information when you see accusations online based on false and misleading accounts of the election.

Sample Tweet

All official information about election proceedings can be found here [link to webpage]. Please exercise caution and verify information when you see accusations online based on false and misleading information about this [week's] election.

Peer Email

Dear [Colleague],

We are contacting you regarding the false accusations that polling officials interfered with the voting procedures in order to disrupt the outcome of this [week's] presidential election. All official sources of information about our electoral processes can be found [link to relevant webpage or communication channel]. While we take all accusations of fraud seriously, we have not currently identified any evidence that would suggest any wrongdoing in this election. I am writing to provide some information that may be helpful to you in responding to inquiries from the media or the public.

The false online posts and public accusations make claims that are designed to reduce public trust in the electoral system and vote outcome. These posts and statements are incorrect. The integrity of our electoral system is a top priority. There are established mechanisms to ensure elections have proper oversight and include appropriate checks and balances to eliminate fraud. More information about these oversight mechanisms can be found [insert relevant webpage or communication channel].

To investigate this matter, [name of relevant EMB officials] are coordinating with [relevant law enforcement and /or government agency]. As you know, disinformation investigations can take time and we want to ensure that all information we provide is accurate. We will provide more information when we can.

Please feel free to use the information above as you communicate with your colleagues and the public. If you have further questions, please contact [name of designated DRT member].

Sincerely,

[Name]

Q&A

Is it true that EMB trained polling officials interfered with voting procedures and influenced the outcome of this election?

- The election was conducted in full accordance with the law and no evidence of fraud at polling sites has been reported.
- Official sources of information about our electoral processes and the EMB's role can be found here [*insert relevant communications channels*].

Are these accusations a coordinated attempt to influence public trust in the electoral process?

- We cannot speculate about that. As you know, investigating disinformation can take time, and we want to ensure that all information we provide is accurate. We will provide more information when we can.
- To investigate this matter, [name of relevant EMB officials] are coordinating with [relevant law enforcement/government agency].

What evidence has been presented to assure the public that polling officials did not engage in fraudulent acts to disrupt the outcome of this election?

- Official sources of information about our electoral processes and the EMB's role can be found here [*insert relevant communications channels*].
- The integrity of our electoral system is our top priority. There are established mechanisms to ensure elections have proper oversight and include appropriate checks and balances to eliminate fraud. More information about these oversight mechanisms can be found [insert relevant webpage or communication channel].
- Please exercise caution and verify information when you see or hear accusations based on false and misleading accounts of this election process.

If the accusations are false, why did the opinion polls consistently show the opposition party in the lead before the election? Isn't it possible that the polling officials were influenced by the current administration and asked to change votes to ensure another term for the current party?

- This is an ongoing investigation, and we will provide more information when we can. We are coordinating with [relevant law enforcement / government agency].
- The integrity of our electoral system is our top priority. There are established mechanisms to ensure elections have proper oversight and include appropriate checks and balances to eliminate fraud. More information about these oversight mechanisms can be found [*insert relevant webpage or communication channel*].

Scenario 2: Rumors emerge online that there will be significant violence at polling stations on election day

Scenario Summary

In the weeks leading up to a national election, rumors began circulating online that extremist groups are planning to incite violence at polling stations across the country on election day. Networks of social media accounts with unclear origins push these narratives online until they are receiving daily coverage on television, as well. The public is growing increasingly concerned about whether it will be possible to vote peacefully and if it is safe to go to the polling stations on election day.

Interim Statement

[To be filled in]

Key Messages

[To be filled in]

Sample Tweet

[To be filled in]

Peer Email

[To be filled in]

Q&A

[To be filled in]

Images and/or Infographic

[To be filled in]

Scenario 3: Allegations that the EMB has deliberately delayed the supply of election materials to key opposition district(s) where a particular ethnic group is the majority.

Scenario Summary

Three weeks before a national election several significant storms hit the Northwest region of the country, delaying the delivery of election materials to this region. This part of the country is home to one particular ethnic group associated with the opposition party. Disinformation begins to circulate on Facebook that the EMB's explanation about the condition of the roads is incorrect and that the EMB is deliberately delaying the supply of election materials because these are key opposition districts. Old pictures of roads in excellent condition are shared online and falsely conveyed as the current condition.

Interim Statement

[To be filled in]

Key Messages

[To be filled in]

Sample Tweet

[To be filled in]

Peer Email

[To be filled in]

Q&A

[To be filled in]

Images and/or Infographic

[To be filled in]

Scenario 4: Forged documents that show that specific election commissioners interfered with the election outcome begin to circulate and go viral.

Scenario Summary

A set of forged email communications between two female election commissioners begin to circulate on social media. The fake communications make it look like these two female election commissioners are partial to certain political affiliations based on their love interests and note that they will do "anything" to help that party get into power, even if it means using their power to interfere with the election outcome. The email exchange was completely fabricated, but this is hard to prove – it is the word of the EMB vs. the well-done forged communications circulating online.

Interim Statement

[To be filled in]

Key Messages

[To be filled in]

Sample Tweet

[To be filled in]

Peer Email

[To be filled in]

Q&A

[To be filled in]

Images and/or Infographic

[To be filled in]