SMARTMATIC

Safeguarding Elections in the Age of Fake News

» Tools & tips for election officials to mitigate disinformation and respond in a crisis

"[Fake news and misinformation]

are not technical problems; they are human problems that technology has simply helped scale, yet we keep attempting purely technological solutions. We can't machine-learn our way out of this disaster, which is actually a perfect storm of poor civics knowledge and poor information literacy."

– Mike DeVito, researcher, Northwestern University

Chapter 1

A Perfect Storm

By now, everyone who works in or serves the election ecosystem has heard of fake news. Of course, the term "fake news" did not suddenly spring up during the 2016 US presidential campaign. It's existed under many names –from 'propaganda' to 'influence campaign'– for as long as human beings have used the spoken word. But the advent of social media has supercharged its impact like never before.

Public chatter about mis- and disinformation continues to skyrocket, accumulating 25 million mentions — a 30% increase from last year, according to data from Zignal Labs, an intelligence collection firm.

Two areas particularly vulnerable to misleading narratives are election systems and election processes. Inauthentic content around elections – including video, infographics, memes, factoids and articles – can significantly diminish election management bodies (EMBs) and their effectiveness. It is no longer enough for election officials to smartly and competently administer elections. They must fight fake news.

Disinformation forces organizations to defend their credibility, and that usually means new workflows and expenses. Efforts to identify disinformation and respond to it tax organizations, drawing time, money and resources away from the real work of elections. False information has also been anecdotally linked to staff attrition.

Creating effective strategies against disinformation disseminated by state and nonstate actors is an evolving practice. Election organizations need to support their staffs in these efforts and respond to falsehoods using well-defined, streamlined workflows instead of ad-hoc responses.

Communications experts agree that having a well-developed crisis communication plan is critical to managing a crisis, if and when it happens. This handbook includes best practices, guidelines and resources to help EMBs coordinate their internal and external communications responses to crises caused by misinformation or disinformation. The best plans to fight false information are integrated across the organization. This kind of holistic approach will help protect your reputation, your infrastructure and your staff.

> **Note:** In the years since the 2016 US presidential election, the term "fake news" has become pejorative, commonly associated with voters and politicians on one end of the political spectrum. For this reason, the remainder of this document will use the terms like misinformation (inaccurate/misleading information that is spread without malice) and disinformation (inaccurate/misleading information that is intentionally spread to harm or sow confusion) and a number of other synonyms for 'fake news.'

How False Information Impacts the Work of EMBs

The spread of false information – malicious or not – has profound effects, not just on the people and organizations involved in elections, but on every facet of society. Former Connecticut Secretary of State Denise Merrill called misinformation, "the issue of our lifetime."

A 2022 Pew Center survey reported that a median of 70% of people across 19 countries believe that the spread of false information online is a major threat to their country. In places like Canada, Germany and Malaysia, more people name false narratives as a threat than any of the other issues asked about in the survey[1].

Digital platforms not only provide channels for spreading false information, but offer tools to actively promote its dissemination until it's viral. A recent study by Soroush Vosoughi, Deb Roy, both of the MIT Media Lab, and MIT Sloan professor Sinan Aral stated:

> *"We investigated the differential diffusion of all of the verified true and false news stories distributed on Twitter from 2006 to 2017. The data comprise ~126,000 stories tweeted by ~3 million people more than 4.5 million times… Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information… Contrary to conventional wisdom, robots accelerated the spread of true and false news at the same rate, implying that false news spreads more than the truth because humans, not robots, are more likely to spread it."* [2]

The study further reported that falsehoods on Twitter are 70% more likely to be retweeted than true information.[3]

Correspondingly, The Science of Fake News report (Lazer et al., 2018) analyzed why "people prefer information that confirms their preexisting attitudes (selective exposure), view information consistent with their preexisting beliefs as more persuasive than dissonant information (confirmation bias) and are inclined to accept information that pleases them (desirability bias)." This explains why voters may be receptive to fake news and why individual biases might prevent acceptance of fact-checking of a given election-related fake news story.

Because of heightened interest in outcomes, election periods are ripe environments for internet trolls and other bad actors to incubate, test and share false and polarizing stories intended to deceive or influence readers.

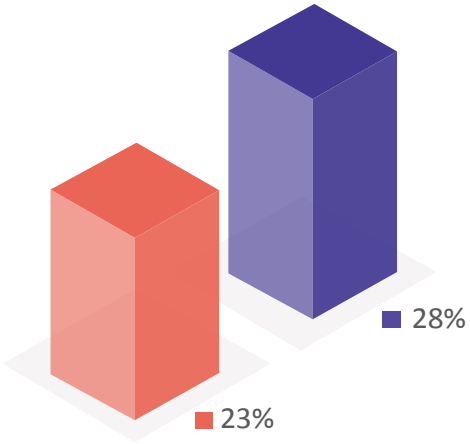
The most obvious targets for disinformation are EMB leadership and spokespersons. But mid- and lower-level staff may also be victimized in attempts to demoralize and paralyze the organization. EMBs must also be aware of other, less-obvious targets. In efforts to turn strategic individuals against the EMB, bad actors may target allies, such as political candidates and government officials who have in the past publicly supported the EMB's work.

A university study reported that falsehoods on Twitter are 70% more likely to be retweeted than true information.

Chapter 2

A Five-step Crisis Communications Guide

According to the 2023 Crisis Communications Survey by software company Capterra, most US businesses admit they are inadequately prepared to communicate during a crisis. More than one quarter (28%) have only informal response plans and 23% have no plans at all. The chances are a survey of EMBs worldwide would yield similar or perhaps even worse numbers.



28% of US businesses have only informal crisis response plans and 23% have no plans at all.

- Capterra survey

But communications professionals know the odds of an organization weathering a crisis without a structured plan in place are very low. Ad-hoc processes and reactionary responses won't adequately protect them. For EMBs, this could lead to questions about the election's integrity and diminish public trust.

By following this guide for building a five-step crisis communication framework, EMBs can mitigate the impact of a disinformation crisis, thereby shielding its reputation and maintaining public trust. This guide is effective in any region of the world and can easily be adapted for organizations large and small.

Step 1 – Audit the Context

Start by gathering all the relevant information to build a strong foundation. The nature of the electoral information environment varies significantly from country to country – it's vulnerabilities, mitigating factors and opportunities. Do this for both information on- and offline, using the following framework as a guide.

Overview

- From what medium(s) do most of your citizens get their election information? Person-to-person? Printed media? Radio? Television? Online?
- Who owns or controls those channels? What are the implications of this ownership? Are the owners related to political candidates?
- In order of influence, list the media about which you need to be most concerned. Are they domestic or foreign?
- How does this vary, if at all, for "opinion influencers" on the national and local scenes?
- Who are creators of false claims that could affect your work or your organization?
- Who are the influencers and largest distributors of information – authentic and false – that affect you directly? (Note: sometimes the biggest distributors are not the creators.)

Identify potential risk

Conduct a SWOT analysis (Strength, Weakness, Opportunity, Threat) to identify vulnerabilities and classify them according to risk level.

- How would a direct false information campaign affect your organization and its ability to execute its mission of delivering trusted, well-run elections?

After identifying risks and potential vulnerabilities, prioritize the issues that pose the biggest threats and assess the potential consequences. Remember: not all risks can be anticipated, so having an adaptable, flexible plan is essential to producing quick, effective responses.

Identify key audiences

To ensure communication channels stay open, maintain and nurture relationships with all election stakeholders before, during and after an election. These relationships must be kept current and should embrace a win-win spirit. Be mindful of the needs and requests of all stakeholders, including:

- **Internal audiences:** Your own staff, related governmental organizations, elected officials, appointees and oversight boards are a few of the internal groups you may need to address. You should do so early and often. Their support will be critical to surviving a crisis.
- **Journalists and editors:** Journalists and editors working in all mediums are important resources when dealing with false information. They are often the first to hear of these inaccuracies and are the leading source of third-party fact checking. Journalists typically play a critical role in shaping reputations – good and bad. Remember, it is important to maintain active relationships even in non-election periods.
- **Political parties and campaigns:** Candidates and political parties are important stakeholders. EMBs should treat them as they would any other high-level stakeholder: neutral but courteous. Unfortunately, politicians and campaigns have been shown in many cases to be the largest disseminators of inaccurate information, so they must be kept at a respectful distance but be monitored closely.
- **Federal, state and local elections communications officials:** It is advantageous to have a comprehensive list of election organizations and associations from areas that border your location. These teams should be seen as partners in disseminating truth.
- **Third-party interest groups:** These are groups that raise awareness and advocate certain positions, such as NGOs, citizen election observer groups and special-interest lobbies. Some of these organizations will support your mission and some won't. It is worth the effort to engage with those who support you and build bridges to communicate civilly with those who don't.
- **Citizens/Voters:** These are the ultimate customer, and a driver for the work EMBs do. Understand and document how stakeholders interact with you, including their channels, frequency, motivations. Communicate with voters via your website, social media and traditional media.
- **Influencers:** This group can include individuals who are in the groups mentioned above but may also include non-stakeholders. These individuals can sway opinion through various channels, including the internet, social media or broadcast media, or as prominent voices in their communities.

Start a team; listen to the conversation

Assemble a rapid response team: An action squad should be assembled to identify false information targeting your organization. Delineate individual's roles and responsibilities to ensure speed and efficiency, and don't forget to designate backups for the most critical positions.

You should also create positions to identify and track false information and its sources, assuming budgets allow for it. If not, assign it as a job task to one or more existing staff.

Make sure communications staff and EMB officers are trained in crisis communications with exercises specifically geared to elections communications. Before an election, promote a crisis-ready culture. This means making sure that critical participants are alert to current events, well-rehearsed and ready to take action.

- Ensure that a member of your organization's leadership team, Communications Director and project leader (or similar officers) are set as decisionmakers for consulting and activating the crisis plan and response.
- Identify spokespeople ahead of time. Consider factors such as prior experience, authority, empathy, communications skills, and relationship with stakeholders. Provide media training for all spokespeople.
- Decide if you need to establish a dedicated war room.
- If your organization doesn't have one, establish a social media manager and a backup. Share their contact information and responsibilities with your key internal stakeholders.
- Ensure that all members of your communications team can access login details, platforms and key messages.

Train phone staff to respond appropriately to hostile callers. Keeping a call log that includes topics discussed in each call can be helpful in identifying specific 'pain points' you should address in your public communication.

Remember to make your staff feel valued and assure them that their work (even if not directly related to the crisis response) is critical to success and to building trust.

Monitor false information: The Center for Internet Security, based in New York, recommends election officials following online mentions of their county or jurisdiction, lead elections officials and other public figures directly involved in their elections. If resources allow for it, jurisdictions should also actively monitor election-related conversations in mainstream and niche social media, following relevant keywords and hashtags.

There are any number of tools available for online monitoring such as Google Alerts, Cision and Meltwater. These tools provide reports detailing conversations and topics in the digital world but they are not specifically focused on disinformation. Hootsuite and Tweetdeck are similar tools for social posts.

Tools specifically designed to separate disinformation and misinformation from facts are widely available today, as are tools to validate the authenticity of online video. Other tools can identify bots from real people. Typically, the best tools come from universities, news reporting organizations and nonprofits. Some of these tools are included in the appendix.

Define success: For most election organizations, success typically means no one is talking about them publicly during and after an election. But in the disinformation age, success may look very different. Your own circumstances will guide your definition.

Step 2 - Develop a Crisis Communications Plan

Dive in. The creation of an action plan, ready-to-use policies, materials and valuable information sources are key to countering false information if a communications crisis arises. Additionally, developing the plan gives your team hands-on experience with topics and resources related to false information, improving their knowledge of this critical area.

Identify communications goals, messages and channels

Explain to your team the purpose of the plan and how to use it: Emphasize that when addressing false information, team members must ensure accuracy and use reliable sources. It's also critical to keep the documentation to prove the vetting, should anyone question the sources. Real-time response is critical for diffusing the impact of false information. Your actions must be quick, informative, accurate and sincere.

Communications process workflow: Draw a clear chain of command in your manual. Outline who will manage the crisis response, who will serve as spokesperson, and who will manage day-to-day crisis communications during an event.

Establish decision-making protocols: Create and share policies that will enable swift choices and quick action while also providing checks and balances to decision-making. You don't want any one person to "hijack" your organization's response. No election organization can (or should) respond to every bit of false information in the public sphere. There aren't enough hours in the day for that.

- Create protocols to facilitate the "go/no go" decision-making process. Recognize that making no response is, in fact, a response option and might be the best response in some cases.
- Establish a baseline (a level below which you will disregard all negative information), an "escalate for review" level and an "immediate action" level.
- Determine the timeframe for communications from the incident response team.

Build from the ground up: There are a few core elements that will inform all other materials you produce as part of your plan.

- Create fact-based key messages and talking points.
- Create a list of terms with a common nomenclature for all stakeholders.
- Develop communications response guidelines (social media included).

Prepare a media toolkit

Include facts and figures, diagrams and infographics, case studies, testimonials, spokespeople's biographies and photos. Share it with journalists and editors prior to elections.

Create templated materials: Have drafts and templates pre-approved, so the team can quickly drop in specific details and finalize when the need arises. Ensure materials adequately address all the potential situations mapped in the audit (first step of this manual).

Statements and press releases: Have prepared statements ready and approved, so the team can quickly add situational specifics. Initial statements should include, at a minimum, the "who, what, when and where," using only reliable sources and confirmed facts. As new information becomes available, confirm it and share it as quickly as possible – in real time if feasible.

- Prepare holding statements for various scenarios.
- Stick to the topic. No crisis ever happens in a vacuum, but you have to keep focused on the main issue at hand. This will also ensure your statement is short.
- For press releases and public statements, be mindful of the tone and timing.
- Ensure review by your legal department.
- Remember, if your statement mentions another organization, you should give them the opportunity to review it prior to publishing.

FAQs: Prepare an FAQ document to address the key issues that are most likely to generate questions. Use FAQs to address issues that may come up but should not be included in initial messaging.

Emergency website plan: Consider developing a crisis microsite – a landing page or microsite prepared in advance of an emergency, but not viewable until it is activated as part of the crisis communications response.

Email blasts: If you have the capabilities already in place, mass emails to your audiences can be very effective. Re-format and reuse the pre-approved language you're using in the press statements and press releases. Remember, don't send one mass email to everyone. Personalize the messages your audience subsets so the content addresses their specific needs. This can include:

- Journalists and media outlets
- Government officials
- Partners, such as vendors and NGOs

Plan offline events: Prepare a press conference contingency plan. Include potential locations, budgets, trustworthy providers, logistics, workflow and agenda.

Messaging and language:

- Displacing deception with explanatory detail has a better chance of correcting the issue than simple debunking. Put the emphasis on information rather than refutation.
- "Pre-bunking" let's you address topics you believe may be targeted by bad actors, so you don't have to debunk it later. This tactic can be particularly effective because it removes fodder from the disinformation cannon before it can be fired.

It's also valuable to infuse your messaging with points from other election-related organizations. In the US this should include organizations such as the Cybersecurity & Infrastructure Security Agency (CISA). This repetition helps drive home key points for voters.

- Promote your office and election staff as the trusted source of information
- Drive voters directly to your website
- Openly communicate plans, procedures and processes
- Encourage stakeholders to be prepared, participate and be patient

Do not amplify and spread false information in your attempts to refute it.

This last point – patience – is critical, particularly for the media and voters. In the age of social media, everyone's expectations for immediate information have gotten shorter. The time between the end of voting and the announcing of preliminary results is fertile ground for misinformation to take root. Level-set public expectations by getting in front of the issue early and often.

- Educate election stakeholders about your secure ballot counting process.
- Provide a realistic timeline for processing ballots and when you'll be issuing periodic updates on unofficial results. Following your local law, make it clear that preliminary results are not final and explain how and when results are made final.
- After voting has concluded, proactively report your processing progress with as much detail as possible.

Address the falsehood directly. When debunking false narratives, describe what's true first, then cite the falsehood - but only if necessary.

Language guidance:

- Reinforce your professionalism and expertise.
- Keep messaging concise, positive and avoid confrontation. Show empathy and concern.
- Make sure your explanation isn't more complicated than the falsehood.
- Address the falsehood directly. When debunking false narratives, CISA recommends describing what's true first, then citing the falsehood (only if necessary). This avoids furthering the falsehoods.
- Say "we" instead of mentioning your organization. When needed to express joint responsibility, say "We are working together with…" or "Working closely with…"
- Be careful not to give information that could change. It's better to say less than to issue statements that vary.
- Provide context. Do not allow your organization to assume the position of "the victim." Rather, explain that disinformation is everyone's problem and why it is.
- Don't blame others even if you have concrete evidence of their involvement in spreading false information.
- Stress that you are taking action (if this is the case), using phrases like "Taking immediate action," or "Taking appropriate measures." Be specific as to what you are doing.

Focus on visions shared across the political spectrum: civic participation, democracy, accountability, having your voice heard, security, integrity.

Step 3 – Before a Crisis Occurs

No one ever said, "Gee, I wish I prepared less and waited longer to do it."
Before the election and before any crisis arises, prepare, train for, and test responses ahead of time.
Consider skillsets, campaigns and ongoing preparedness programs for your organization.

Prepare staff

All team members should be prepared to monitor news, identify red flags, escalate issues and determine next steps.

- Establish a clear chain of command. Staff should know (or be able to easily find) who to notify and how to proceed in a developing situation that could result in a crisis.
- Media train your spokespeople – and practice. A crisis situation is always difficult, even in the best possible circumstances. Rehearse prepared statements and answers to tough questions that reporters may ask to reduce the possibility of errors or embarrassment and sound confident while responding. If possible, similar preparation should be conducted prior to each media interview, briefing or news conference. It is also important to anticipate and address new questions or issues that arise as the story evolves. It is better to over-prepare than to be surprised by the questions.

Prepare and maintain lists of contacts

Your contact lists should include your Incidence Response Team, including communications team, spokespeople and PR consultants.

- Media list (names, titles, etc.) and the internal contact for each journalist.
- Experts and third parties (and their areas of expertise/interest).
- Key executives and their roles.

A contact log should be established to record all inquiries from the media or other external audiences, as well as any direct proactive outreach you have done with individual reporters. This will help to ensure that the many responses required are not overlooked. It will also assist in the post-crisis analysis.

Brief journalists (before, during and after elections)

Be a reliable source of information. Establish relationships before a crisis happens.

- Consider establishing a private on X (formerly known as Twitter) feed for media: Manage media's desire for real-time info. Craft hashtags and social media updates.
- Conduct background briefings to explain the current work you're doing to ensure a secure and efficient mission.
- Explain what and why you do what you do and the scope of your work. Set expectations on the timing of each process.
- Share content (e.g., infographics) that can be published and socialized by media.

Understand & support collaborating journalism and crowd-sourced fact checks

Fact-checking has become the most effective journalistic response to fake news and other forms of misleading information. The 2020 and 2022 US elections proved the value fact-checking organizations bring to the election cycle.

Identify groups of journalists, fact checkers and citizen action groups working on monitoring and verifying news content. Establish an open communication channel with them. There's no reason you can't email fact checkers to introduce yourself and your organization. Tell them you support their work and will count on their support.

If your organization is fact checking, follow best practices provided by the sources included in the appendix herein. Review the resources professional fact checkers use and employ them in your own efforts. Use the following basic steps to get started fact checking:

- Vet the publisher's credibility – Is the outlet known? Does it normally report on election-related topics? Is its URL and domain appropriate for where it publishes from? Who owns the company?
- Vet the author's credibility – Is there an author or is it unattributed? Does the author have prior published articles that you can verify? Do they have a picture in their bio? Does it seem appropriate? (You can do a reverse image search, too. You can find the steps online.)
- Pay attention to quality and timeliness – Are there spelling errors? What's the word usage like (is it natural sounding)? Is everything in caps or are there capitalization errors? Check the date of publication.
- Check the sources and citations – go upstream to the source. Make sure those quoted are real people or organizations. Validate the links in the article.
- Find out who (if anyone) fact-checked the piece or pass it to a fact-checking source.
- Support citizens' collaborative platforms for fact-checking.

If you confirm something is inauthentic:

- Report the false content to fact checkers quickly.
- Tag fact checkers via social media.

Stop it Before it Starts

Google, Facebook and most social media channels employ teams to monitor and mitigate bad information. They are the most effective resource in their respective platforms, but they largely depend on users to flag inaccurate information and alert them to action. These teams should be your first course of action if you're targeted on their platform.

Educate voters, influencers and political stakeholders

Educate your audiences proactively. This allows you to seize the narrative, so you are telling the story on your own terms instead of being reactive after the damage is already done.

Displace, don't dispute. FactCheck.org co-founder Kathleen Hall Jamieson says that simple refutation or debunking of false information isn't as effective as displacing inaccurate materials with correct ones. "It is more effective to have knowledge in place before people are exposed to deception than to debunk after they've been exposed and accepted it," Jamieson said. "Don't negate. Displace."

Step 4 - Taking Action in a Crisis

Your capacity to respond quickly and effectively during a crisis while keeping the spread of false information under control will determine how your organization emerges at the end of the crisis. Avoiding panic and having clear procedures in place will help you find opportunities that manifest within the crisis. Act promptly to protect your organization's integrity.

Let the plan guide you

Activate the Incidence Response Team.

- Prepare your team to take action.
- Implement the crisis management workflow.
- Monitor the media coverage of all election information, not just disinformation. The broader context will help you make informed decisions.

Ensure that your audiences are regularly informed

Give regular updates on the situation to the stakeholders in Step 1. Be as open and cooperative as you can but avoid giving unconfirmed details. If you stay silent, speculation and false information could be perceived as truth.
Inform your entire organization of a developing crisis. Follow the procedures in Steps 2 and 3. Use all available channels and platforms. Be prepared to find false information in a variety of channels.

Be timely and transparent

Take control of your organization's voice across all media before, during and after the crisis. Establish your organization as reliable experts. Promote the truth.

Focus on actions you are taking to address the issue. Establish the facts and double-check them, then distribute them as widely as possible. Avoid mentioning or repeating misinformation in your messages. Focus on providing accurate facts and avoid evolving information and conjecture.

Manage social media: Make your point, give the facts about a situation, rebut any false accusations, suppress speculation, calm nerves and provide useful information throughout all of your social media accounts.

- Facebook: Consider creating a "truth" group in addition to posting facts to your existing page.
- X (the social platform formerly known as Twitter) is an essential platform for breaking news. You should have a profile on Twitter, even if you don't use it often, for the purpose of addressing crises.
- Instagram: Use to share stories. Highlight the people making the election possible, the team and the voters, their culture and their countries.
- Website: Establish a dedicated false information page on your website so users don't have to hunt for answers.
- Be accurate and use pre-approved messaging.
- Stay factual and constructive.
- Coordinate with messages distributed through other channels (website, offline).
- Don't delete negative comments. Respond with key messages. Be courteous and constructive. Know when to stop and take the discussion offline if necessary.

Enlist others to carry your message: You can't possibly reach your whole audience, so use "proxies" to help you get your message out. You can brief 1-2 people in special groups and let them carry the message through their organizations. To ensure consistent, accurate messaging share your prepared materials, such as FAQ and press statements. Some of these groups may include:

- Veterans' groups
- Disability community partners
- Advocacy groups
- Professional organizations (such as the Bar Association)
- Community-based organizations
- Homeowner associations and neighborhood apps like NextDoor
- Community centers and senior centers

Step 5 – Post-election Evaluation

All crises end. How you respond in a crisis will determine how you emerge.

The last step of the communications handbook, evaluation, is essential for successfully closing a false-information crisis. Hopefully, your response was effective enough to avert a crisis. Whether or not a crisis materialized, the evaluation process is as important as the planning and implementation sections. You must determine what went right and what went wrong, and how to fix it before the next situation arises. Make sure to make the process comprehensive and collaborative.

Identify opportunities resulting from the crisis

Remember best practices during crisis communications (online and offline).

- Provide context. You are far more likely to protect a long-term reputation if you put the situation into context.
- Remember: All crises come to an end. How you respond in a crisis will determine how you emerge.
- Use the crisis to learn about opportunities and weaknesses.

Conduct post-election audits and reviews

- Document the lessons learned for future communications planning and crisis readiness.
- Use surveys or interviews and incorporate your stakeholders' feedback.
- Review every aspect of your plan and revise accordingly.
- Review and discuss findings with your team.
- Revise your team, plan and process as needed for next time.

Chapter 3

Final Recommendations

Studies suggest that the growing disinformation phenomenon does not alter news consumption. Thus, establishing and promoting your organization as a trusted source of election information weakens the ability of disinformation promoters to make an impact. It also gives voters confidence in the integrity of the election process.

The following are recommendations from researchers and experts for structuring their own communications protocol:

- Update your Election Crisis Communication Plan at least once a year. This way, you will stay current with your messages, methods, materials and changing circumstances.
- Provide consistent, transparent and secure experiences for all stakeholders.
- Support partnerships between social networks and fact-checkers. These platforms can help in addressing and countering the spread of false information.
- Encourage communication and collaboration with other stakeholders before and during an election. Good coordination facilitates the fight against false information.
- When addressing falsehoods, draw attention to hard news and reliable facts. In the face of well-sourced material and facts, false information tends to fade away.
- Support efforts to improve the assessment of the quality of information sources, through education and training.

This guide is intended to provide management boards with an easy-to-follow, step-by-step guide to address a disinformation communication crisis. Providing fact-checked data and stories at the right time and through the right channel will go a long way in minimizing the negative impact of false information. In doing so, you will increase trust in the election process. However, this handbook is simply a collection of industry best practices and recommendations from experts and should in no way be construed as legal counsel. Your organization should only seek and accept legal guidance from a lawyer licensed to practice in your locale.

---

[1]Pew Research Center, August 31, 2022, Climate Change Remains Top Global Threat Across 19-Country Survey, https://www.pewresearch.org

[2]Vosoughi, et al, "The spread of true and false news online", SCIENCE, 9 Mar 2018, Vol 359, Issue 6380, pp. 1146-1151, https://www.science.org

[3]Ibid.

Glossary

Bots are social media accounts operated entirely by computer programs and are designed to generate posts and/or engage with content on a particular platform. In disinformation campaigns, bots can be used to draw attention to misleading narratives, to hijack platforms' trending lists and to create the illusion of public discussion and support. Researchers and technologists take different approaches to identifying bots, using algorithms or simpler rules based on the number of posts per day.

Botnet is a collection or network of bots that acts in coordination and is typically operated by one person or group. Commercial botnets can include as many as tens of thousands of bots.

Dark ads are advertisements that are only visible to publishers and their target audiences. For example, Facebook allows advertisers to create posts that reach specific users based on their demographic profile, page 'likes' and their listed interests (but these ads are not publicly visible). These types of targeted posts cost money and therefore considered a form of advertising. Because these posts are only seen by a segment of the audience, they are difficult to monitor or track.

Deepfakes are fabricated media produced using artificial intelligence. By synthesizing different elements of existing video or audio files, AI enables relatively easy methods for creating 'new' content, in which individuals appear to speak words and perform actions which are not based on reality. It is likely we will see examples of this type of synthetic media used more frequently in disinformation campaigns, as these techniques become more sophisticated.

Disinformation is false information deliberately created or disseminated with the express purpose to cause harm. Producers of disinformation typically have political, financial, psychological or social motivations.

Fact-checking is the process of determining the truthfulness and accuracy of official, published information such as politicians' statements and news reports. Fact-checking emerged in the U.S. in the 1990s, as a way of authenticating claims made in political ads airing on television. There are now approximately 150 fact-checking organizations in the world, and many now also debunk mis- and disinformation from unofficial sources circulating online.

Fake news is "false stories that appear to be news, spread on the Internet or using other media, usually created to influence political views or as a joke." (Cambridge Dictionary)

Fake followers are anonymous, or imposter social media accounts created to portray false impressions of popularity about another account. Social media users can pay for fake followers as well as fake likes, views and shares to give the appearance of a larger audience.

Influencers are thought leaders in a specific topic area with a strong social follower base.

Malinformation is genuine information shared to cause harm. This includes private or revealing information spread to harm a person or reputation.

Manufactured amplification occurs when the reach or spread of information is boosted through artificial means. This includes human and automated manipulation of search engine results and trending lists, and the promotion of certain links or hashtags on social media. There are online price lists for varying types of amplification, including prices for generating fake votes and signatures in online polls and petitions, and the cost of downranking specific content from search engine results.

Meme Coined by biologist Richard Dawkins in 1976, is an idea or behavior that spreads person to person throughout a culture by propagating rapidly. The term is most frequently used to describe captioned photos or GIFs that spread online. Most are humorous, sarcastic or ironic.

Misinformation is information that is false, but not deliberately intended to mislead or cause harm. For example, individuals who don't know a piece of information is false may spread it on social media to be helpful.

Potemkin village(s) is a false organization - companies, research institutes, or think tanks - created to give credibility to disinformation.

Propaganda is biased or misleading information spread to persuade an audience, but often has a political

connotation. It is worth noting that the lines between advertising, publicity, journalism and propaganda are often unclear or deliberately muddled.

Shill is a promoter or spokesperson who gives the impression of being independent, but actually cooperates with or receives payment from someone else.

Sock puppet is an online account that uses a false identity designed specifically to deceive. Sock puppets are used on social platforms to inflate another account's follower numbers to amplify false information. The term is considered synonymous with the term "bot."

Trolling is the act of deliberately posting offensive or inflammatory content to an online community with the intent of provoking readers or disrupting conversation. Today, the term "troll" is most used to refer to any person harassing or insulting others online.

Troll farm is a group of individuals engaging in trolling or bot-like promotion of narratives in a coordinated fashion.

Whataboutism is a cheap rhetorical tactic of shifting criticism from oneself by drawing a false comparison with an unrelated issue.

Sources "Information Disorder: The Essential Glossary" ; "Journalist's Resource: Information disorder: The essential glossary".

Appendix

The nonprofit Rand Corp. has a good index of tools from a variety of sources specifically designed to help fight disinformation: https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html. Mozilla, the company behind the Firefox browser, is one of the companies behind the Social Media Analysis Toolkit (SMAT), a free, open source, and intuitive way to scrutinize what's trending on internet platforms.

Cybersecurity & Infrastructure Security Agency (CISA) offers toolkits and guidance for battling false information. https://www.cisa.gov/mdm

Fake Domains or Fake Twitter Account tools
Botometer (Indiana University) https://botometer.iuni.iu.edu/#!/
Bot Sentinel https://botsentinel.com/

Image Search & Validation Tools
Yandex https://yandex.com/images/
Google reverse image search instructions
https://support.google.com/websearch/answer/1325808?hl=en&co=GENIE.Platform%3DDesktop
Tin Eye https://tineye.com/
Foto Forensics https://fotoforensics.com/

Fact-checking tools
Claimbuster (University of Texas – Arlington) https://idir.uta.edu/claimbuster/
Emergent (Columbia University) http://www.emergent.info/about

Fact-checking organizations
Factcheck.org (University of Pennsylvania) https://www.factcheck.org/
Fact checking and media bias https://mediabiasfactcheck.com/
Center for Research, Transparency and Accountability (CRTA) (Serbia) https://crta.rs/en/about-us/
Uschi Jonas, journalist at the fact-checking team of CORRECTIV (Germany)
https://correctiv.org/en/investigations-2/
Carlos Hernández-Echevarría, Head of Public Policy and Institutional Development at non-profit fact-checker Maldita.es (Spain) https://maldita.es/

Tijana Cvjetićanin, founder of Istinomjer https://istinomjer.ba/ and Raskrinkavanje
https://credibilitycoalition.org/credcatalog/project/raskrinkavanje/ (Zašto ne) (Bosnia and Herzegovina)

Other resources
Belfer Center's National Counter Information Operations Strategy
https://www.belfercenter.org/sites/default/files/files/publication/CounterIO.pdf

StopFake.org tools to fight disinformation/misinformation
https://www.stopfake.org/en/category/tools/

info@smartmatic.com

SmartmaticTechnology

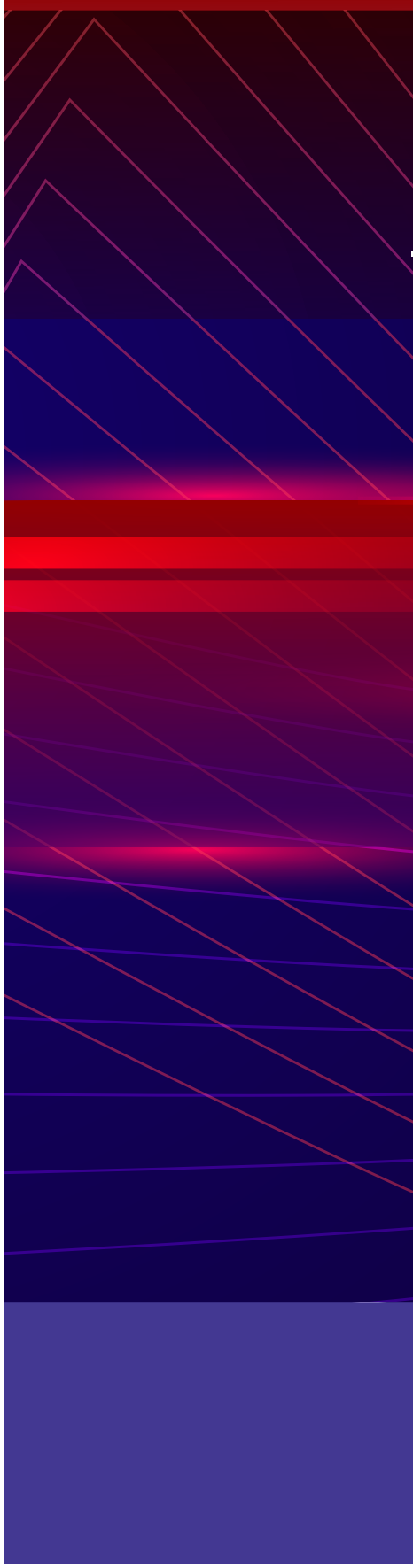
SmartmaticTechnology

Smartmatic_

Smartmatic
SmartmaticEsp

Smartmatic

SmartmaticGroup



www.smartmatic.com