



CENTER FOR  
TECH AND  
CIVIC LIFE

# **COMBATING ELECTION MISINFORMATION**

**July 30, 2020**

# TABLE OF CONTENTS

- INTRODUCTION..... 5**
- INSTRUCTORS..... 6**
- OUTLINE..... 8**
- WHY ARE WE TALKING ABOUT INFLUENCE OPERATIONS?..... 10**
  - A BIGGER SCALE IN 2020 ..... 10
  - A TOP CONCERN OF VOTERS..... 11
  - SOURCES ..... 11
- KEY TERMS AND CONCEPTS ..... 13**
  - INFORMATION OPERATIONS AND INFLUENCE OPERATIONS ..... 13
  - MISINFORMATION..... 13
  - DISINFORMATION..... 14
  - MALINFORMATION ..... 14
  - GETTING CLEAR ON THE DISTINCTIONS BETWEEN MISINFORMATION, DISINFORMATION, AND MALINFORMATION ..... 15
  - FALSE NEWS/FAKE NEWS ..... 16
  - SOURCES ..... 16
- COMMON SOURCES, GOALS, AND THEMES ..... 18**
  - WHO DISTRIBUTES MISLEADING OR FALSE ELECTION INFORMATION? ..... 18
  - GOAL: TO DAMAGE THE APPEAL OF DEMOCRACY..... 19
  - GOAL: TO DISCOURAGE PARTICIPATION OR DISENFRANCHISE ..... 19
  - GOAL: TO BOOST TURNOUT FOR A PREFERRED CANDIDATE OR PARTY ..... 20
  - GOAL: TO DELEGITIMIZE ELECTION RESULTS AND TRANSFER OF POWER ..... 21



SOURCES .....	21
<b>COMMON FORMS OF INFLUENCE OPERATIONS .....</b>	<b>23</b>
A QUICK WORD ABOUT INFLUENCE OPERATIONS, POLITICS, AND EMOTIONS.....	23
WEBSITE SPOOFING OR MANIPULATION .....	24
BREACHES AND LEAKS .....	25
FALSE NEWS STORY .....	26
DECEPTIVE EMAILS, TEXTS, ROBOCALLS.....	28
SOCIAL MEDIA POSTS.....	30
SOURCES .....	35
<b>BREAKOUT EXERCISE .....</b>	<b>38</b>
SCENARIO .....	38
PLAN YOUR RESONSE.....	39
HOW'D THEY DO? .....	40
SOURCES .....	41
<b>GETTING AHEAD OF INFLUENCE OPERATIONS .....</b>	<b>42</b>
BE VOCAL ABOUT THE PROBLEM AND DRIVE PEOPLE TO TRUSTED SOURCES .....	42
SHOW YOUR ELECTION OFFICE AS AN OFFICIAL SOURCE OF INFORMATION.....	43
PUBLISH ACCURATE AND USEFUL INFORMATION REGULARLY .....	45
CREATE A RAPID RESPONSE PROGRAM OR TELEPHONE HELP LINE.....	46
SECURE YOUR COMMUNICATION CHANNELS.....	46
BUILD RELATIONSHIPS WITH SOCIAL MEDIA AND YOUR WEBSITE PUBLISHER .....	47
LEARN HOW TO REPORT FALSE CONTENT ON SOCIAL MEDIA.....	48
ESTABLISH MEDIA MONITORING TO SPOT MENTIONS OR FALSE INFO .....	52
STRENGTHEN RELATIONSHIPS WITH LOCAL MEDIA AND JOURNALISTS .....	52



WORK WITH FACT CHECKING ORGANIZATIONS.....	53
PREPARE YOUR COMMUNICATIONS PLANS AND PROCEDURES.....	53
SOURCES .....	54
<b>RESPONDING TO INFLUENCE OPERATIONS .....</b>	<b>56</b>
INTRODUCING: AN INFLUENCE OPERATIONS RESPONSE FRAMEWORK .....	56
ACKNOWLEDGE: AFFIRM EMOTIONS AND SHARED GOALS .....	57
INFORM: PROVIDE FACTS TO OFFSET THE FALSEHOODS.....	57
EXPLAIN: GIVE AN ALTERNATIVE NARRATIVE.....	58
EMPOWER: HELP PEOPLE LEARN MORE AND RESOLVE CONCERNS .....	59
SOURCES .....	60
<b>GROUP DISCUSSION .....</b>	<b>61</b>
AS QUESTIONS COME UP FOR YOU.....	61
<b>AN ELECTION OFFICIAL’S CHECKLIST FOR COMBATING INFLUENCE OPERATIONS .....</b>	<b>62</b>
GETTING AHEAD OF INFLUENCE OPERATIONS .....	62
RESPONDING TO INFLUENCE OPERATIONS.....	62



# INTRODUCTION

When it comes to elections, misleading information can be a powerfully disruptive force. Facing growing information threats against democracy, election officials can take steps to boost voter confidence and minimize confusion. This course will help you strengthen your role as a reliable source of information and create a defensive strategy to combat misinformation.



## Resources you'll need for this training

- A computer with internet access
- A pen and paper to take notes and doodle



### **Attribution-NonCommercial-ShareAlike**

#### **CC BY-NC-SA**

The training curriculum was developed by the Center for Tech and Civic Life (CTCL), a 501(c)(3) nonprofit organization based in Chicago, IL. The curriculum is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike International License.

This license lets you remix, adapt, and build upon the curriculum non-commercially, as long as you credit CTCL and license your new creations under the identical terms.

Learn more about CTCL professional development courses at [www.techandcivicliflife.org/courses](http://www.techandcivicliflife.org/courses).



## INSTRUCTORS



**Rocío Hernandez** is a Training Associate at the Center for Tech and Civic Life. She helps train election administrators who want to increase their reach and capacity. Before joining CTCL, Rocío worked in education research where she identified opportunities to increase the impact of college readiness programs. Rocío holds a BA in Urban Studies and Sociology from Stanford University.

**Email:** [rocio@technandcivicliflife.org](mailto:rocio@technandcivicliflife.org)

**Twitter:** @rocioehc1



**Emma Llansó** is the Director of CDT's Free Expression Project, which works to promote law and policy that support Internet users' free expression rights in the United States and around the world. Emma joined CDT in 2009. She earned a B.A. in anthropology from the University of Delaware and a J.D. from Yale Law School.

**Email:** [emma@cdt.org](mailto:emma@cdt.org)

**Twitter:** @ellanso





**Kurt Sampsel** is Senior Project Manager at the Center for Tech and Civic Life, where he contributes to the organization's training program and manages tech and implementation projects. Prior to joining CTCL, Kurt earned a Ph.D. as a researcher in media studies and taught college communications courses at Carnegie Mellon University.

**Email:** [kurt@techandcivicliflife.org](mailto:kurt@techandcivicliflife.org)

**Twitter:** [@kurt\\_sampsel](https://twitter.com/kurt_sampsel)



# OUTLINE

- Key terms and concepts
- Common sources, goals, and themes
- Common forms of influence operations
- Breakout exercise
- Getting ahead of influence operations
- Responding to influence operations
- Discussion





## Objectives

After completing this course, you will be able to:

- Understand terms and concepts related to information operations
- Identify different forms of misinformation, malinformation, and disinformation and how to respond
- Develop resilience with a defensive communications strategy



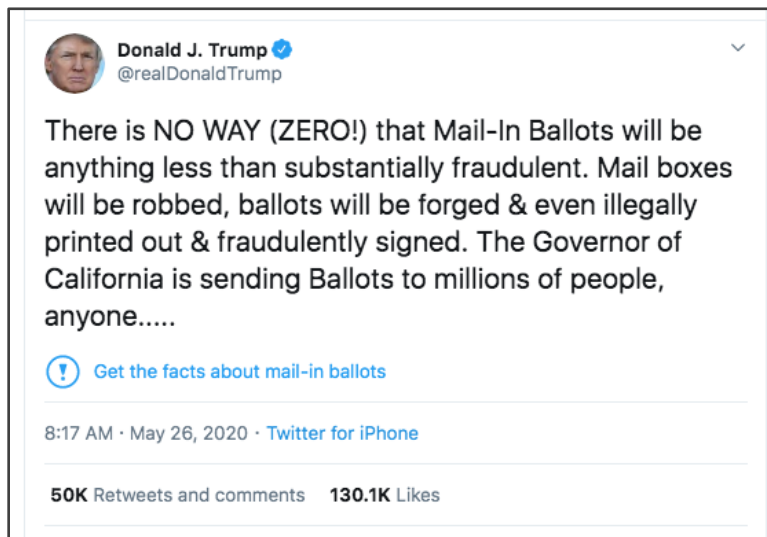
# WHY ARE WE TALKING ABOUT INFLUENCE OPERATIONS?

In the lead up to the 2016 General Election, we saw influence campaigns play a significant role. In particular, we saw a prevalent campaign of social media content launched by Russia’s Internet Research Agency that sought to divide Americans along political lines and especially targeted swing states like Wisconsin and Pennsylvania.

Similar efforts have continued since then. We know that election misinformation is a serious problem already in 2020 and, with the COVID-19 pandemic, there are new opportunities for people to exploit fears, uncertainty, and change in the election this year.

## A BIGGER SCALE IN 2020

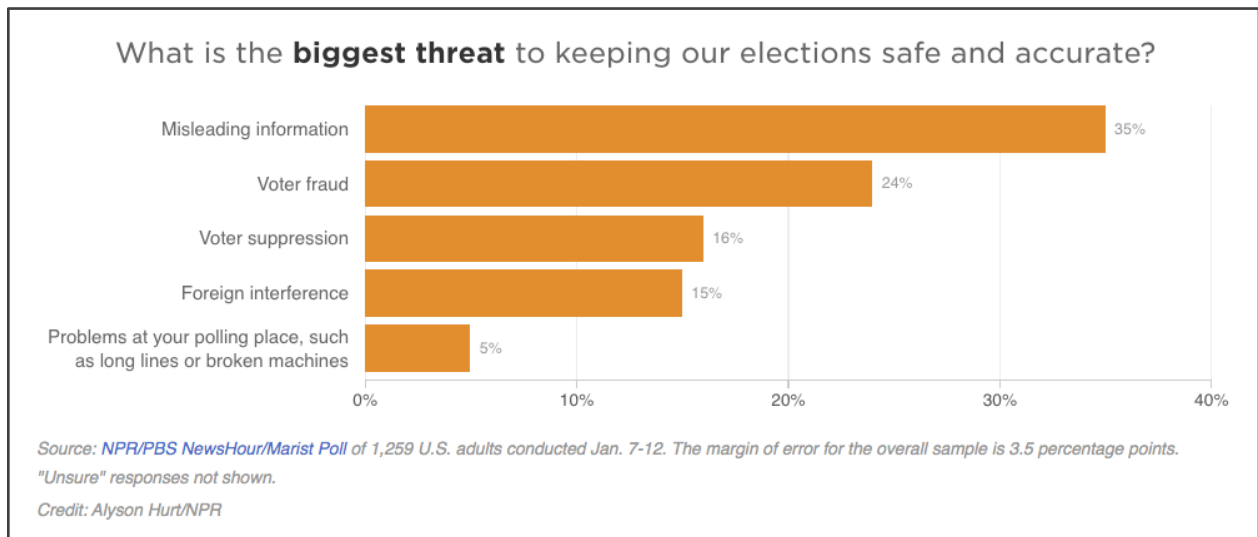
In 2020, sources of election disinformation run the full gamut – from foreign powers to ordinary voters and even the White House. President Trump’s statements on voting by mail, voter fraud, and whether or not he’ll accept the results of the election have had the effect of undermining confidence in our democratic processes on a bigger scale than we’ve ever seen.



In the face of this challenge, election departments will need to address false voting information of various kinds, from various sources.

## A TOP CONCERN OF VOTERS

Ordinary voters are worried about election falsehoods, too. This NPR/PBS NewsHour/Marist Poll asked respondents in January about what they see as the biggest threat to elections in 2020. The largest proportion of respondents -- 35% -- said that misleading information was the biggest threat.



59% of those surveyed said that they believe it's hard to tell the difference between what is factual and what is misleading information, and 55% said they believe it will be HARDER to identify false information in 2020 than it was in 2016.

This course is intended to help election departments serve voters in this difficult climate.

## SOURCES

Donald Trump: "There Is No Way (Zero!) That Mail-in Ballots Will Be Anything Less Than Substantially Fraudulent"

<https://twitter.com/realDonaldTrump/status/1265255835124539392>



Brett Neely: "NPR Poll: Majority of Americans Believe Trump Encourages Election Interference"  
<https://www.npr.org/2020/01/21/797101409/npr-poll-majority-of-americans-believe-trump-encourages-election-interference>



## KEY TERMS AND CONCEPTS

Learning some terminology will be helpful for making sense of how influence operations work and how they can be responded to.

## INFORMATION OPERATIONS AND INFLUENCE OPERATIONS

The term “IO” can refer to both information operations and influence operations. You may also run into the terms “information disorder” or “deceptive campaigns.” In most uses, these are the same basic idea, although we should acknowledge that even experts don’t agree on these terms 100%.

**In general, it’s the distribution of information that has a misleading, disruptive, or antisocial effect on people’s behavior or thinking.**

In information operations, the information can be either true or false, and the effect that it achieves can either be a change in behavior or thinking or just a reinforcement of existing positions.

We should again emphasize that IO is normally thought of as having a disruptive or antisocial effect. This means that normal advertising like a grocery store commercial would not qualify as influence operations, even if, on a basic level, it does use information to affect people’s behavior.

Another important point to make here is that information operations are to be distinguished from cyber operations. Both information operations and cyber operations use technology to disrupt elections, but with cyber operations, it’s the technology that’s the main tool, while with influence operations, the information is the main tool of disruption. Sometimes, however, information operations and cyber operations go hand in hand, especially with things like phishing and data breaches.

## MISINFORMATION

Misinformation is the most general of the three terms we use to discuss different types of influence operations. It’s the term we used in the title of the course because it’s the most familiar, but it does have a more specific meaning we want to highlight.



**Misinformation can be an accident or an honest mistake. It's false information – and by “false” we mean factually inaccurate – but it's distributed without the intent to cause harm.**

So, let's say an excited Michigan voter is trying to get their friends to turn out on Election Day and posts on Facebook a note encouraging their friends to vote and explaining that they can register to vote on Election day at their polling place. Now, that is not the case. Michigan voters do have same-day registration, but they must go to their clerk's office. If our Facebook poster didn't understand that and said it anyway, that's a case of misinformation.

This could also be something like a legitimate news story that contains a factual error.

## **DISINFORMATION**

While misinformation is false information distributed *without* the intent to cause harm, disinformation flips that question of intent. **This is incorrect information deployed with the clear intent to cause harm.**

So, an attempt at voter suppression that distributes the message that one party votes on Tuesday and the other party votes on Wednesday would be a case of disinformation. With disinformation, the message maker is knowingly sharing false information to cause harm.

The information could be something really simple like the example of one party voting on a Wednesday, or could be an elaborate fabrication, such as a deepfake video ostensibly showing a public figure saying something that they're not actually saying.

To sum up, the main difference between mis- and disinformation is the question of motivation. Misinformation can be an accident, but disinformation never is.

## **MALINFORMATION**

Malinformation is probably the least familiar term here. What's distinctive about malinformation is that, unlike mis- and disinformation, **malinformation is factually accurate or truthful. But like disinformation, it is distributed with the intent to cause harm.**



So, how could truthful information be harmful? One way is when private information is disclosed to the public following a data breach or leak. Someone’s stolen email messages could be an example here.

Another example of malinformation is taking accurate information and being intentionally unclear about the context or implications to get a strong reaction. A common example of this is to highlight cases of voter fraud or election irregularities to imply that fraud is a common problem rather than a rare occurrence.

All in all, malinformation can be highly technical and spectacular -- it can be hacking or Wikileaks or cyber warfare – or it can be fairly ordinary, like if a voter discourages participation on Election Day by tweeting out a photo of a long line at a polling place.

## GETTING CLEAR ON THE DISTINCTIONS BETWEEN MISINFORMATION, DISINFORMATION, AND MALINFORMATION

We know these three related terms are a little complicated. This infographic can help you get clear on their distinctions. While both mis- and disinformation are not truthful, they’re different in that misinformation doesn’t come with an intent to cause harm, while disinformation does. Malinformation is also deployed with an intent to cause harm, but unlike mis- and disinformation, the information here is true, accurate, or factual. So it’s true information that has the effect of misleading people.

	Truthful?	Intended to cause harm?
<b>Misinformation</b>	No	No
<b>Disinformation</b>	No	Yes
<b>Malinformation</b>	Yes	Yes

So, why do these differences matter so much? This isn’t just an academic exercise.



The reason is that they affect what kinds of responses are effective to counteract the disruption these different types of information create.

For example, if someone is spreading misinformation in a social media post, it could make sense for the website to take down the post (and the inaccurate information) but not to punish the person further by banning them or suspending their account, because they didn't have a harmful intent.

## FALSE NEWS/FAKE NEWS

Fake news, or false news, is a familiar but troublesome term. Some experts steer clear of this term, but we think it's important to touch on because it can be a common form of influence operations and yet it's often misunderstood.

First, let's be clear about what it isn't. It isn't unflattering or even politically biased news coverage or editorializing. It's also not news content that contains unintentional reporting mistakes or minor factual errors. It's not lazy or imperfect journalism.

Instead, **it's intentionally and verifiably false information that's presented in the form of genuine news content to deceive readers.** You might say it's "masquerading" as real news.

Because of the question of intent and falseness, fake news overlaps the most with the category of disinformation rather than misinformation or malinformation.

## SOURCES

Belfer Center: "The State and Local Election Cybersecurity Playbook"

<https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>

Brookings Institution: "How to Combat Fake News and Disinformation"

<https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/>

Carnegie Endowment: "The Challenges of Countering Influence Operations"

<https://carnegieendowment.org/2020/06/10/challenges-of-counteracting-influence-operations-pub-82031>





Center for Information Technology and Society: "What Is Fake News"

<https://www.cits.ucsb.edu/fake-news/what-is-fake-news>

John Cook and Stephan Lewandowsky: "The Debunking Handbook"

[https://skepticalscience.com/docs/Debunking\\_Handbook.pdf](https://skepticalscience.com/docs/Debunking_Handbook.pdf)

Council of Europe: "Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making"

<https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>

First Draft: "Definitions" lesson from Protection from Deception course

<https://firstdraftnews.org/latest/course-training-us-election-misinformation/>

First Draft: "Information Disorder, Part 3: Useful Graphics"

<https://medium.com/1st-draft/information-disorder-part-3-useful-graphics-2446c7dbb485>



## COMMON SOURCES, GOALS, AND THEMES

To understand influence operations, it makes sense to talk about who does it, what the goals are, and what some of the common themes are. This matters because even though there are always new examples of things like disinformation being created, they tend to keep doing the same basic things over and over again. If you can get familiar with the recurring goals and themes, you'll be able to recognize and understand new examples as they emerge.

## WHO DISTRIBUTES MISLEADING OR FALSE ELECTION INFORMATION?

Who participates in influence operations? Here's how we can categorize most of the actors:

- Nation-state actors (Russia, Iran, China, etc.)
- Domestic actors driven by partisanship
- Ordinary voters (often unintentionally)

**Nation-state actors like Russia, Iran, China, and North Korea** are often associated with information operations. For instance, Russia pursued a wide-ranging campaign of influence operations against American voters in 2016 that included things like inciting rallies by extremist groups and amplifying divisive ideas and hate speech.

These non-American actors are important, but you can't overlook domestic actors, too. Many of the influence operations you'll find on social media channels are created by **domestic actors motivated by partisanship**. Sometimes they're prominent – like a member of a state's political party – but often they're just regular people who happen to run a politics-oriented Facebook group and care more about riling people up than checking their facts.

And, of course, **ordinary voters** are guilty of circulating unverified rumors or myths about voting, even if they aren't trying to have a disruptive effect.

Next, we'll survey a few common goals of influence operations in the elections field and the kinds of themes you're likely to come across related to each goal.



First, let's be clear that these goals are specific to information operations in elections and not information operations overall. That's important because a common motivation for influence operations can be financial gain, but that's not a common goal when it comes to election misinformation.

Normally, influence actors want some sort of political or electoral outcome – even if it's a really general one like this first one.

## **GOAL: TO DAMAGE THE APPEAL OF DEMOCRACY**

*Common themes associated with this goal: Democracy is a sham. Democracy is no better than an authoritarian or autocratic system. All politicians are corrupt. The political parties are the same.*

This goal is mostly the domain of nation-state actors like Russia who seek to reduce scrutiny and criticism of their own political systems by damaging the appeal of western democracy. If American democracy seems messy, corrupt, and disorganized, people are more likely to accept messiness, corruption, and disorganization from their own leaders. Because this goal is outward looking, you won't really see it used by domestic actors, unlike the next goals.

## **GOAL: TO DISCOURAGE PARTICIPATION OR DISENFRANCHISE**

*Common themes associated with this goal: Don't come out. Your mail ballot won't be counted. Democrats vote on Tuesday and Republicans vote on Wednesday. Tomorrow's election has been rescheduled. You can now vote online. You must show your birth certificate to vote. We'll have people at the polls making sure nobody votes who isn't eligible.*

If this list of common themes in red seems longer than the rest, that's because it is. Discouraging participation is, unfortunately, a quite common goal of influence operations. It's a regular theme of domestic political actors who are working in bad faith as well as state-nation actors.

To take just one example, the Brennan Center for Justice has shown that in 2016 Russia's Internet Research Agency ran paid Facebook ads intended to discourage turnout for nonwhite voters, especially Black voters.



But domestic actors do it too. False information about voting online or needing to show a birth certificate or the election date is commonly deployed with the intent of reducing turnout of opponents who are seen as not persuadable.

## **GOAL: TO BOOST TURNOUT FOR A PREFERRED CANDIDATE OR PARTY**

*Common themes associated with this goal: Party X is trying to commit fraud, so it's extra important for Party Y supporters to vote. Party Y is participating in voter suppression, so Party X supporters must turn out.*

Of course, just as it makes sense to suppress participation by opponents, it makes sense to influence operators to boost participation for the candidates or parties that they prefer.

On top of the obvious approach of saying false *good* things about someone's preferred candidate and false *bad* things about opponents, some of the most common themes that contribute to this goal focus on accusing opponents of voter suppression or fraud.

That's interesting, right? So just as influence operations can suppress the vote AS a goal, they can also reference the risk of voter suppression by opponents to boost voter turnout for their side.

Something that's important to take away from all this is that although election officials should understand these IO tactics and themes, you should avoid focusing too much on these messy accusations because the accusations themselves actually might not be the point.

We should be clear that, unlike the previous two goals, there's nothing intrinsically wrong or anti-democratic about the goal of boosting turnout or support. In this case, it's the *means of doing it* that's the problem.



## GOAL: TO DELEGITIMIZE ELECTION RESULTS AND TRANSFER OF POWER

*Common themes associated with this goal: Voter fraud is rampant. Election officials and poll workers don't know what they're doing. Equipment is switching votes. My friend got the wrong party's ballot in the mail.*

Finally and perhaps most destructively, we have the goal of delegitimizing the election itself, the results, and the transfer of power of our leaders. This often takes the form of the unproven anecdote – “I heard rumors about fraud,” “I had a bad experience at the polls,” “a friend on Facebook witnessed such-and-such problem, and therefore, we can't trust the results of the election.”

There's a famous example from 2016 about a Pennsylvania voter whose voting machine allegedly wouldn't allow him to select his preferred candidate. The initial tweet was retweeted by a Kremlin-backed account masquerading as the Tennessee Republican party, and ultimately the story was picked up by dozens of media outlets. The truth was that the machine was working properly, and the voter just wasn't following the directions.

As you can imagine, cases like this can be hugely disruptive.

## SOURCES

Ad Hoc Committee for 2020 Election Fairness and Legitimacy: “Fair Elections during a Crisis”  
<https://www.law.uci.edu/faculty/full-time/hasen/2020ElectionReport.pdf>

Belfer Center: “National Counter-information Operations Strategy”

<https://www.belfercenter.org/publication/national-counter-information-operations-strategy>

Demos: “The Attack on Vote-by-Mail: Weaponizing ‘Voter Fraud’ Claims to Suppress the Vote”

<https://www.demos.org/policy-briefs/attack-vote-mail-weaponizing-voter-fraud-claims-suppress-vote>

Electronic Privacy Information Center: “E-deceptive Campaign Practices Report 2010: Internet Technology and Democracy 2.0”



[https://epic.org/privacy/voting/E\\_Deceptive\\_Report\\_10\\_2010.pdf](https://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf)

Graphika: "Secondary Infektion"

<https://secondaryinfektion.org/download>

First Draft: "Motivations" lesson from Protection from Deception course

<https://firstdraftnews.org/latest/course-training-us-election-misinformation/>

Center for Strategic and International Studies: "Countering Adversary Threats to Democratic Institutions"

[https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180214\\_Spaulding\\_CounteringAdversaryThreats\\_Web2.pdf?EzqGtMwOajQIIH8eRNN0Z10T49OV63lh](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180214_Spaulding_CounteringAdversaryThreats_Web2.pdf?EzqGtMwOajQIIH8eRNN0Z10T49OV63lh)

Shawn Musgrave: "The Secret Twitter Rooms of Trump Nation"

<https://www.politico.eu/article/twitter-donald-trump-the-secret-twitter-rooms-of-trump-nation/>

Brandy Zadrozny and Ben Collins: "How a Right-wing Troll and a Russian Twitter Account Created 2016's Biggest Voter Fraud Story"

<https://www.nbcnews.com/tech/tech-news/how-right-wing-troll-russian-twitter-account-created-2016-s-n925711>



# COMMON FORMS OF INFLUENCE OPERATIONS

This next section covers some real-world examples of misleading election information. As you might imagine, there are many different forms that influence operations can take. But to make things manageable, we'll look at just five of the most common ones.

## A QUICK WORD ABOUT INFLUENCE OPERATIONS, POLITICS, AND EMOTIONS

Election administration and political polarization are often linked when it comes to influence operations.

We know that, as election officials, you are probably not used to thinking about your work in political terms. And to be clear, as nonpartisan organizations, we aren't used to talking about politics in our work, either. But influence operations targeting election administration routinely use political appeals, and here's why that is.

As is the case in all persuasion, **emotion is an effective tool for provoking a response and bypassing people's reasoning and critical thinking.** If you're angry or fearful, you're more likely to react without thinking.

And the fact is, because of the way that political loyalties work in the United States, **political matters are just more likely to provoke an emotional response than election administration issues are.** If someone says your candidate is a crook, that's going to upset you more than if someone says your absentee ballot request is due on the wrong date.

So **that's why so much election misinformation exploits political loyalties conflicts instead of just referencing details of how elections are run.** People combine election administration with politics because it makes it more effective that way.

We hope you'll keep this in mind as we look at the case studies that follow, some of which use explicit political messages and some of which don't.

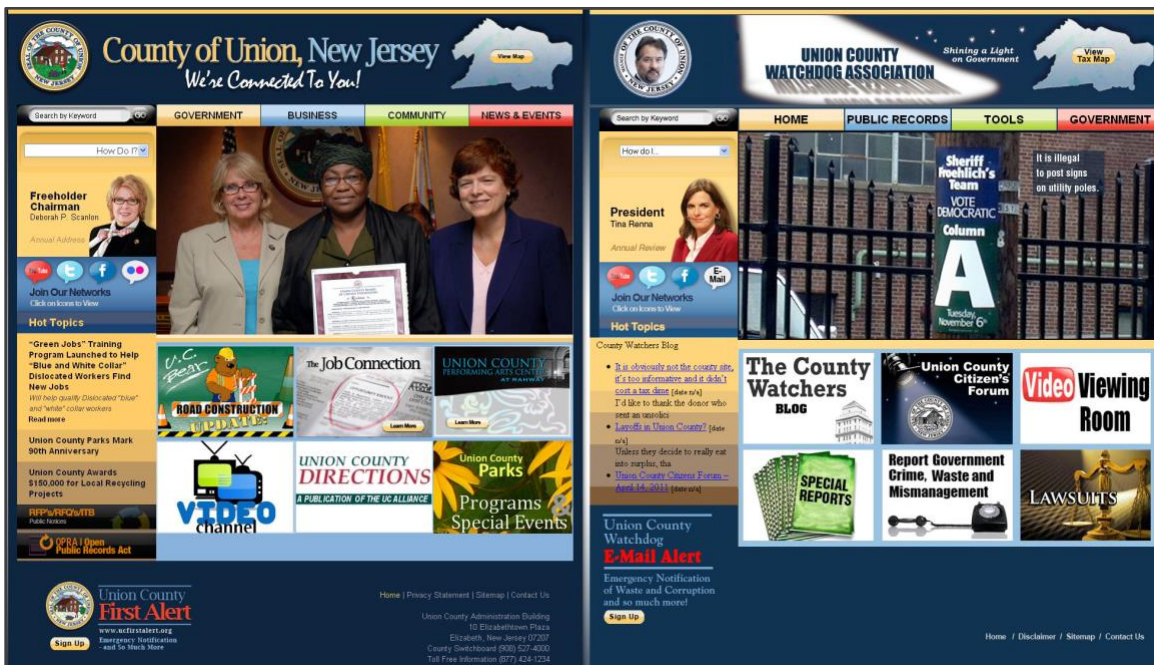


# WEBSITE SPOOFING OR MANIPULATION

**Website spoofing** is when an imitation website is created to fool visitors into believing they're on the official site. There's also manipulation, which simply means an unauthorized user edits an official website.

Although this is something that election security experts have been warning about for some time, we have not yet seen reports of spoof election websites in the wild. What you see below is a spoof website created by a government watchdog organization in Union County, New Jersey.

The real county website is at left and the spoof at right.



Even though this isn't a genuine spoof, creating a website is easy for anyone with web publishing skills, so the risk of spoof or imitator websites is a very real one.

When it comes to something like election results, in particular, election security experts have pointed out that manipulating data on an official website could be almost as disruptive as manipulating the vote tallies themselves. Even if published vote tallies are changed and then fixed back by the election office, people still might distrust the validity of the correct results.





It's not easy for ordinary people or even experts to spot spoof websites. You might think that the little lock icon beside the URL in your browser indicates that the site is legitimate, but that just indicates that you have a secure *connection* to the site. You can have a secure connection to a spoof site. So, in other words, that lock icon is very different than the blue checkmark on social media. It does *not* suggest that the site is verified.

## BREACHES AND LEAKS

Breaches and leaks deal with factual information, so they're both cases of malinformation.

A **breach** occurs when a malicious actor *outside* an organization gains access to private information and then makes it public. A **leak** is similarly making public information that should be private, but with a leak, it's someone *inside* the organization that releases it.

We most often hear about leaks and breaches when it comes to military intelligence or politicians' emails. We haven't seen a lot of it with elections, but a 2018 case from North Carolina will give you a sense of what can happen and what consequences could come. During early voting for the 2018 General Election in Bladen County, a poll worker blew the whistle on fellow elections workers who tallied vote totals before Election Day – which is a violation of state rules – and then leaked those initial vote tallies to people involved in the campaign of one of the candidates on the ballot.



Now, in this case, the leaked information was allegedly given to a political campaign rather than the public at large, but you can imagine how vote tallies that were made public could influence voter participation. In the Bladen County case, the alleged leak certainly proved to damage voter confidence.

The Bladen County Board of Elections launched an investigation but, as far as we can tell, was unable to conclusively prove the leak occurred. But because of this case and irregularities with ballots in another county, the state board ultimately ordered an entirely new election for the contested House race.

## FALSE NEWS STORY

Even though false news, or fake news, stories aren't an especially common form of information operations related to elections, there have been some prominent examples, including this notorious story from the 2016 election that claimed a maintenance worker had found tens of thousands of pre-filled ballots in a warehouse several weeks before Election Day.



The story was quickly debunked when people found that the image that was used has been taken in England the year earlier. But the story was still shared widely and gained the attention of a New York Times journalist who profiled the creator, a recent college graduate named



Cameron Harris who claimed he created the story and several other fake news articles as a way to earn money. According to the New York Times, this story went viral enough to earn its creator about \$5,000 in ad revenue.

This story is especially relevant for this course because it specifically names Franklin County, Ohio as where this supposedly happened. This prompted officials there to respond.

After the Christian Times fake news story got widespread public attention, Ohio election officials responded.

John Husted, then the Republican Secretary of State for Ohio, publicly denounced the story in the media, and the Franklin County Board of Elections also [issued a public statement about it](#).

Below is a screenshot of part of that press release.

Claims falsely challenging the integrity of the elections administration are taken seriously as public confidence in the electoral process is important. The Franklin County Board of Elections has numerous ballot and election security measures in place.

- The computer system used to create the ballot and tabulate results is not connected to an outside network and thus is not vulnerable to outside intrusion.
- Each ballot storage vault is maintained under a double lock requiring a Democrat and Republican to simultaneously unlock.
- A double lock system is used to secure the Vote Center and must be unlocked by a Democrat and Republican simultaneously.
- Both parties are required to sign a chain of custody for all mailed ballots delivered to or picked up from the USPS.
- Access to sensitive ballot storage areas are secured by keys that are maintained in storage containers requiring palm scan access.
- Votes are recorded in three ways (1) in a hard drive within the voting machine, (2) on the removable voting machine data card, and (3) on a paper tape inside the voting machine.
- When the vote is counted, it's done in a public setting which can be observed by parties, any campaign, the media, and the public.

You can see that they took a really smart approach here, which was to not just debunk the claims in the story but also share information about their ballot and election security measures in place.



## DECEPTIVE EMAILS, TEXTS, ROBOCALLS

Next up are deceptive emails, texts, and robocalls. (In other countries, WhatsApp and other messaging apps are also common sources of false information, and this may become more common in the U.S. soon.)

### George Mason University case study

For a first example, let's go back in time a little bit to look at a deceptive email from the 2008 General Election. At George Mason University in Fairfax, Virginia, a malicious actor gained access to the university provost's email account and sent this message to the entire university community, including students, faculty, and staff. About thirty-five thousand people received this message, which was made to look like it was from the university's provost, and claimed, at 1:00 a.m. on Election Day morning, that Election Day was being moved.

```
List-Owner <mailto:ANNOUNCE04-L-request@LISTSERV.GMU.EDU>
List-Subscribe
<mailto:ANNOUNCE04-L-subscribe-request@LISTSERV.GMU.EDU>
List-Unsubscribe
<mailto:ANNOUNCE04-L-unsubscribe-request@LISTSERV.GMU.EDU>
List-Help
<mailto:LISTSERV@LISTSERV.GMU.EDU?body=INFO+ANNOUNCE04-L>

To the Mason Community:

Please note that election day has been moved to November 5th. We
apologize for any inconvenience this may cause you.

Peter N. Stearns
Provost
```

The email was sent through servers run by a Washington, D.C.-based company that works on Democratic political campaigns but originated from a computer in Germany. The company's chief technology officer distanced himself from the email and said its attempt at voter suppression were opposite the company's stated goals.

Later that day, the real university provost issued a statement about the deceptive email message and encouraged the university community to participate in the election. We haven't been able to verify if the local election office took an action or not.

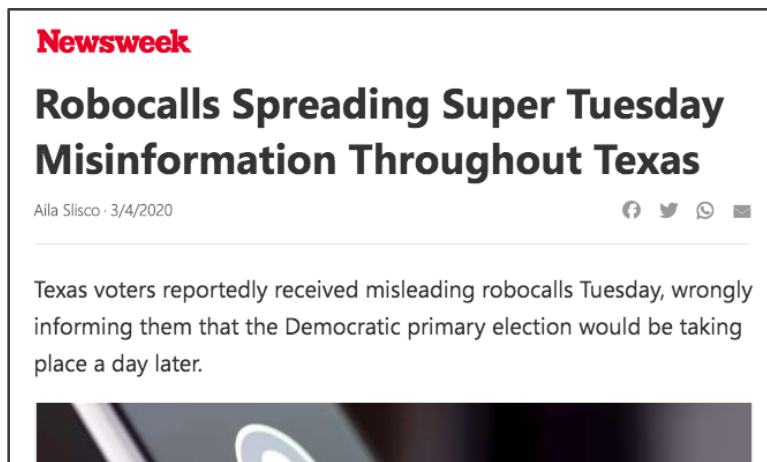


Writing about this email in a report on deceptive practices, the Electronic Privacy Information Center said that the George Mason case demonstrated “that deceptive practices that target e-mail, instant messaging, and cell phone users can compress the timeline for launching successful disinformation and misinformation attacks from days to hours or minutes.”

That’s certainly true with these instant communication methods. Let’s look at a more recent example.

## Texas robocall case study

During the March 2020 primary in Texas, there were widespread – and varied – reports about robocalls that contained misleading information. Like with the George Mason email, it was the date of the election that was the focus of the misinformation. Most reports say that the recorded message in the calls encouraged voters to vote, quote, “tomorrow” for the Democratic primary even though they were received on Election Day. There were reports of Spanish-language calls, as well.



In this Texas robocall case, the Secretary of State’s office corrected the record in a Tweet.





That seems like a good response, but of course it's incredibly challenging to respond to an influence operation event *on* Election Day, and it's impossible to know how many people may have received the robocall but did not see the subsequent correction.

The best guidance we can offer here is to review your department's policies and procedures for issuing press releases and conducting interviews with the press so that you're as prepared as possible on Election Day and don't need to scramble to find your state communications officer's phone number when something like this happens.

These last-minute messages about Election Day being moved or cancelled may be especially troublesome this year because of COVID-19. We've seen in at least two states that rescheduling the election due to the pandemic was being decided by courts within 24 hours.

## SOCIAL MEDIA POSTS

Social media is probably the most common place you'll find election misinformation because, of course, there are no message gatekeepers, it doesn't cost anything to post, and the social media platforms have been reluctant to deal with misleading content (with a few famous exceptions).

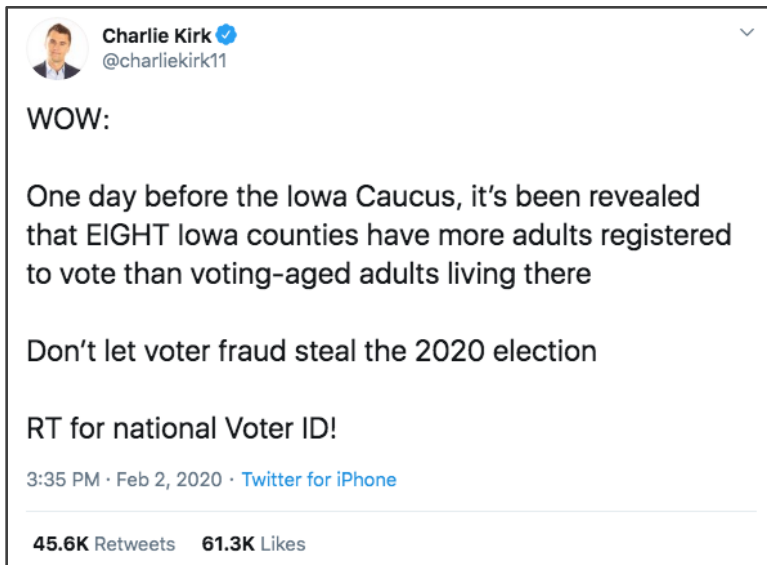
## Judicial Watch/Iowa case study

Here's a case of influence operations from February of this year. On the day before the Iowa caucus, Tom Fitton, the head of the conservative watchdog organization Judicial Watch, posted this tweet claiming that eight Iowa counties' voter registration rolls exceeded the number of total eligible voters.





That same day, Charlie Kirk, another famous conservative figure, tweeted about the supposedly problematic voter rolls. Kirk's tweet boosted the message to a much larger audience.



The next day, Paul Pate, the Republican Secretary of State for Iowa, responded to Fitton and Kirk. He disputed the tweets and provided correct registration data.





So, is Fitton’s original information about bloated voter rolls disinformation or misinformation? The information was proven to be factually inaccurate, and while we can’t know Fitton’s or Kirk’s intentions 100%, the fact that the announcement came one day before the Iowa caucus and used words like “big” and “wow” in all-caps suggests a deliberate intent to affect the caucus.

So, this qualifies as disinformation.

Before we move on, it’s important to take note of the numbers here. Fitton’s original tweet got sixty-five hundred retweets and eighty-seven hundred likes, Kirk’s got forty-five thousand retweets and sixty-one thousand likes, while Pate’s correction message received just ninety retweets and four hundred forty-four likes.

This is an important – if discouraging – lesson showing that even when you’re able to correct false information, your correction may not be heard as loudly as the original disinformation.

## Cook County polling place case study

Of course, not all information operations on social media come from public figures or activists, and not all misleading posts make such a big splash. Here’s a more low-key example of information operations on social media during the 2020 primary elections.

In this case, a Facebook poster grabbed this image from Twitter of a sign at a Cook County, Illinois polling place indicating that poll workers didn’t show up.







This is a real photo, and the sign in the window is real. But you can see that the Facebook poster uses the photo to make the argument that “Today’s primary results are not legitimate.” That’s a really unfortunate message.

I think we can agree with the poster that well-run polling places are vitally important and that a polling place not opening is a problem that must be addressed. But to highlight a problem at a single polling place and conclude that it invalidates the results is misleading and damages trust. Because it’s a real photo, this qualifies as malinformation. The big reason is that context and additional information are missing.

Context might sound like a minor or academic detail, but it can be a major contributor to misleading content online.

When you take a photo of a polling place that didn’t open, don’t explain the context or the significance, and claim that election results are not valid, you’re removing important context, and that’s what makes this malinformation.



For context, take a look at the original Twitter post that served as the source of the image for the Facebook re-posting. This post was published at 8:20 a.m., and you can see that it got lots of attention.



Brian included the Cook County Clerk's Twitter handle in the tweet, and the Clerk's account responded just seven minutes later to ask for details on the exact location of the polling place.



After a quick exchange of information, the polling place began processing voters. James Scalzitti, who's the Director of communications at the Cook County Clerk, told Time magazine that the Clerk's office sent additional staff to the site and had it running by 9 a.m., about 40 minutes after Brian's original post. He added that the site would stay open an extra hour in the evening to accommodate voters who were unable to vote in the morning.



Again, I think we can agree that election departments must serve voters with well-run polling places that open and close at the times specified by law. But on balance, it seems like the Clerk's office made a good-faith effort to correct this problem promptly.

While it's true that there were other problems with voting in Cook County during this primary, the Facebook poster's message about election results not being legitimate is misleading and unfortunate. Seeing this may have discouraged would-be voters from participating and may have damaged trust.

It's a shame that more people didn't see the Clerk's office working to address the problem instead.

## SOURCES

ABC 6 WSYX/WTTE: "Board of Elections Pushes Back After Article Claiming Filled-out Ohio Ballots Found"

<https://abc6onyourside.com/news/local/board-of-elections-pushes-back-after-internet-article-claiming-ballots-were-found>

Madeleine Carlisle: "Poll Workers Didn't Show Up at Some Primary Election Precincts on Tuesday Because of COVID-19 Concerns, Limiting People's Ability to Vote"

<https://time.com/5805133/florida-illinois-arizona-primary-cornavirus-workers/>

Electronic Privacy Information Center: "E-deceptive Campaign Practices Report 2010: Internet Technology and Democracy 2.0"

[https://epic.org/privacy/voting/E\\_Deceptive\\_Report\\_10\\_2010.pdf](https://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf)

Merritt Enright, Ben Collins, and Matthew Mulligan: "Robocalls in Texas Push Wrong Day for Democratic Primary"

<https://www.nbcnews.com/politics/2020-election/live-blog/2020-super-tuesday-live-updates-14-states-hold-primaries-n1146871/ncrd1148626#liveBlogHeader>

Franklin County Board of Elections: "Press Release: Oct. 1, 2016"

[https://static.ow.ly/docs/Media%20release%202010-1-15\\_5l8K.pdf](https://static.ow.ly/docs/Media%20release%202010-1-15_5l8K.pdf)



Amy Gardner: "N.C. Board Declares a New Election in Contested House Race after the GOP Candidate Admitted He Was Mistaken in His Testimony"

[https://www.washingtonpost.com/politics/candidate-says-new-congressional-election-warranted-in-north-carolina/2019/02/21/acae4482-35e0-11e9-854a-7a14d7fec96a\\_story.html](https://www.washingtonpost.com/politics/candidate-says-new-congressional-election-warranted-in-north-carolina/2019/02/21/acae4482-35e0-11e9-854a-7a14d7fec96a_story.html)

Ryan Hutchins: "Activists Spoof Official Union County Website, but Officials Aren't Laughing"

[https://www.nj.com/news/2011/04/activists\\_spoof\\_official\\_union.html](https://www.nj.com/news/2011/04/activists_spoof_official_union.html)

Mary Ellen Klas: "Website Hack Could Be as Bad as Vote Attack, Warns [sic] Florida Officials"

<https://www.tampabay.com/florida-politics/buzz/2019/12/04/web-site-hack-could-be-as-bad-as-vote-attack-warns-florida-officials/>

Brian Krebs: "Election Hoax Sent via D.C. Based E-campaign Group"

[http://voices.washingtonpost.com/securityfix/2008/11/election\\_hoax\\_email\\_sent\\_via.html?nav=rss\\_blog](http://voices.washingtonpost.com/securityfix/2008/11/election_hoax_email_sent_via.html?nav=rss_blog)

Brian Murphy: "Bladen County Early Votes Too Soon in 2018. Witness Alleges Numbers Were Leaked"

<https://www.newsobserver.com/news/politics-government/article222898975.html>

NPR: "How Does One Create a 'Fake News Masterpiece' and What Happens Next?"

<https://www.npr.org/2017/01/22/511103621/how-does-one-create-a-fake-news-masterpiece-and-what-happens-next>

Scott Shane: "From Headline to Photograph, a Fake News Masterpiece"

<https://www.nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html>

Aila Slisco: "Robocalls Spreading Super Tuesday Misinformation Throughout Texas"

<https://www.msn.com/en-us/news/elections-2020/robocalls-spreading-super-tuesday-misinformation-throughout-texas/ar-BB10I3vk>



Isaac Stanley-Becker and Tony Romm: "Conservatives Spread False Claims on Twitter about Electoral Fraud as Iowans Prepare to Caucus"

<https://www.washingtonpost.com/politics/2020/02/03/conservatives-push-false-claims-voter-fraud-twitter-iowans-prepare-caucus/>

Jai Vijayan: "County Election Websites Can Be Easily Spoofed to Spread Misinformation"

<https://www.darkreading.com/vulnerabilities---threats/county-election-websites-can-be-easily-spoofed-to-spread-misinformation/d/d-id/1333132>

Brandy Zadrozny and Jason Abbruzzese: "'Wake-up Call': Iowa Caucus Disinformation Serves as Warning about 2020 Election"

<https://www.nbcnews.com/tech/social-media/wake-call-iowa-caucus-disinformation-serves-warning-about-2020-election-n1130111>

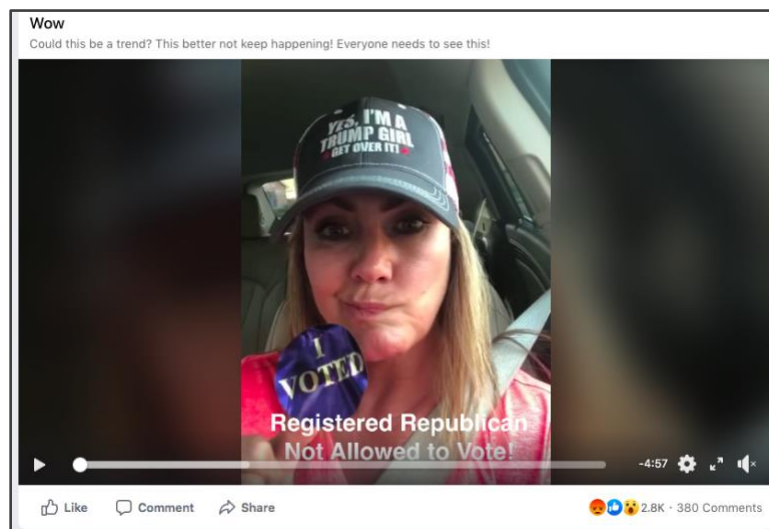


## BREAKOUT EXERCISE

Now's your opportunity to practice responding to an instance of misleading election information. In this 10-minute exercise, we'll introduce a scenario and let you think about how to respond.

## SCENARIO

You are the Clerk of Court for Lafayette Parish, Louisiana, and today is the July 11, 2020 presidential primary. Your office has received many phone calls from voters complaining that they can't vote for the candidate of their choice in the closed primary. You've also received a few calls from outside your community asking what's going on. You discover there's a viral Facebook video about the election that has received millions of views.



In the video, the poster claims she tried to vote Republican in the primary but was told by election workers that she couldn't because she was registered as a Democrat. You look at the comments and see words like "fraud," "corruption," "cheating," and "meddling."

But a colleague checks her registration record and shows you that she has been registered as a Democrat for several years, and you have no reason to believe the record is wrong. So, it seems the video poster is wrong and is misleading people – not just in your community but nationwide – about what's happening.



This video is a classic example of an unverified anecdote, and it's one of the most common ways that false information about elections can spread.

## PLAN YOUR RESPONSE

What should you do? How should you correct the record? Take 3 minutes and respond to the following questions.

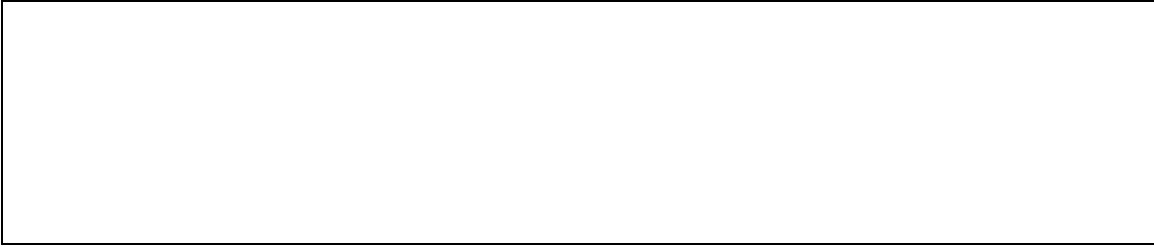
How do you respond?

What do you say?

Where do you place your message?

How can you encourage worried voters?





## HOW'D THEY DO?

Since this exercise is based on a real event, you can look at how Lafayette Parish election officials responded and consider what they did well and what they could have done better.

The Lafayette Parish Clerk doesn't have an official Twitter or Facebook account, and they didn't post about this event on their website or issue a press release. But office staff did speak with local media about it.

### Here's a key passage from a [local news story](#):

*A Lafayette Parish woman wearing a Trump hat posted a video on Facebook on Saturday saying she was not allowed to vote and putting the blame on election officials, alleging corruption.*

*Menard and Clerk of Court Louis Perret both contacted the woman, providing her with her voter registration information that shows she is registered as a Democrat. She originally was registered as a Democrat, switched it to Republican around 2011, then got online and switched her voter registration back to Democrat, they said.*

*As recently as April, she updated her address and kept her registration as a Democrat, Perret said.*

*"Her allegations are completely baseless and false," he added.*

*Around 20 voters visited the Registrar's Office on Monday morning to change their party affiliation, Menard said, primarily from Democrat to Republican.*

*It's not unusual to get 200 complaints during such a closed-primary election, she added.*





*Menard asked voters to be informed of what will be on their ballot before the Nov. 3 presidential election because there will be ballot blackouts once again for Republican Executive Committee, Lafayette City Marshal, judges, justices of the peace and constables.*

## Your assessment

So, how did the Lafayette Parish staff do? What did they do well? What would you do differently?

## SOURCES

Katie Easter: "Voters Run into Issues during Primary Election"

<https://www.katc.com/homepage-showcase/voters-run-into-issues-during-primary-election>

Saranac Hale Spencer: "Video Falseley Stokes Concerns about Voting in Lousiana Primary"

<https://www.factcheck.org/2020/07/video-falsely-stokes-concerns-about-voting-in-louisiana-primary/>

Claire Taylor: "250 Voter Complaints Saturday in Lafayette Parish Due to Wrong Party"

[https://www.theadvocate.com/acadiana/news/politics/article\\_1a57bb8a-c546-11ea-84ee-c370fe710d22.html](https://www.theadvocate.com/acadiana/news/politics/article_1a57bb8a-c546-11ea-84ee-c370fe710d22.html)

YouTube: "#VoterLockOut Are the Democrats aka #Demoncrats" [The original Facebook video has been deleted but is viewable here.]

<https://www.youtube.com/watch?v=sDsWnKlJwXg>



# GETTING AHEAD OF INFLUENCE OPERATIONS

This section covers things you can do to get ahead of influence operations. These are all the things you can do in advance to make it so that influence operations will have less of a disruptive impact.

## BE VOCAL ABOUT THE PROBLEM AND DRIVE PEOPLE TO TRUSTED SOURCES

An important proactive step that's easy to overlook is to talk about the problem of misleading election information. This might look like a paragraph on your website where you talk about the problem. It might be a series of tweets in which you debunk common myths about elections.

Or, the next time you're interviewed for a news story – perhaps one of these frequent stories on how COVID-19 will affect voting in your area – mention that another top concern that you have is about people being misled about how to participate.

No matter where or how you speak out about the problem, always mention a source or two of *trustworthy* election information for voters to rely on – for instance, your county election website and the Secretary of State's Twitter account. The point is that you make clear that the problem is on your radar and that there are trustworthy places for people to go to find good information.



You can see that basic approach in this nice [campaign that the California Secretary of State did in 2018](#). You can see that the message is simple and drives people to go to the SOS website for trustworthy information.

## SHOW YOUR ELECTION OFFICE AS AN OFFICIAL SOURCE OF INFORMATION

And speaking of official sources of information, you should put the work in to make sure that your election department is immediately recognizable as an official source of information. That means doing things like these:

- Set up https and .gov for your election website
- Get verified on Twitter and Facebook (blue check)
- Make your social media accounts look and feel official (add a county seal, add info about the upcoming election, show photos of your staff, etc.)
- Have contact information displayed prominently on your website and social media profiles

Need help getting started? Here are some relevant resources.

### Setting up https

Implementing https will require several technical steps, including obtaining a security certificate. We encourage you to partner with your county IT or website vendor to make this happen.

You'll need to purchase a security certificate. This verifies ownership of the website along with your organization's name and details. You need to provide additional documents to confirm your office's identity. The certificate generally cost less than \$100 per year.

Learn more at <https://https.cio.gov/>.

Ultimately, to implement https, you're looking at some staff time and a reasonable annual fee. We suggest that you give your office a month to complete the process, so don't do this the day or week before an election. The last thing you want to do is make your website unavailable during key election moments.



## Setting up dot gov

Registering your .gov domain does require some paperwork. You'll need a couple points of contact on the registration form, including a technical contact like your County IT or website vendor, so you will definitely need to partner with them on this.

In addition to the documentation, you'll also pay \$400 per year for your domain. This is certainly much more expensive than, say, a Google domain that costs \$12 per year, but the benefits of your website being more secure and trusted are significant, especially in our current election information ecosystem.

Get started by visiting <https://home.dotgov.gov>.

Give yourself a few months to migrate to dot gov. Again, this isn't something you should attempt to do the day or week before an election.

Please note that https is required for a dot gov domain.

So, if you can't get the dot gov domain this year, you should try to implement https this year, with the goal of moving to dot gov for next year.

## Getting verified on Twitter and Facebook

To start the verification process on social media, there are two steps to take. First, you must prepare your accounts for verification. Facebook and Twitter have different account requirements. Then, you can contact your chief election official – typically your state election authority like the Secretary of State – who will work with NASS and NASED to get the accounts verified.

**For Twitter**, you should first make sure the email associated with the account is an official government email.



Two-factor authentication must also be turned on for the account. This means that when you log in, you will have to verify your identity with another method such as an authenticator app or code in your text messages.

Next, you must make sure your profile is personal to your office. This means you should have a personalized cover photo and profile photo. Photos that highlight your community are especially great.

You must also include the purpose of the agency in the bio section of the page. The page should also include a link to the official website of your election office. Finally, the account should be active and using the platform.

Once these six steps are completed on your Twitter account, you are ready to reach out to your chief election official.

**For Facebook**, there are fewer steps to prepare your accounts. First you must have personalized photos. You must also make ensure that the page is specific to your office; it should not represent any other entities.

Those are the only requirements from Facebook before reaching out to your chief election official.

(Alternately, if your state election authority is unable or unwilling to support locals with the verification process, you can try to get verified on your own. Start the process here:

<https://www.facebook.com/help/1288173394636262>)

## **PUBLISH ACCURATE AND USEFUL INFORMATION REGULARLY**

In addition to visually signifying that you're a trusted source of information with your dot gov and your county seal and so on, you need to actually have a history of publishing useful, accurate information on a regular basis.

Imagine for a moment that there are two county election departments. One county has a strong website with information on what's on the ballot, how to become a poll worker, and their local election security practices, and they post regularly on Twitter and Facebook accounts, which are followed by local journalists. The other county's election website is pretty bare bones – basically



just election results and some downloadable forms – and they don't have a social media presence.

Now, if misleading election information is circulating, you can guess which of these election offices will be better positioned to respond and be trusted by their community.

If you've got this covered, great. If you are one of those election offices with a barebones site and little or no social media presence, this might be an area to work on.

## **CREATE A RAPID RESPONSE PROGRAM OR TELEPHONE HELP LINE**

Ensure that if voters have a problem on Election Day, they can get a solution from you instead of venting about it publicly and possibly misleading people. This might be as simple as making sure you have the phone lines sufficiently staffed, or you might decide to create something a little more advanced.

The Electronic Privacy Information Center says that "Whether [election misinformation is] by design or accident, the best defense is to be prepared with accurate information on election participation and the means to deliver it to those who need it."

So, especially during the COVID-19 pandemic, it's a great idea to make sure you have procedure experts on call both for voters and for journalists who may have questions. Of course, even for your everyday staff and election workers, training is essential to keep in mind here.

## **SECURE YOUR COMMUNICATION CHANNELS**

Your communication channels are precious, so you need to protect them. To help avoid any unauthorized user editing your website or commandeering your social media accounts, review who has access to them currently and if the password has been changed recently – especially if there have been staff transitions.

Here are some steps you should take:

- Review permissions for website and social media



- Improve passwords or use password manager
- Set up two-factor authentication
- Draft or revise a social media policy

If you need more background about passwords and two-factor authentication, you can enroll in CTCL's self-paced cybersecurity courses for free through the Election Assistance Commission: <https://learn.techandcivicle.org/library/by/category/cybersecurity>

## **BUILD RELATIONSHIPS WITH SOCIAL MEDIA AND YOUR WEBSITE PUBLISHER**

Protecting access to your website and social media accounts is important, but you should also have contacts prepared in case something bad happens.

For a website, this might look like your office webmaster or your website vendor or both. For social media, there are also people you can contact for help if you need it.

For your reference, we've providing contacts for Facebook, the largest social media platform. This contact information is accurate as of July 2020.

### **Contacts for Facebook**

Southwest and California (AZ, CO, KS, NE, NM, NV, OK, TX, UT, CA)

- Jannelle Watson - [jannelle@fb.com](mailto:jannelle@fb.com)

Northeast and mid-Atlantic (CT, DC, DE, MA, MD, ME, NH, NJ, NY, PA, RI, VA, VT, PR)

- Khalid Pagan - [kpagan@fb.com](mailto:kpagan@fb.com)

Midwest and South (AL, AR, FL, GA, IA, IL, IN, KY, LA, MI, MN, MO, MS, NC, OH, SC, TN, WI, WV)

- Rachel Holland - [rachelholland@fb.com](mailto:rachelholland@fb.com)

Northwest (AK, HI, ID, MT, ND, OR, WA, SD, WY)

- Eva Guidarini - [eguidarini@fb.com](mailto:eguidarini@fb.com)



## LEARN HOW TO REPORT FALSE CONTENT ON SOCIAL MEDIA

In the event of an influence operation, you should reach out to the contacts you have, as we just discussed, but on an ongoing basis, you can also use the regular reporting mechanisms on social media platforms to report any false content you find about elections – whether it’s directly relevant to your community or not.

Below is some basic information on reporting content on several social media platforms


### Reporting content on Facebook

It’s easy to report a post on Facebook. Click the three dots in the top right and select **Find support or report post**. You’ll be prompted to select a reason for reporting, and “voter interference” is one of the available options for categorizing your report.





**Please select a problem to continue** ✕

 You can report the post after selecting a problem.

Nudity Violence Harassment

Suicide or Self-Injury False News Spam


Unauthorized Sales Hate Speech


Terrorism **Voter Interference**

🔍 Something Else

---

Other Steps You Can Take

 **Block**  
You won't be able to see or contact each other.

 **Unfollow**  
Stop seeing posts from this Page

[Next](#)

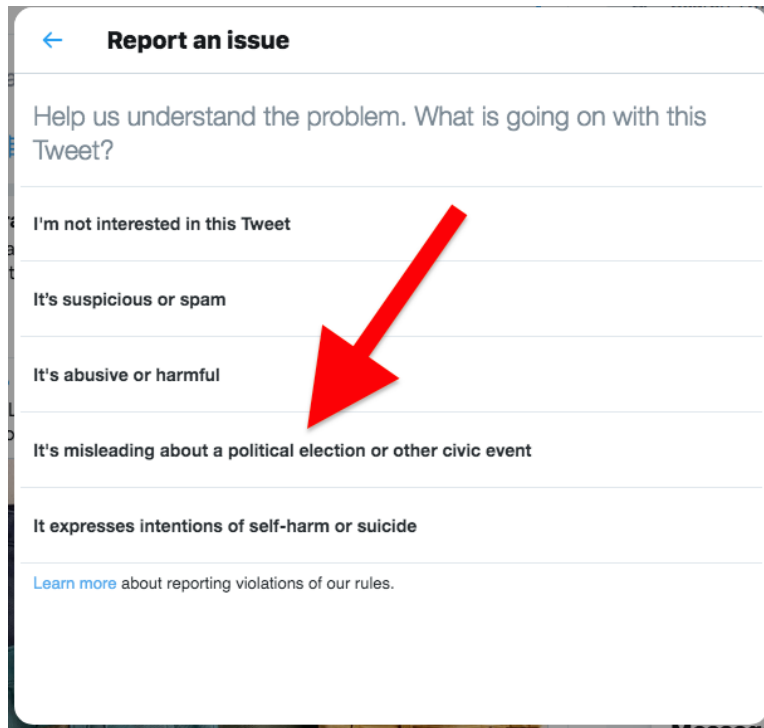
After you submit, you'll get a status update about what action was taken with the post.

For details about Facebook's election misinformation processes, review this article:  
<https://about.fb.com/news/2019/10/update-on-election-integrity-efforts/>.

## Reporting content on Twitter

Reporting tweets is quite similar to reporting Facebook posts. First, click the V "down arrow" symbol in the top right of the tweet and select **Report tweet**. After you do, you can categorize it by selecting **It's misleading about a political election or other civic event**.



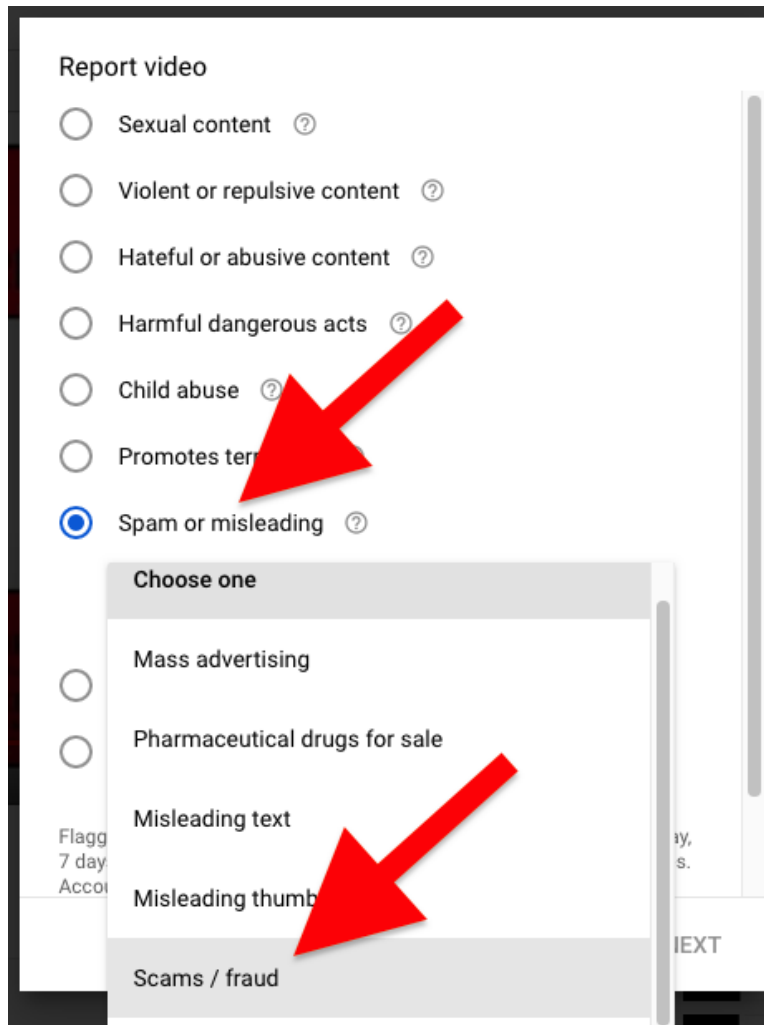


Twitter's Civic Integrity policy gives a general overview of Twitter's relevant policy against voter suppression misinformation: <https://help.twitter.com/en/rules-and-policies/election-integrity-policy>.

## Reporting content on YouTube

To report a YouTube video with false information, click the three dots to the right, below the video, and select **Report**. When prompted, select **Spam or misleading**. Next, from the dropdown menu, you will probably want to select **scam/fraud** to flag inaccurate information within the video itself.





After making a selection and clicking **Next**, you will have the opportunity to indicate the timestamp of when the inaccurate information occurs in the video and to provide additional details about the nature of the problem. Click **Report** once you have finished adding information.

To better understand YouTube’s policies on scams and deceptive practices, review this article: <https://support.google.com/youtube/answer/2801973?hl=en>.



## ESTABLISH MEDIA MONITORING TO SPOT MENTIONS OR FALSE INFO

It's important to know what's being said about your election department and voting in your area, and establishing a system for media monitoring is a good way to do that.

Some election authorities have special systems and programs in place to monitor the conversation about elections in their areas, but you can also do simple things like these:

- Set up [Google Alerts](#) for your election department name to find mentions
- Regularly check social media notifications and mentions
- Do regular Google searches to spot possible spoof sites

Do you remember how the Cook County Clerk provided a quick response to that tweet about the polling place not being open? The reason that happened so quickly is that someone in the Clerk's office was monitoring Twitter, so that shows what the benefits can be here. Monitoring is a good habit all the time, but it's extra important on Election Day.

## STRENGTHEN RELATIONSHIPS WITH LOCAL MEDIA AND JOURNALISTS

Another proactive step you can take that could really pay off in the event of an influence operation is to strengthen your relationships with local media outlets and the people who work there.

If you already have strong relationships, that's great. But if not, it's well worth cultivating relationships with journalists.

COVID-19 could provide you with the perfect opportunity to schedule a call with your local media outlets to share information about how local voters will cast ballots this year. While you're doing that, you're also establishing a bond with the journalist. Just seeing that you're proactive and that you care will make a positive impression on the reporter and the people who read their story.



In the event of a viral election myth circulating in your area, it'll be great to have someone in your local press whom you know and who probably trusts you. This will help if you need to go on the record to correct a piece of information that's false or misleading.

## **WORK WITH FACT CHECKING ORGANIZATIONS**

In addition to having connections with local news, you can think about how national fact-checking organizations might be able to help you deal with information operations.

FactCheck.org actually did a fact check on the Lafayette Parish viral Facebook video and declared its claims false.

Here are some ways you can leverage the services of fact checking organizations:

- Tag them in social media posts with false content
- Report false content to them
- Review their resources to verify or debunk questionable information

One caveat to keep in mind here is that it takes a little bit of time for these organizations to do their fact checks. For instance, the Lafayette Parish fact check was published three days after the election occurred. So just keep in mind this lag time.

### **A few relevant fact checking organizations**

- [FactCheck.org](https://www.factcheck.org/)
- [Politifact](https://www.politifact.com/)
- [Snopes](https://www.snopes.com/)

## **PREPARE YOUR COMMUNICATIONS PLANS AND PROCEDURES**

And our last best practice to help you prepare in the event of an influence operation event is to prepare your communications plans and procedures.



Many election departments have a set of policies and procedures for doing things like issuing a press release and conducting interviews with the press in the event of a crisis or emergency. Getting familiar with these plans – or creating them from scratch, if needed – will be helpful so that you’re not trying to track down the phone number for your state public information officer at 11:00 a.m. or whenever you have a problem.

You also may want to add to your existing plans some ideas specific to dealing with false or misleading information.

So maybe think about how you’ll judge whether or not an election myth is significant enough to be worth addressing at all. A one-off tweet that’s not getting much attention may be something you just pay attention to rather than springing into crisis mode. If something is judged to be significant, you need to consider things like contacting the relevant publishing platforms, reporting the post, contacting media, posting a correction on your outreach channels, and so on. With each of these steps come questions about who should do the talking, what they should say, and who needs to approve it all.

What your procedures look like is up to you and will be different for every election department, but the point here is to have a clear sense of your plans ahead of time to help avoid having to make difficult calls in the heat of the moment.

## SOURCES

Ad Hoc Committee for 2020 Election Fairness and Legitimacy: “Fair Elections during a Crisis”  
<https://www.law.uci.edu/faculty/full-time/hasen/2020ElectionReport.pdf>

Alliance for Securing Democracy: “20 for 20: 20 Ways to Protect the 2020 Presidential Election”  
<https://securingdemocracy.gmfus.org/20-for-20-20-ways-to-protect-the-2020-presidential-election>

Belfer Center: “National Counter-information Operations Strategy”  
<https://www.belfercenter.org/publication/national-counter-information-operations-strategy>

Belfer Center: “The State and Local Election Cybersecurity Playbook”



<https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook>

Electronic Privacy Information Center: "E-deceptive Campaign Practices Report 2010: Internet Technology and Democracy 2.0"

[https://epic.org/privacy/voting/E\\_Deceptive\\_Report\\_10\\_2010.pdf](https://epic.org/privacy/voting/E_Deceptive_Report_10_2010.pdf)

Miles Parks: "1 Simple Step Could Help Election Security. Governments Aren't Doing It"

<https://www.npr.org/2020/01/29/800131854/1-simple-step-could-help-election-security-governments-arent-doing-it>



# RESPONDING TO INFLUENCE OPERATIONS

The previous section covers things you can do in advance of an influence operation event. But what should you actually say or do once an event has occurred and you decide it needs to be addressed?

There's a huge body of research devoted to effective methods for debunking falsehoods. We've digested best practices down into a four-step response framework to make it easy for you to approach.

## INTRODUCING: AN INFLUENCE OPERATIONS RESPONSE FRAMEWORK

When it comes to responding to influence operations, most people's intuitive sense is to just say the original information was false and then to provide a fact check.

But research shows that's not enough to effectively respond, in large part because emotions are triggered with influence operations and because falsehoods often stick in people's memory. This framework is intended to correct the record effectively.

<b>1. Acknowledge</b>	Acknowledge the emotions behind the falsehood you're responding to and affirm shared goals
<b>2. Inform</b>	Provide correct (or additional) information to counter the original falsehood
<b>3. Explain</b>	Offer an alternative explanation or narrative to fill the gap left by the original falsehood
<b>4. Empower</b>	Give people a way to gain further information and resolve any concerns that may linger

Let's examine each of these individually.





## ACKNOWLEDGE: AFFIRM EMOTIONS AND SHARED GOALS



Before you deploy facts, you need to need to prime your audience a little by acknowledging the emotions and norms behind the original falsehood you're responding to

- Emphasize shared feelings and goals
- Focus on visions shared across the political spectrum: civic participation, democracy, accountability, having your voice heard, security, integrity
- Example: "As County Clerk, my top priority is to ensure every eligible voter is able to participate as they intend."

No matter what the falsehood, you can find *some* way to affirm shared goals. These are the sort of things you might put in an election office mission or vision statement.

This step is incredibly important because experts have demonstrated that if you affirm people's feelings and beliefs, they will then be much more receptive to messages that otherwise they might feel threaten their values or invalidate their feelings.

Also, remember that emotions and values are a critical part of why false information gets shared in the first place, so that means your response also needs to account for the emotional elements of communication and idea sharing.

## INFORM: PROVIDE FACTS TO OFFSET THE FALSEHOODS



Now you get to deploy your facts. The way you do that will vary depending on the type of influence operation, and that's why we introduced mis-, dis-, and malinformation. Here's how you should approach the task of providing information:

- For mis- and disinformation, provide correct information
- For malinformation, provide additional information to reframe the misleading information
- Avoid repeating the falsehood. If you must mention it, include it in the text but not the headline.

This last point deserves a bit of explanation. Experts believe that by repeating a falsehood, you give it more oxygen and could have the effect of spreading it further.

So, if the myth is that one party votes on Tuesday and another on Wednesday, just say that, as always, all eligible voters vote on Tuesday. If you feel you must reference the myth, just don't lead with it. Include it in your paragraph but not in your headline.

## **EXPLAIN: GIVE AN ALTERNATIVE NARRATIVE**



After you've provided your facts, it's good to give a bit of explanation to account for how you got there. This is important because studies have shown that even when people accept a correction, the original misinformation often sticks in their minds, too. So, this alternative narrative could be an explanation for why or how the falsehood came about or suggestions for why the people who promoted the falsehood may not be credible.

- Give an alternative causal explanation to fill in the gaps
- Example: "As recently as April, she updated her address and kept her registration as a Democrat"
- Make sure your explanation isn't more complicated than the myth



The Lafayette Parish election officials did a good job of this when responding to the Facebook user who claimed poll workers were wrong about her voter registration. They looked at her record and found she originally registered as a Republican in 2011 and then switched to be a Democrat a few years later. They told the local newspaper that “As recently as April, she updated her address and kept her registration as a Democrat.”

That’s a good alternative narrative to explain what happened.

One final thing to remember here is to keep your explanation as simple as possible. Myths are often attractive because they’re simple. Try to make the truth simple, as well.

## **EMPOWER: HELP PEOPLE LEARN MORE AND RESOLVE CONCERNS**



Finally, just in case your audience has some lingering concerns, you can empower them to learn more and resolve those concerns. We’ve already seen a few examples of this, like when Secretary of State Paul Pate provided a link to the accurate voter registration records. And when the Texas Secretary of State’s office encouraged voters to use their official Twitter account as a source of reliable information. We’ve seen that most cases of false information are intended to leave voters feeling powerless, so the idea here is to do just the opposite.

- Provide pathway sot help voters take an action relevant to the topic at hand
- Example: “To double check which party you’re registered with, verify your registration at [countyelections.gov](http://countyelections.gov)”

In the Lafayette Parish case, you could encourage anyone worried they might not be able to vote for their preferred party to double check their voter registration on your website.



## SOURCES

Belfer Center: "Election Cyber Incident Communications Coordination Guide"

<https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide>

John Cook and Stephan Lewandowsky: "The Debunking Handbook"

[https://skepticalscience.com/docs/Debunking\\_Handbook.pdf](https://skepticalscience.com/docs/Debunking_Handbook.pdf)

Council of Europe: "Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making"

<https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>

First Draft: "How Emotional Skepticism Can Help Protect Vulnerable Communities"

<https://www.youtube.com/watch?v=UOLk8YhfmYM&feature=youtu.be>

Ideas42: "Official Communications with Voters During COVID-19"

<https://www.ideas42.org/wp-content/uploads/2020/07/COVID-Voter-Communications.pdf>

E.K. Vraga, S.C. Kim, J. Cook, and L. Bode: "Testing the Effectiveness of Correction Placement and Type on Instagram"

[https://www.climatechangecommunication.org/wp-content/uploads/2020/06/Vraga\\_2020\\_Facts\\_v\\_Logic\\_prepress.pdf](https://www.climatechangecommunication.org/wp-content/uploads/2020/06/Vraga_2020_Facts_v_Logic_prepress.pdf)



## GROUP DISCUSSION

As the final part of our course, we want to chat with you about your ideas and plans regarding influence operations in elections.

- What resonated with you from today's course?
- What are your next steps?
- What questions do you have about what we covered today?
- What questions do you have about what we *didn't* cover today?

## AS QUESTIONS COME UP FOR YOU

Even after the course is over, we want to serve as a resource for you! We can't help on every inquiry, but we're committed to at least pointing you in the right direction.

Email us at [hello@techandcivicliflife.org](mailto:hello@techandcivicliflife.org).



# AN ELECTION OFFICIAL'S CHECKLIST FOR COMBATING INFLUENCE OPERATIONS

For use with the participant guide accompanying CTCL's Combating Election Misinformation course. Questions? Email [courses@techandcivicliflife.org](mailto:courses@techandcivicliflife.org).

## GETTING AHEAD OF INFLUENCE OPERATIONS

See "Getting Ahead" section of the participant guide for details on each of these best practices.:

- Be vocal about the problem of election misinformation and drive people to trusted sources
- Show that your election office is an official source of information about where and how to vote
- Publish accurate and useful information about voting processes regularly
- Create a rapid response program or telephone help line for voters' questions
- Secure your communication channels (website and social media)
- Build relationships with social media companies and your website publisher
- Learn how to report false content on social media
- Establish media monitoring to spot mentions or false info
- Strengthen relationships with local media and journalists
- Work with fact checking organizations
- Prepare your communications plans and procedures

## RESPONDING TO INFLUENCE OPERATIONS

See "Responding" section of the participant guide for details on this four-step framework



### 1. Acknowledge

- Acknowledge the emotions and norms behind the falsehood you're responding to
- Emphasize shared feelings and goals



- Focus on visions shared across the political spectrum: civic participation, democracy, accountability, having your voice heard, security, integrity
- Ex: "As County Clerk, my top priority is to ensure every eligible voter is able to participate as they intend"



## 2. Inform

- Provide correct (or additional) information to counter the original falsehood
- For mis- and disinformation (false information), provide correct information
- For malinformation (true but disruptive information), provide additional information to reframe the misleading information
- Avoid repeating the falsehood. If you must mention it, include it in the text but not the headline.



## 3. Explain

- Offer an alternative explanation of narrative to fill the gap left by the original falsehood
- Explain why or how the original falsehood came about, suggest why the people who promoted it may not be credible, offer additional information to support your facts.
- Make sure your explanation isn't more complicated than the myth
- Ex.: "As recently as April, she updated her address and kept her registration as a Democrat"



## 4. Empower

- Give people a way to gain further information and resolve any concerns that may linger
- Provide pathways to help voters take an action relevant to the topic at hand
- Ex.: "To double check which party you're registered with, verify your registration at [countyelections.org](http://countyelections.org)"

