Disinformation Toolkit

Sarah Oh
Disinformation Consultant

Travis L. Adkins
Director, Global Governance and
Civic Engagement, InterAction

June 2018

Overview

Acknowledgements

Cover illustration © westwindgraphics and hurca.com / Fotolia; page icons: Vecteezy.com

Letter from Our CEO

On behalf of InterAction's member organizations, we are pleased to present this resource on online disinformation. This report captures insights from on-the-ground experience responding to disinformation attacks such as those that we have seen abruptly disrupt relief efforts of the White Helmets in Syria, or those that have longer-term, more sustained effects, as we have seen play a role in the evolving humanitarian crisis affecting the Rohingya in Myanmar. This resource provides suggested entry points to investigate specific areas where our members believe leaders of nongovernmental organizations (NGOs) can better assess and prepare their organizations for online disinformation. It provides practical tips for how organization leaders, as well as communications and security experts, can increase their preparedness.

Online disinformation entered the public consciousness in the United States after the 2016 presidential elections, but is now a threat we anticipate will affect our sector's work in the months and years to come. Although this problem has long been an issue for our community, the nature of these trends and behaviors—and the rapid rate at which they can manufacture dissent about assistance internationally, or sow confusion about the communities our members support—is new and worrisome. We need to respond swiftly and strategically as a community of practitioners.
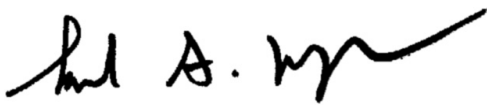
Indeed, understanding how information can be weaponized and ultimately harm our work is critical for the humanitarian and international development sectors. Our members serve the most vulnerable populations in challenging environments, whether due to evolving politics or a crisis. Many of the communities our members support live in information vacuums, where credible and critical information is either unavailable or difficult to access. The spread of false information with the intent to manipulate, or harm, can mean the difference between life or death in these environments. We believe supporting our members to work with each other to identify and push back on harmful behaviors and trends related to online information will decrease our sector's vulnerability to false information and propaganda designed to divide communities or cause violence.

To tackle this new threat, NGOs in the development and humanitarian sectors must adapt. Critical to this adaptation is thinking about the functions of our communications staff and the range of tools our security advisors use. Increasing these capacities will promote conversations that will allow our organizations to better respond to information threats and challenges. It is also essential for our sector to work closely with others studying digital security and digital literacy, including researchers and private sector partners seeking solutions that address some of the trends and behaviors discussed in this report.   ▶

As the largest alliance of U.S.-based nonprofits that work around the world, we believe it is critical to raise awareness about the evolving threat of online disinformation. Whether our members are providing emergency assistance to people fleeing conflicts, promoting democratic governance in places with evolving institutions and civil society, or promoting peace as faith-based or faith-founded organizations, we are all united by our shared mission of making the world a more peaceful and prosperous place. Confronting this new challenge is indeed critical to this mission and worthy of our time and resources.

We hope this report begins a critical dialogue within our community about the scale of the problem we face concerning online disinformation, and, more importantly, what we can do to protect ourselves against it. As a community, we remain committed to leveraging the knowledge, expertise, and private resources from the NGO community to build stronger defenses against bad actors and abuse of online platforms that provide critical information to members and our beneficiary communities. Please view InterAction's website for more resources at www.interaction.org. If you would like further information about these papers, please contact InterAction at 202.667.8227.

Samuel A. Worthington
CEO, InterAction

Terms

▶ **Bot**

Software application that runs automated tasks over the internet

▶ **Counter-messaging**

Message that offers an alternative to false information or false narratives; it can also seek to delegitimize false content

▶ **Denial of service**

An interruption in an authorized user's access to a computer network, typically one caused with malicious intent

▶ **Disinformation**

False or inaccurate information that is shared with the explicit intent to mislead

▶ **Misinformation**

False or inaccurate information

▶ **Rumor**

Story or report that is of doubtful truth

▶ **Search Engine Optimization**

Process of maximizing the number of visitors to a website by ensuring the site is visible at the top of results returned by a search engine

Disinformation Online:
An Evolving Global Threat

There is growing concern that international NGOs and civil society are vulnerable to online attacks and campaigns that spread false information. These attacks are designed to intentionally sow division and confusion, disparage targeted organizations and their leaders, and promote inaccurate views about the communities they support. From Muslim-based foundations in the U.S. to humanitarian assistance organizations assisting refugees in Europe, disinformation campaigns have visibly burdened the operation of NGOs and put beneficiary communities in harm's way.

In politics, candidates and parties have already suffered consequences from large-scale disinformation attacks. There is clear evidence that false pages and ads promoting politically divisive content on Facebook, for example, affected public attitudes around the 2016[1] U.S. elections.[2] Perhaps most troubling on the global stage is the use of disinformation campaigns by states themselves to disparage international organizations working in their countries and to assert claims against these organizations without substantial evidence. In the Philippines, for example, President Rodrigo Duterte's online propaganda machine[3] has criticized international organizations with false claims, asking the organizations to leave if they express dissatisfaction.

> Disinformation campaigns have visibly burdened the operation of NGOs and put beneficiary communities in harm's way.

Disinformation is not a new phenomenon. In fact, governments, organized nonstate actors, and individuals have used campaigns throughout history to deliberately spread false information to influence public opinion or obscure the truth. The strategies deployed by the Kremlin in Eastern Europe and in the Baltic states provide the most vivid examples of targeted disinformation campaigns in recent years. Russia's active efforts to spread rumors through false online news

---

1   Weedon, J., W. Nuland, and A. Stamos. 2017. *Information Operations and Facebook* (version 1.0). Facebook, p. 11. Available at https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

2   The Omidyar Group. 2017. *Is Social Media a Threat to Democracy?* Available at https://www.omidyargroup.com/wp-content/uploads/2017/10/Social-Media-and-Democracy-October-5-2017.pdf.

3   Hofileña, Chay F. "Fake Accounts, Manufactured Reality on Social Media," *Rappler*. October 9, 2016, updated January 28, 2018. Available at https://www.rappler.com/newsbreak/investigative/148347-fake-accounts-manufactured-reality-social-media.

stories and to use abusive trolls to manipulate the emotions of audiences online, are an extension of strategies long used offline.[4]

The proliferation of social media, however, has made this complicated problem more urgent. Today, rumors and lies travel farther and more quickly. Social media has become a primary source of news around the world, playing a more outsized role in shaping public debate about policy issues in the United States and Western Europe. It plays perhaps a more significant role in disseminating political and community information in sub-Saharan Africa, Asia, Latin America, Eastern Europe, and the Middle East, where media markets are less diverse and democratic institutions are at varying stages of consolidation. Disinformation, or false information that is intended to mislead an audience, has the potential to change public opinion, amplify an issue, and change the outcome of political events.

In response to this growing and complex problem, InterAction has created this resource to help international organizations initiate a conversation on how disinformation might impact them. In this report, we try to address the following questions: How does online disinformation affect my work overseas? And what can I do about it? This report draws on desk research and interviews with civil society organizations and international aid organizations providing direct development and humanitarian assistance around the world.

> There are simple steps international advocacy organizations and humanitarian group can take to be better prepared for disinformation attacks.

In 2018, government leaders, private sector companies, foundations, and activists in the United States and Western Europe started using a range of responses including regulatory remedies, technology solutions to filter online content, and public education initiatives to promote information literacy around political events in their countries. Opinions about what can or should be done to address the production and spread of misinformation, disinformation, and false information are varied and surfacing the best solutions remains a work in progress. We do know, however, that there are simple steps international advocacy organizations and humanitarian groups can take to be better prepared for disinformation attacks.

---

4   Paul C. and M. Matthews. 2016. "The Russian 'Firehose of Falsehood' Propaganda Model." Rand Perspective paper. Available at https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

How Does Online Disinformation Affect **International NGOs** and **Civil Society**?

I nterest in so-called "fake news" around the U.S. elections has led to a conflation of terms when discussing false information online and, at times, messy arguments about how disinformation campaigns manifest, spread, and affect society.

Online disinformation can take many forms: promoting accurate information in false contexts, manipulating original content, or completely fabricating and promoting imposter content.[5]

Strategies to disseminate online disinformation cover a wide spectrum. The following methods have been documented by international organizations:

1. Coordinated bot networks (see the White Helmets case study);

2. Use of fake domains in which an adversary creates a similar looking website or social media profile to a targeted website;

3. Hijacking attacks called "double switch attacks" in which adversaries gain control of an organization's or individual's account and spreads misinformation through those accounts; and

4. DNS (denial of service) redirection from specific websites to alternative websites by state-owned telecoms.

---

5   Omidyar, P. 2017. "Point of View: Is Social Media a Threat to Democracy?" Note accompanying the report (supra.). Available at https://www.omidyargroup.com/pov/2017/10/09/social_media_and_democracy/.

It is useful to assess disinformation content based on whom the campaigns intend to target:

1. **Individuals:** visible or politically connected leaders of organizations, national, and international staff.

2. **Organizations**: network organizations, funders, and small grassroots and community-based organizations that partner with large organizations.

3. **Affected populations:** parts of society that receive assistance from international organizations (e.g., refugees, interfaith communities).

Groups interviewed for this report cited several examples of how disinformation attacks can negatively impact their organizations. The most cited consequence has been the influence of these attacks on organizations providing critical information. In 2017, Access Now's Digital Security Helpline documented several cases in which leaders in Bahrain, Myanmar, and Venezuela had problems recovering their accounts after they were taken over by an adversary that disseminated false information through those accounts. Second, the costs of responding to these threats and concerns are high. Fighting off trolls and false claims, for example, have cost members of the Together Project significant human resources and capital. Without question, these attacks put in-country staff, partner organizations, and the community as a whole at risk; and if they remain untamed, many worry the attacks could lead to operations being halted.

Targeting Western-Backed Organizations:
The White Helmets

While the volunteer first responders known as the **White Helmets** have gained international attention for their search-and-rescue operations in the Syrian civil war, they have also become the target of a heavy disinformation campaign intending to sow confusion about the conflict in Syria. Disinformation agents leveraged a network of news sites such as RT and Sputnik News, and published several articles characterizing the White Helmets as a terrorist organization with ties to Al-Qaeda and access to chemical weapons. The claims were amplified on social media, with RT-affiliated reporters sharing the fake news content with their followers, who in turn shared the content throughout their networks. This fueled doubts in people's minds about the motivations of the White Helmets. Russia-backed disinformation campaigns against the White Helmets not only distract attention away from the aftermath of airstrikes, they also work to justify Russia's role in backing President Bashar al-Assad in the conflict against Syrian rebels.[6]

---

6   For more information see: Solon, O. "How Syria's White Helmets Became Victims of an Online Propaganda Machine." *The Guardian*. December 18, 2017. Available at https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

Organizations that need to defend their credibility because of disinformation are burdened with new expenses and workflows to mitigate risk. The amount of time that a team spends identifying disinformation and responding can be taxing.

The **Together Project** is a hub of advocacy and solidarity for U.S.-based NGOs that provide development and humanitarian relief around the world, and confront discrimination or targeted prejudicial regulations in the U.S. due to their operating principles or religious faith. One member of the Together Project reports that it spent more than $100,000 in one year on outside SEO (search engine optimization) consultants to improve search results for their organization and its leaders. Another member organization calls attention to the issues it has with managing its social media accounts.

Conditions for Vulnerability to Disinformation Attacks

Researchers have noted that specific environmental conditions may heighten vulnerability to disinformation and put an international organization at higher risk of a becoming a target for a disinformation attack. Attacks may be more likely to occur in regions affected by active conflict, authoritarian governments, and/or uneven connectivity infrastructure. The following conditions are notable:

1. **Lack of reliable and credible information**. In environments where press freedoms are under threat, journalists are intimidated, or the state controls the media, disinformation can reach wider audiences. When information is created and distributed with malintent in places where information on specific topics is not readily available, it can have harmful effects on vulnerable audiences.

2. **High levels of ambient fear**. In environments experiencing high degrees of uncertainty, including areas affected by conflict, humanitarian emergencies, or natural disasters, audiences may be more susceptible to misinterpreting, or taking actions on disinformation; this, in turn, increases the negative effect and impact it has on an audience.

3. **Asymmetrical information environments**. When there is a lack of access to information, existing information channels are vulnerable to co-optation or manipulation. Asymmetry can be caused by media ownership, political issues around language, and even practical issues such the information dissemination mechanisms that are employed.

4. **Political events or power transitions.** Critical social and political periods and events, such as the period before national elections, present environments that exacerbate the trends described above, and provide fertile opportunities for governments to surveil and limit the flow of information.

5. **Past history of political and other leaders targeting civil society.** Environments where there is some benefit to be gained in undermining the credibility of an international actors like human rights groups may be more vulnerable.

Asymmetrical Information Environments:
Spreading Anti-Muslim Narratives on Facebook in Myanmar

More than half a million **Rohingya**, an ethnic minority group, have fled Myanmar since August 2017 to escape violence at the hands of the government-backed military. The United Nations has described the persecution as a "textbook example of ethnic cleansing."[7] The violence has grown in large part, says the United Nations, due to unsubstantiated rumors and doctored photos that have gone viral on Facebook in Myanmar and that have spread or re-enforced dangerous, false beliefs about the Rohingya. The images, even when debunked, have fueled waves of anti-Rohingya fervor.[8]

The rise in disinformation about the Rohingya took place alongside the adoption of smartphones and an increase in mobile connectivity throughout Myanmar in the past five years. Social media is the main source for news, and due to the nature of the platform, the content spreads quickly without context or fact-checking. This situation demonstrates how disinformation, through social media, incites real-life harassment and violence during a sensitive transition period.

7   Al Hussien, Z. R. "Darker and More Dangerous: High Commissioner Updates the Human Rights Council on Human Rights Issues in 40 Countries." Opening statement to the United Nations Human Rights Council, 36th Session, September 11, 2017. Available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22041.

8   Gowan, A. Bearak. "Fake News on Facebook Fans the Flames of Hate Against the Rohingya in Burma." *The Washington Post*. December 8, 2017. Available at https://www.washingtonpost.com/world/asia_pacific/fake-news-on-facebook-fans-the-flames-of-hate-against-the-rohingya-in-burma/2017/12/07/2c1fe830-ca1f-11e7-b506-8a10ed11ecf5_story.html?noredirect=on&utm_term=.2f004177d326.

Preparing for Online Disinformation Threats

Individual organizations and leaders within the international development and humanitarian assistance community have begun to test new methods for protecting organizations against false claims and exaggerated information online that disparage them or their work. This section provides both questions to help groups determine their organizational vulnerabilities and also practical ideas for protecting against possible risks.

Developing and deploying strategies for anticipating disinformation strategies and techniques used by states and nonstate actors is an evolving area of practice. Organizations will need to support their staff to develop dynamic ways to identify and respond to disinformation and move from ad hoc response systems to more streamlined workflows around handling disinformation. This section provides suggestions for organizations to develop dynamic reporting and response mechanisms for identifying, assessing, and taking action on disinformation threats.

> Organizations will need to support their staff to develop dynamic ways to identify and respond to disinformation and move from ad hoc response systems to more streamlined workflows around handling disinformation.

Identifying your risk

Preparing for disinformation, responding to disinformation, and sharing insights and learnings about attacks will naturally fall on the communication and security leads within your organization. As front-line actors, internal communication and security team experts are best positioned to become better informed about disinformation risks, and to update existing risk assessment and response activities to respond to disinformation threats.

For Communication Leaders:

Discuss your organization's disinformation-related risks to identify weak spots and opportunities for proactively preparing for a possible attack. Conduct a media threat assessment as part of larger risk assessments (see resources at the end of this report) and seek to answer the following questions:

1. Has your organization suffered from a disinformation event before?

2. If so, was the organization able to determine who was behind it, and why?

3. What steps did the organization take before? Are these defensive steps still valid or sufficient?

Train yourself and your team members who are most likely to be on social media on how to identify disinformation.

1. Are you aware of what early warning signals might be? (For example, are you aware of what a bot might look like?)

For Security Leaders:
Disparaging attacks against organizations and leaders, even if false, have in the past posed physical threats to offices and individuals. In this way, online disinformation should be an issue security leads are briefed on, as they develop risk mitigation, emergency crisis response plans and seek to answer the following questions:

1. Who might gain by undermining your organization's credibility?

2. What tools do they have at their disposal (e.g., access to state media)?

3. Would you have the ability to respond (consider messaging, channels to reach key populations, allies, etc.)?

Developing Your Organization's Risk Mitigation Plan

Organizations working on highly visible issues or with at-risk beneficiary communities should discuss what kind of risk mitigation plan is needed. This section summarizes steps you might consider taking to develop a strategy for identifying and responding to online disinformation that could affect your organization's operations and the safety of your staff, as well as your beneficiaries.

We recommend thinking about your disinformation preparation strategy in four parts:

Your Strategy to Tackle Disinformation

> Organizations working on highly visible issues or with at-risk beneficiary communities should discuss what kind of risk mitigation plan is needed.

1. Evaluate your media and information ecosystem.

2. Determine *who* is spreading the false information about your organization, leaders, or programs and develop a hypothesis about *why* they are sharing this information.

3. Determine *what* they are spreading or saying and *how* it is spreading.

4. Take actions to counter this information and work with your organization's leaders to integrate these preferred actions into existing workflows within your organization.

Below are some strategies for taking these actions. These suggestions should be viewed as conversation starters for you and your communications and security staff. The steps that you decide to take or not take should be tailored to the unique context in which your organization operates.

(1) Your Media Ecosystem

Understand online media use and the online media environment in which your programs operate. The first question to ask yourself is: How vulnerable is my media environment to abuse?

Action needed

The organizations interviewed for this report noted that there is a greater need to monitor social media for conversations about their work and their organizations. In fact, several organizations indicated that watching local online media is usually an afterthought. Consult your national staff and learn from them on how information is received by and travels to and within the communities that matter most to your organization.

Possible discussion questions could include:

Questions about your audience:

1. How do people get information about news, politics, and their community?

2. What sources of information are most important for political news?

3. What information sources seem to matter to your core audiences (more than others)?

Questions about your threats:

1. Who are the distributors (i.e., who shares the posts that go viral) that affect your work or your organization?

2. Who are likely creators (i.e., who develops the content that goes viral) of false claims that affect your work or your organization?

3. Do you have any hypotheses on how they disseminate their information and messages?

4. What are their motivations?
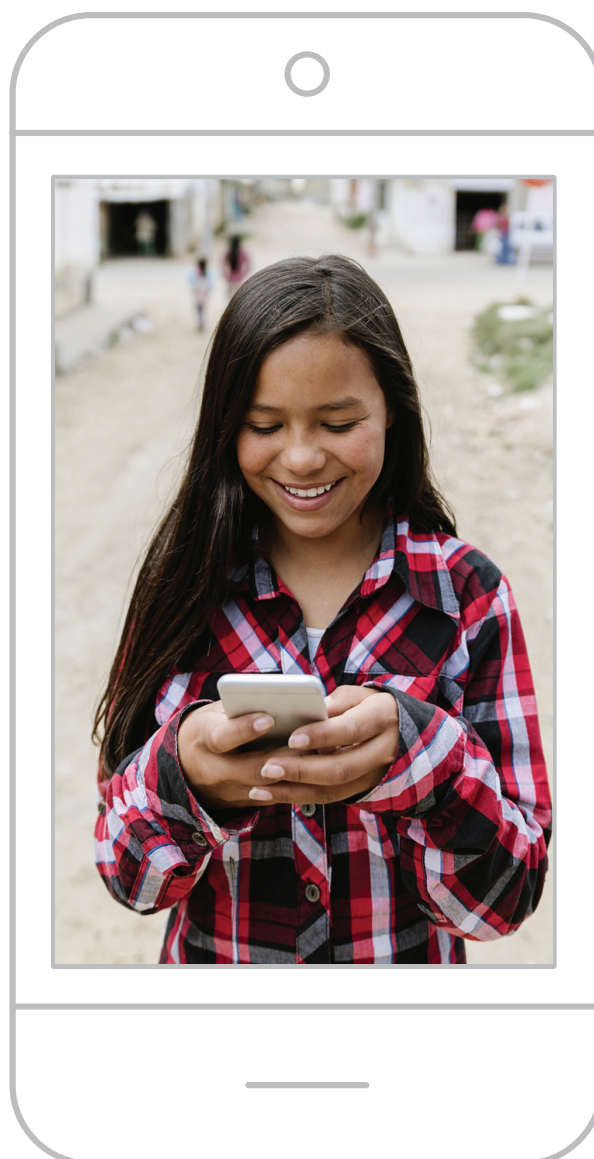
(2) Who Creates Disinformation? And Why?

Disinformation researchers cite two primary actors that create and disseminate disinformation content:

1. **State or state-aligned groups, and political actors with political goals** who create and spread disinformation. The Kremlin's tactics are well documented.[9] In more recent history, in the Philippines, the president's office has built a propaganda machine, in the form of fake accounts and bot networks, that disparages organizations and journalists, and disseminates narratives with specific political goals.[10]

2. **Nonstate actors such as terrorist organizations, extremist groups, political parties, and corporate actors** who have developed and distributed disinformation online. These groups have political aims to recruit supporters, create confusion, or disparage groups who oppose them.

Note: be careful to distinguish groups with politically motivated goals from **individuals and groups motivated by economic incentives who create and disseminate false information.** These are actors who have identified methods to earn a living by creating and disseminating false information; they may support state and nonstate actors in achieving their political goals. In the United States, reports of Macedonian teenagers building false information content farms showed how these cottage industries generate revenue and support industry around the creation and dissemination of false information.[11] **Civil society and advocacy groups** have also promoted disinformation for satirical purposes.

A common goal for these groups is to **sow confusion or discontent** among targeted communities. In Myanmar, for example, Facebook has been repeatedly jammed after major terrorist attacks with doctored photos and false information about the attacks from outside sources.[12]

> Be careful to distinguish groups with politically motivated goals from individuals and groups motivated by economic incentives who create and disseminate false information.

---

9 The Economist. "Turning Politics up to 11: Russian Disinformation Distorts American and Eur." Print edition briefing. February 22, 2018. Available at https://www.economist.com/news/briefing/21737297-mueller-indictment-reveals-some-kremlins-tactics-russian-disinformation-distorts.

10 Ressa, M. A. "Propoganda War: Weaponizing the Inter." *Rappler*. October 3, 2016. Available at https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet.

11 Silverman S. and L. Alexander. "How Teens in the Balkans are Duping Trump Supporters with Fake News." *BuzzFeed*. November 3, 2016. Available at https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.rhwrGxYwe#.ckErgk72y.

12 Head, J. "Myanmar Conflict: Fake Photos Inflame Tension," *BBC*. September 2, 2017. Available at http://www.bbc.com/news/world-asia-41123878.

Disinformation can also take the form of ongoing, more diffusive attacks to **discredit individuals or organizations** conducted through the following ways: paid pro-government commentators; political bots; hijacked accounts (hacking, impersonation, phishing); fake news around elections; and pro-government media and propaganda.

(3) What are They Saying? Where is it Appearing?

Disinformation is disseminated through the Internet through websites, social media platforms, such as Facebook and Twitter, and smart-phone messaging applications such as WhatsApp, Viber, and Instagram, but will vary depending on how actors are seeking to reach their intended audiences.

Commonly cited areas where disinformation has appeared include the following:

- Websites (articles)
- Facebook pages
- Messages through Facebook Messenger, Whatsapp, and Viber
- Posts in Facebook groups
- Comments on highly visible news pages
- Posts on Instagram (posts)
- Tweets on Twitter (tweets)

In preparing this report, we found that international NGOs knew disinformation was a problem, and said that their colleagues were monitoring these trends and behaviors, but admitted collecting data on these trends was challenging.

Organizations may consider developing a system to systematically record and log problematic posts, photos, or text content in a spreadsheet (see appendix for sample) as they occur and share these materials with other groups who are experiencing attacks or observing worrisome trends. By aggregating and collecting this information, research partners may be able to support research that identifies sources and networks leading to the spread of disinformation. *Crowdtangle* is one tool organizations can use to see where specific pieces of online content are shared and to separate amplifiers from sources.

(4) Decide Whether and How to Take Further Action

Have discussions with your communications and security leads to discuss whether actions need to be taken to counter disinformation.

Depending on the circumstances and your organization's goals, the following could be options for response against disinformation events:

Advantages and Disadvantages of Countering Online Disinformation

Action	Advantage	Disadvantage
Let the disinformation *die out and monitor* conversations.	Allows a conversation that may not be visible to your audience to die out more quickly.	Audiences that may have engaged with the disinformation may harbor false views about you and your organization.
Directly counter the disinformation and refute false facts with your organization's existing online media channels.[13]	Allows organizations to correct false statements or claims about them or their work. (If this course is taken, it should be done swiftly.)	Developing and publishing content, and then monitoring response to it takes time and human resources. There is also the possibility that counter-messages can backfire, or reinforce initial false claims or disinformation.
Promote alternative messages that provide information to your audience, through new narratives.	Allows you to change the conversation by presenting new information or alternative messages.	Developing and publishing content, and then monitoring response to it, takes time and human resources.

If your organization has experienced a large-scale disinformation event, you may also consider the following actions:

1. **Archiving** social media content. If this is an area of increased vulnerability for you, consider connecting with open source investigation labs or media organizations that focus on social media information archiving.

2. **Conducting a formal, after-event assessment.** Discuss how you would have handled the event differently, or resources that you wish you would have had. Discuss and assess the experience so that you can be prepared for the next event.

3. **Discuss the event with partners and donors**. Discuss what happened to you and your colleagues with critical stakeholders, including your partners and donors.

---

13 See, e.g., the Internews rumor tracking and debunking programs supporting refugees in the Mediterranean, available at https://www.internews.org/updates/news-moves-mediterranean-rumor-tracker.

4. **Engage platforms**. Disinformation is also an urgent issue for technology platforms to address. If there were any issues related to engagement with the platforms directly in requesting removal of content, tell your organization's policy contact.

Engaging National Staff

International NGOs and civil society interviewed for this report suggested it would be prudent for national staff teams to be involved in threat assessment and response activities related to disinformation. On-the-ground staff may be more likely to identify problematic trends as they occur, and will have valuable perspectives on what an appropriate response might be. Discuss and identify pathways for team members to share patterns and behaviors. Also discuss steps they might take to flag and—if necessary—to respond to disinformation. Additional recommendations follow below.

> On-the-ground staff may be more likely to identify problematic trends as they occur, and will have valuable perspectives on what an appropriate response might be.

- Develop an **internal system for documenting and reporting instances** of disinformation online that may affect an organization's operations. Discussing the issue with staff, and designating a preferred method of communication around the problem, would highlight the importance of sharing events when they occur. It would also allow organizational leaders to get a more accurate picture of threats against the organization.

- An important element of doing this successfully is **developing an open culture where staff members feel comfortable and are encouraged to report disinformation** events as they occur.

Longer Term Strategies: Building Community Resilience

Proactive measures to establish relationships, build trust, and promote information about what organizations are doing, and who they are, helps make a strong defense against false claims. Inversely, groups with weak community relationships and that infrequently share information with their communities will be more susceptible to disinformation attacks. Practitioners know this work is essential, but it is not a priority when working under stress or in crisis environments where immediate relief or protection are needed. Below are suggestions to get started quickly and take steps toward preparing your organization to be ready if and when an unexpected disinformation event occurs.

- **Proactively develop relationships with credible information sources.** Based on the media ecosystem assessment suggested above, build relationships with a network of trusted journalists. Organize one-on-one meetings to brief them on your work, regularly invite them to your events and activities if appropriate, and maintain of drumbeat of information to these journalists.

- **Identify and coordinate with partners who share the same vulnerabilities.** International NGOs contacted in preparing this report have suggested the importance and value of investing time in identifying and working with like-minded organizations to discuss vulnerabilities and attacks when they occur. For example, the Together Project, a coalition supported by InterAction, has developed a space for Muslim-interest foundations in the U.S. to find allies who can carry important messages to different constituencies, including larger interfaith coalitions. These relationships have allowed the alliance to strategically deploy surrogates to promote positive messages at the local level (whether it is commemorating a holiday, supporting disaster response, or sharing content around significant political events) and to members of Congress when advocating for specific issues. Working together as a network and addressing the problem together has been an essential part of sharing insights and brainstorming solutions.

- **Develop a plan for proactively communicating who you are and what you do locally.** Working on sensitive issues means there is often a tension between needing to be discreet and needing to be more vocal to correct inaccurate information or promote accurate details. Encouraging the spread of your messages can help you shape your narratives, and help others reject information that may be inconsistent with their beliefs about your organization. If you do not proactively share what your organization does and what you stand for, then someone else may fill information gaps with inaccurate information.

  International NGOs and civil society organizations feel uncomfortable proactively advocating for their work. Organizations need to do more to promote who they are, and proactively share these messages with their partners and stakeholders more than ever. Discuss with your colleagues your approach to balancing proactive communications about your activities and events, with the potential risk of that information negatively affecting communities you support.

- **Anticipate risk, and share resources before the crisis.** NGOs have noted the benefit of developing systems for translating stock messages to be used in crisis situations. Translators Without Borders, through a proactive communications "words of relief" program, translates critical messages before crises. The organization developed a library of statements on topics such as flood warnings to build up resilience when attacks or disasters occur, so people are more informed. This was deployed with success through the Red Cross and the International Federation of Red Cross and Red Crescent Societies (IFRC) during the 2017 hurricane season in the Caribbean. Messages were translated into Creole and Spanish in late September and October of 2017. Translators Without Borders emphasized the need to provide the right content, that is relevant, and is in a format that is accessible.

  While this toolkit focuses primarily on online disinformation campaigns, some audiences may have other mechanisms that they use to receive and share information (which may not be online, due to lack of technology, connection, and trust in those sources). Effective responses to those campaigns need to appreciate the information landscape in that particular context.

Risk Assessment Tool

Assessing the Vulnerability of Your Media Environment

Specific factors[14] make media more prone to abuse in areas undergoing a major transition or conflict. Assessing the presence of these factors can help you and your colleagues determine how vulnerable media might be to abuse by state and nonstate actors.

How to use this tool: *mark a tally under "likely" "somewhat likely" or "unlikely" under each indicator. Add up the tallies for column at the bottom of the spreadsheet.*

Category	Indicator	Likely or True	Somewhat Likely or True	Unlikely or Not True
Social Media Use and Access				
	Reach is wide. Social media penetration or access is high.			
	Accessibility is wide. Social media adoption and usage is high.			
	People rely on social media as a primary news source.			
	The accounts with the highest number of followers or readership sharing political news are run by a small number of people with similar viewpoints or political views.			
Traditional Media Institutions				
	State capture of traditional media is high and the state wields a strong influence on media organizations.			
	There is extreme hostility from the state towards independent media.			

14 Criteria adapted from Frohardt, M., J Temin. 2010. *Use and Abuse of Media in Vulnerable Societies*. United States Institute of Peace. Available at https://www.usip.org/publications/2003/10/use-and-abuse-media-vulnerable-societies

Journalists and Media Professionals

	There are significant challenges for journalists to carry out their work. They may be harassed or targeted by groups to deter them from doing their work.			
	There is a lack of diversity in ownership of media outlets.			

Government Institutions

	There is a lack of legislation to protect journalists and media outlets from state abuse. Or existing legislation is poorly enforced and has the same effect in terms of poorly protecting journalists and media outlets from abuse.			

Civil Society

	Perspectives of vulnerable voices (e.g., persecuted minorities, opposition groups) are hardly visible and unprotected. They are often subject to harassment and abuse on social media or in traditional media.			
	There is a recent history of attacks against civil society organizations online.			

Dangerous Content

	There is documentation that content is being created and disseminated (offline or online) in an organized way to create fear.			
	Total:			

Review your total in the first column and read the description below that corresponds with your score.

10 to 12   HIGH Vulnerability

Prioritize developing a disinformation response plan with your in-country colleagues. Continue to monitor threats and update your plan as needed.

8 or 9   MEDIUM Vulnerability

Discuss a disinformation response plan with your in-country colleagues as a team. Continue to monitor threats and update your plan as needed.

7 or lower   LOW Vulnerability

Monitor threats and deputize your communication and security leads at your organization to develop a response plan.

Additional **Resources**

How to conduct a information ecosystem assessment

- **Listening Post Collective (Internews)**   https://www.listeningpostcollective.org/playbook
- **Assessing Your Media Ecosystem (Internews)**   https://www.internews.org/sites/default/files/resources/Internews_Mapping_Information_Ecosystems_2015.pdf

How to Detect Fake Domains or Twitter Accounts

- **Fake Domain Detective (Access Now)**   http://fakedomains.accessnow.org/
- **Botometer (Indiana University)**   https://botometer.iuni.iu.edu/#!/

Verification

- **Verification Handbook (European Journalism Centre)**   http://verificationhandbook.com/

Disinformation Response

- **Defusing Hate: A Strategic Guide to Counteract Dangerous Speech (U.S. Holocaust Memorial Museum)**   https://www.ushmm.org/confront-genocide/how-to-prevent-genocide/hate-speech-and-incitement-to-genocide/defusing-hate-a-guide-to-counteract-dangerous-speech