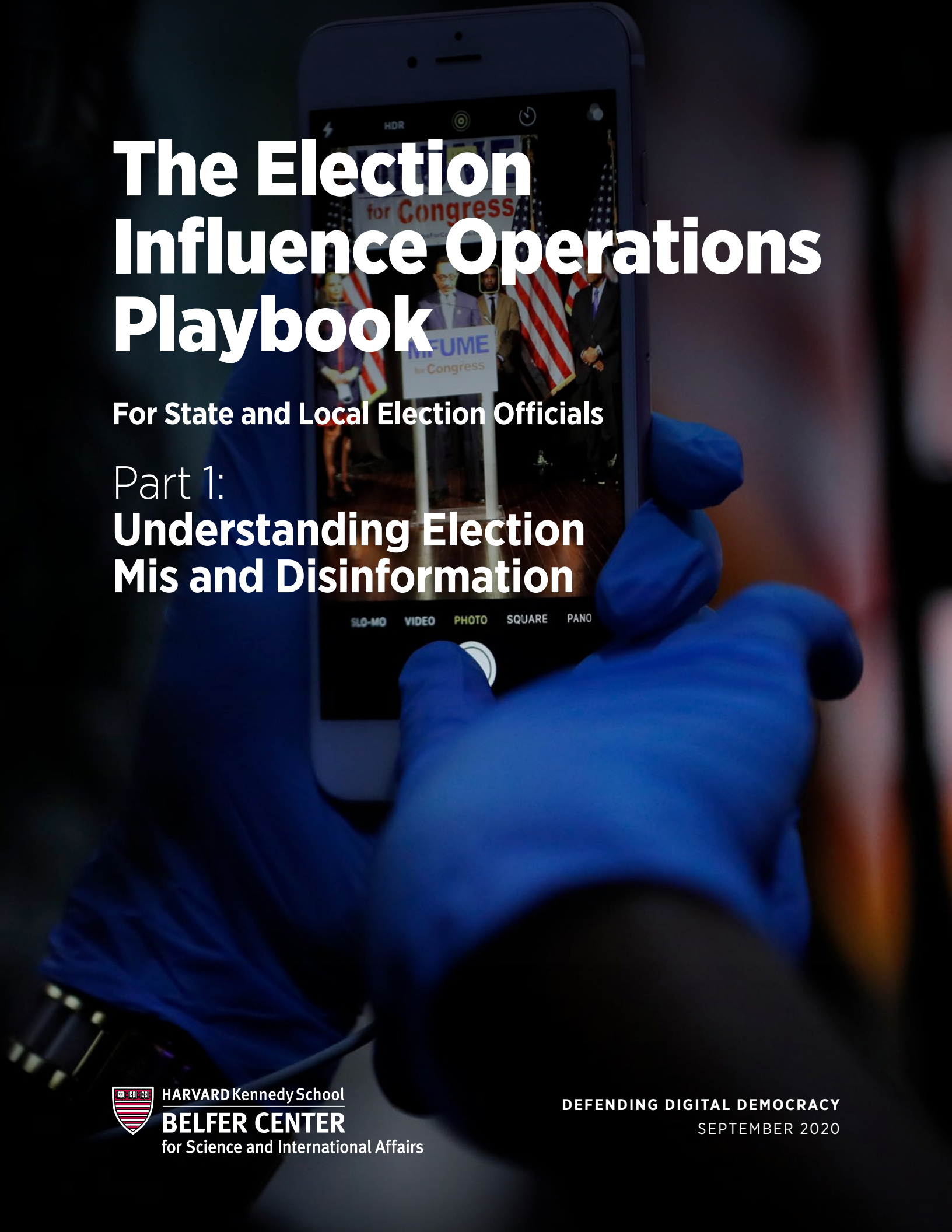


The Election Influence Operations Playbook

For State and Local Election Officials

Part 1: Understanding Election Mis and Disinformation

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
SEPTEMBER 2020

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design & Layout by Andrew Facini

Cover photo: A staff member in the Kweisi Mfume campaign uses gloves while holding a cell phone during an election night news conference at his campaign headquarters after Mfume, a Democrat, won Maryland's 7th Congressional District special election, Tuesday, April 28, 2020, in Baltimore. (AP Photo/ Julio Cortez)

The Election Influence Operations Playbook

Part 1: Understanding Election Mis and Disinformation

Contents

Authors and Contributors

The Defending Digital Democracy Project would like to thank everyone who contributed to making this Playbook a helpful resource for officials to best counter this pressing threat.

AUTHORS

Eric Rosenbach, Co-Director, Belfer Center; Director, Defending Digital Democracy Project

Maria Barsallo Lynch, Executive Director, D3P

Siobhan Gorman, Partner, Brunswick Group, Senior Advisor, D3P

Preston Golson, Director, Brunswick Group; D3P

Robby Mook, Co-Founder, Senior Advisor, Senior Fellow, D3P

Nick Anway, D3P, Harvard Kennedy School

Gabe Cederberg, D3P, Harvard University

Bo Julie Crowley, D3P, Harvard Kennedy School

Jordan D'Amato, D3P, Harvard Kennedy School

Raj Gambhir, D3P, Harvard University

Matthew Graydon, D3P, Massachusetts Institute of Technology

Gauri Gupta, D3P, Tufts University, Fletcher School

Simon Jones, D3P, Harvard Kennedy School

Matt McCalpin, D3P, Harvard Kennedy School

Nagela Nukuna, D3P, Harvard Kennedy School

D'Seanté Parks, D3P, Harvard Kennedy School

Freida Siregar, D3P, Harvard Kennedy School

Reed Southard, D3P, Harvard Kennedy School

David Stansbury, D3P, Harvard Kennedy School

Danielle Thoman, D3P, Harvard Kennedy School

CONTRIBUTORS

Debora Plunkett, Belfer Cyber Project, Principal, Plunkett Associates LLC; Senior Advisor, D3P

Suzanne Spaulding, Senior Advisor for Homeland Security, Center for Strategic and International Studies; Senior Advisor, D3P

Michael Steed, Founder and Managing Partner, Paladin Capital Group; Senior Advisor, D3P

Michelle Barton, D3P, Harvard Kennedy School

Alberto Castellón, D3P, Harvard Kennedy School

Caitlin Chase, D3P, Harvard Kennedy School

Mari Dugas, D3P, Harvard Kennedy School

Jeff Fields, D3P, Harvard Kennedy School

Sasha Maria Mathew, D3P, Harvard Kennedy School

Maya Nandakumar, D3P, Harvard Kennedy School

Janice Shelsta, D3P, Harvard Kennedy School

Utsav Sohoni, D3P, Harvard Kennedy School

Ashley Whitlock, D3P, Harvard Kennedy School

CONTRIBUTORS, CONTINUED

Lori Augino, Director of Elections, Office of the Secretary of State, OR

Ginny Badanes, Director of Strategic Projects, Cybersecurity & Democracy, Microsoft

Maria Benson, Director of Communications, National Association of Secretaries of State

Tyler Brey, Press Secretary, Secretary of State's Office, LA

Karen Brinson Bell, Executive Director, State Board of Elections, NC

Amy Cohen, Executive Director, National Association of State Election Directors

Veronica Degraffenreid, Director of Election Operations, NC

Alan Farley, Administrator, Rutherford County, TN Election Commission

Patrick Gannon, PIO, State Board of Elections, NC

Amy Kelly, State Board of Elections, IL

Donald Kersey, General Counsel. Secretary of State's Office, WV

Nicole Lagace, Senior Advisor to Sec of State Nellie M. Gorbea, Chief of Information, Department of State, RI

Susan Lapsley, Deputy Sec of State, HAVA Director and Chief Counsel, Secretary of State's Office, CA

Sam Mahood, Press Secretary, Secretary of State's Office, CA

Matt Masterson, Senior Cybersecurity Advisor, DHS Cybersecurity & Infrastructure Security Agency

Brandee Patrick, Public Information Director, Secretary of State's Office, LA

Leslie Reynolds, Executive Director, National Association of Secretaries of State

Rob Rock, Director of Elections, RI Department of State

Brian Scully, Chief, Countering Foreign Influence Task Force, DHS/CISA/NRMC

Paula Valle Castañon, Deputy Sec of State, Chief Communications Officer, Secretary of State's Office, CA

Mac Warner, Secretary of State, WV

Meagan Wolfe, Administrator, WI Elections Commission

Communications Team, Secretary of State's Office, OH

Center for Internet Security

Elections Infrastructure Information Sharing and Analysis Center

Google Civics Team

Politics & Government Outreach Team, Facebook

Twitter Legal

BELFER CENTER COMMUNICATIONS AND DESIGN

Andrew Facini, Publishing Manager, Belfer Center

Katie Shultz, D3P, Harvard Kennedy School

Belfer Center Communications Team

About the Defending Digital Democracy Project

We established the Defending Digital Democracy Project (D3P) in July 2017 with one goal: to help defend democratic elections from cyber-attacks and information operations. Over the last three years, we have worked to provide campaign and election professionals in the democratic process with practical guides, trainings, recommendations and support in navigating the evolving threats to these processes.

In November 2017, we released "**The Campaign Cybersecurity Playbook**" for campaign professionals. In February 2018, we released a set of three guides designed to be used together by election administrators to understand pressing cybersecurity threats to elections and recommendations to counter them: "**The State and Local Election Cybersecurity Playbook**," "**The Election Cyber Incident Communications Coordination Guide**," and "**The Election Incident Communications Plan Template**." In December 2019, we released the "**The Elections Battle Staff Playbook,**" to build on how election officials continue their work in countering this new era of information threats to the already demanding work in administering elections.[1]

D3P is a bipartisan team of cybersecurity, political, national security, technology, elections and policy experts. Throughout the course of our work, we've visited with over 34 state and local election offices, observed the November 2017 election, the 2018 midterms and conducted interviews across the election and national security field and conducted research to identify nuances in election processes and corresponding risk considerations. We have had the honor of training hundreds of officials from across the country during national "tabletop exercise (TTXs)" to increase awareness of the cybersecurity and information threats elections face and explore mitigation strategies. Ahead of the 2020 election we conducted a live national TTX and trained over 750 officials nationally through sessions on cyber and information threats and digital TTXs.

We have had the honor of training hundreds of officials from across the country during national TTXs. After releasing a first version of the Influence Operations Playbook in 2019, we received feedback on vital information that would help officials report incidents. We also wanted to spend time researching and recommending how to best respond to these incidents and develop communications tools. In less than a year, so much has changed in what we know about influence operations, as have the tools available to report and counter them. As with all of our work, we hope these guides support the incredible work that you do to defend democracy.

Influence Operations are an evolving threat. There are not concrete solutions. The strategies to counter these threats to elections will also continue to evolve. The recommendations shared throughout the Playbook are informed by what we know today with an understanding that we will continue to learn more about the best strategies and tools to bolster our ability to counter these threats. Frameworks and recommendations shared in this Playbook are meant to be a starting point and should be adapted for your jurisdiction's needs

Thank you for your leadership and public service.

Best of luck,
The D3P Team

1 D3P Playbooks can be found at: https://www.belfercenter.org/project/defending-digital-democracy#!playbooks

The Playbook Approach

This series of Playbooks aim to provide election officials with resources and recommendations on how to navigate information threats targeting elections.

The Playbook is divided into three parts that are intended to work together to understand, counter, and respond to influence operations:

The Election Influence Operations Playbook
For State and Local Officials

- *Part 1: Understanding Election Mis and Disinformation*
- *Part 2: The Mis/Disinformation Response Plan*
- *Part 3: The Mis/Disinformation Scenario Plans*

Part 1 provides an introduction to Influence Operations: what they are, who is carrying them out, why they can impact our elections, and how they work. It is designed as a preface to Parts 2 and 3, which provide tactical, detailed advice on tangible steps you can take to counter, report, and respond.

Executive Summary

The threat of Influence Operations (IO) strikes the core of our democracy by seeking to influence hearts and minds with divisive and often false information. Although malicious actors are targeting the whole of society, these D3P Playbooks focus on **a subset of influence operations—the types of disinformation attacks and misinformation incidents most commonly seen around elections**, where election officials are best positioned to counter them.

We understand that election officials face a large and growing list of responsibilities in conducting accurate, accessible, and secure elections. In this era of attacks on democracy, your preparations, your response, and your voice as a trusted source within your jurisdiction, in coordination with other officials across your state, will strengthen your ability to effectively counter these threats.

This Playbook helps you both respond to and report these incidents. It connects you to organizations that can support your process, like the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the Federal Bureau of Investigation (FBI), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).

Social media platforms are creating more ways for election officials to report false information that may affect elections. This Playbook provides you with an introduction to some of the most prominent online platforms where these incidents could gain traction and shares information so you can report incidents. It also highlights tools that can aid your response.

U.S. national security officials have warned that malicious actors will continue to use influence operations and disinformation attacks against the United States during and in the lead up to the 2020 election. Election officials must be prepared. Our hope is that this Playbook can be a resource to help you counter these evolving threats in your work protecting our democracy.

101: Influence Operations, Disinformation and Misinformation

What are Influence Operations?
Defining Mis/Disinformation

Influence Operations (IO), also known as Information Operations, are a series of warfare tactics historically used to collect information, influence or disrupt the decision making of an adversary.[2,3] IO strategies intentionally disseminate information to manipulate public opinion and/or influence behavior. IO can involve a number of tactics. One of these tactics, most recently and commonly seen in an effort to disrupt elections, is spreading *false* information intentionally, known as "disinformation."[4] Skilled influence operations often deliberately spread disinformation in highly public places like social media. This is done in the hope that people who have no connection to the operation will mistakenly share this disinformation. Inaccurate information spread in error without malicious intent is known as 'misinformation'.[5]

> **Disinformation** *is false or inaccurate information that is spread deliberately with malicious intent.*
>
> **Misinformation** *is false or inaccurate information that is spread mistakenly or unintentionally.*

IO tactics can include using non-genuine accounts on social media sites (known as 'bots'), altered videos to make people appear to say or do things they did not (known as 'deep fakes'), photographs or short videos with text embellishments or captions (known as 'memes'), and other means of publicizing incorrect or completely fabricated information. Content is often highly emotive, designed to increase the likelihood that it will be further shared organically by others.

2 "Information Operations, Joint Publication 3-13" Joint Chiefs of Staff. November 20, 2014.https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

3 "Information Operations" Rand Corporation. https://www.rand.org/topics/information-operations.html.

4 "Information Disorder: Toward an interdisciplinary framework for research and policymaking" Claire Wardel, Hossein Derakhshan, Council of Europe. September 2017. https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking/.

5 Ibid.

These are only some tactics using information to influence. This Playbook explores mis and disinformation incidents that specifically focus on elections operations and infrastructure. As an election official you may not often see or know what the motivation is behind the incidents you encounter, or whether they are mis or disinformation. Throughout these guides we refer to mis/disinformation *incidents* together, as the strategies for countering or responding to them are the same.

Who is Engaging in Mis/Disinformation?

Social media has made it easy for bad actors, including nation states, to organize coordinated influence operations at an unprecedented scale. These same technologies have enabled individuals to engage with mis and disinformation, independently of coordination by nation-states or other actors. Individuals that engage with malicious intent in spreading or amplifying mis or disinformation are often referred to as 'trolls'. Their engagement in furthering this information can help spur its spread and traction.

The U.S. intelligence community concluded that the Russian government ran a disinformation operation to distort U.S. public opinion during the 2016 elections.[6] Russian intelligence officers created hundreds of fictitious U.S. personas to polarize and pollute our political discussion. But Russia is not alone. China is conducting a long-term disinformation operation to manipulate sentiments of American audiences into supporting and voting for pro-China policies.[7] Iran is similarly recognized as a state actor emergent in its use of IO tactics.

In the past couple of years, there has been a rise in domestic use of disinformation whereby domestic actors capitalize on either domestically or foreign-generated disinformation by pushing it aggressively on social media to further their agenda. In 2016, foreign actors largely created false content that they perpetuated, now their prevailing tactics seek to amplify domestically created content. This trend raises cause for concern that election targeted IO can also be used by foreign or domestic actors for political purposes, and election officials, in particular, have voiced alarm about how to counter domestic disinformation campaigns.

6 "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution." Office of the Director of National Intelligence. January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

7 "China's Influence & American Interests: Promoting Constructive Vigilance." Hoover Institution, Stanford University. November 2018. https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance.

Why do Mis/Disinformation Incidents Matter?

By feeding U.S. social media and daily news a steady diet of misleading information, adversaries are trying to erode Americans' trust in election processes and outcomes. These attacks seek to influence policy priorities, sway voter turnout, disrupt the timing and location of election processes like voting and registration, and undermine the public's faith in election officials.

In 2018, Pew Research Center found that 47% of Americans feel somewhat confident in the accuracy of their vote being counted.[8] In 2020, research from Gallup showed that a majority of the public (59%) feel low confidence in the honesty of the elections process.[9] Mis and disinformation incidents can exacerbate issues of confidence and distrust in the integrity of the election . As an official, your ability to recognize and counter these incidents to ensure voters are not deceived in exercising their right to vote, is essential.

Although reporting these incidents has been an important part of countering them, we believe the equally important countermeasure is your response. Your ability to be a trusted voice in sharing accurate information that counters false information is important. Always consider how your responses may interact with the complex factors behind these incidents, which may be difficult to predict and plan for.

During our work to write these guides, we collected some example scenarios that are drawn from past events, or narratives we judge to be highly likely in the coming election. While mis/disinformation vary, common mis/disinformation messages most likely to gain traction in elections are:

- The voting process is confusing and difficult (particularly with the rise in vote by mail).
- There has been a failure in the mechanics of how elections are run.
- Political partisans are "stealing the election."
- The people who run elections are corrupt.
- COVID-19 concerns are impeding voting or delaying the election.

8 "Elections in America: Concerns Over Security, Divisions Over Expanding Access to Voting Pew Research Center" Pew Research Center. October 2018. https://www.pewresearch.org/politics/2018/10/29/confidence-in-accurate-vote-counts-election-administration/

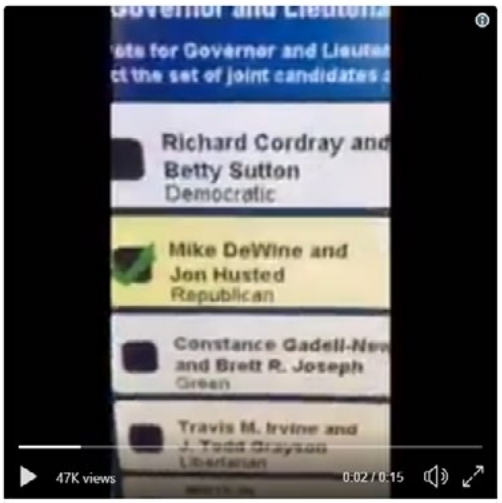
9 "Faith in Elections in Relatively Low Supply." Gallup. "https://news.gallup.com/poll/285608/faith-elections-relatively-short-supply.aspx. Feb 13.2020.

- Results that are not in by election night call into question the administration or legitimacy of the election.

Part 3 of the IO Playbook, the Mis/Disinformation Scenario Plans, offers scenario planning materials expanding on these examples. It is available exclusively for election officials.

Case Study on Misinformation: Franklin County, Ohio

Misinformation incident:
Video with Mistaken Information



Incident: On Election Day in 2018, a video went viral on Twitter and Facebook that showed a dysfunctional voting machine in Franklin County, Ohio. The video claimed the machine was intentionally changing a vote from one candidate to another after it had been cast.

Franklin County officials spotted the tweet and Facebook post and immediately investigated the incident. They found that the posts were misleading. In reality, a voting machine had a simple paper jam which delayed the printed paper ballot several minutes after a vote was cast on the device.

> More voter fraud in Ohio. Why is it that all the errors are always the Democrats?? Because the only way they win is if they cheat!! This madness needs to stop.
>
> See something say something!!@realDonaldTrump @POTUS @VP @DHSgov @FBI do something. pic.twitter.com/CcMO6HPFza
>
> — WWG1WGA (@findtruthQ) November 6, 2018

Reporting: Franklin County officials escalated the issue to the Ohio Secretary of State's Office, who worked with NASS, NASED, and other federal agencies to report this misleading content to Facebook and Twitter. After an investigation from independent fact-checkers, Facebook took the video down under its voter suppression policies. Twitter did not remove the video, but promoted tweets by Franklin County's spokesperson that exposed the original content as disinformation.

Response: In parallel, Ohio state and Franklin County officials launched a public communications effort to correct the misleading information. Spokespersons for the Ohio Secretary of State and Franklin County Board of Elections coordinated outreach to CNN, the Associated Press, and other news organizations to clarify why the video was false. The Franklin County Board of Elections posted an article on its Facebook page.

Within hours, County officials had successfully limited the scope and impact of this incident.

Case Studies on Disinformation: North Carolina

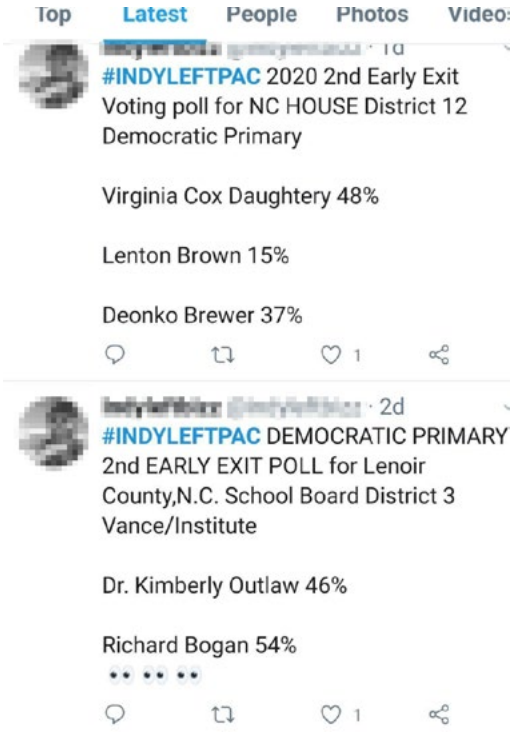
Disinformation Incident:
Fake Facebook Page in Swain County

Incident: In December 2019, a County Sheriff in North Carolina notified local election officials that they had seen a suspicious Facebook page. It claimed to be the page of Swain County' Board of Elections. Swain County Board of Elections confirmed that they did not have a Facebook page.

Reporting: Swain County Officials swiftly reported the spoof page to their State Board of Elections. Officials made use of the links they had established with Facebook representatives ahead of the election. They included a screenshot of the spoof page, as well as the URL. Facebook took the page down on the same day it was reported.

Response: State and County Officials assessed that the page was currently low profile, with few active followers and likes. They decided that a public communications response would likely bring more attention to the spoof site and chose not to respond via public communications channels. Within hours, Swain County and North Carolina officials had resolved the incident.

Disinformation Incident: Twitter Results Disinformation Amplified in Lenoir County



Incident: In November of 2019, Lenoir County held municipal elections. Lenoir is a rural county in North Carolina.

A candidate standing in the election notified the Lenoir County Board that an account on Twitter had begun posting "exit poll results". At the time, the exit polls had not yet taken place. In-person early voting had not yet begun, and the number of by-mail absentee ballots cast was so small that the percentages being reported by the account were impossible.

Officials later noted the manner in which this Twitter account reported "results" sought to stoke tension around divisive issues. The posts began to gain traction, receiving attention from other candidates.

Reporting: Lenoir County Board of Election officials reported the incident to North Carolina Board of Elections (NCBE) officials. Other actors also reported the Twitter account to the NCBE too.

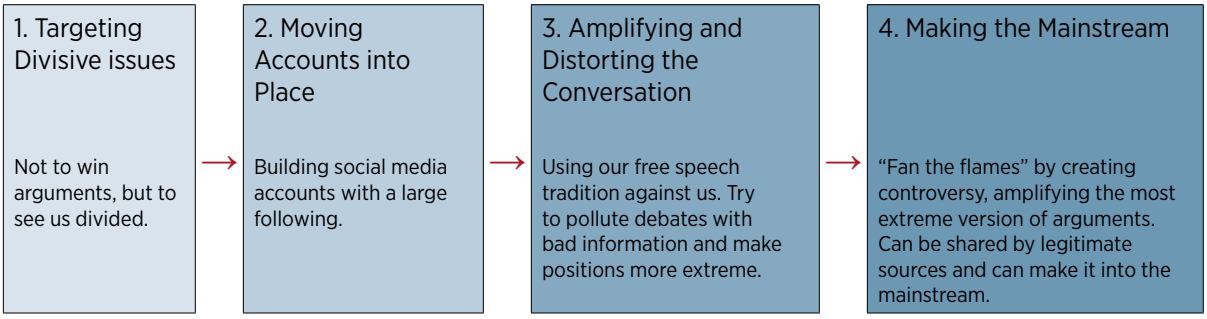
The NCBE reported the incident to Twitter, using the social network's reporting portal. NASED also reported the incident to Twitter after being made aware of it by NCBE. Twitter investigated swiftly and was able to respond to the NCBE within hours. However, in this case Twitter determined that the content did not violate their policies and the tweets were not taken down. NASED continued to engage with Twitter to clarify how the decision on the incident applied to Twitter's policies.

Response: NCBE worked with Lenoir County Board officials to respond. Given the traction, officials refuted claims from their Twitter account. The account's suggestions of "voting straight ticket" for one political party indicated that this was a potential disinformation incident. North Carolina prohibits voting this way.

Although the incident could not be removed, reporting was important.

The Cycle of an Influence Operation

The full scope of an influence operation is varied and hard to piece together with publicly available information. However, analyzing past election cycles, there are broad trends that help detail how many incidents of disinformation coordinate to reach different phases in an overall influence operation.[10] Understanding this broader process can help your analysis of incidents you might face.



1. Targeting Divisive Issues[11]

Influence Operations seek to target societal wedge issues and intensify them. Issues we might consider politically divisive have been a prime target. The goal of these operations is to further divide us and stoke tensions among us.

The U.S. Department of Justice's criminal complaint against one of the alleged actors in the Russian influence operations during the 2016 election details some of the issues chosen to conduct IO:[12]

10 Cybersecurity and Infrastructure Security Agency (CISA) "War on Pineapple: Understanding Foreign Interference in 5 Steps." https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_The-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf. June 2019.

11 Cybersecurity and Infrastructure Security Agency (CISA) "War on Pineapple: Understanding Foreign Interference in 5 Steps." https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_The-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf. June 2019.

12 United States of America v. Elena Alekseevna Khusyaynova. No.I.18-MJ-464. United States District Court, Eastern District of Virginia, Alexandria Division. September 28, 2018. Paragraph 25. https://www.justice.gov/usao-edva/press-release/file/1102591/download

- Immigration
- Gun control and the Second Amendment
- The confederate flag
- Racial issues and race relations
- LGBTQ issues
- The Women's March
- The NFL national anthem debate

The complaint notes that these actors used incidents like shootings of church members in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada to further themes and messages.

2. Moving Accounts into Place[13]

Influence operations conducted by malicious actors often invest time and resources in building large followers of authentic and inauthentic users ('bots') on social media platforms. Actors can have multiple social media accounts. They use tools like paid advertising, and algorithmic learning to better target messages and ads for increased engagement by platform users with the content they create or share.[14]

Dividing America: How Russia Hacked Social Media and Democracy
Sen. Michael Bennet

13 Cybersecurity and Infrastructure Security Agency (CISA) "War on Pineapple: Understanding Foreign Interference in 5 Steps." https://www.dhs.gov/sites/default/files/publications/19_0717_cisa_The-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf. June 2019.

14 Michael Bennet. "Dividing America: How Russia Hacked Social Media and Democracy." July 2019.

These examples were created by Russia in the 2016 election. In the 'Don't Shoot' example on the right, they created a fake website and linked it to a Facebook page. Using paid advertising, this Facebook page targeted users interested in this issue and engaged them. To Facebook users, this looked like a valid official organization. False content is created with the goal of engaging users. In the 'We the People' example on the left, the Russians targeted supporters of a presidential candidate, and those of a similar political ideology. They created Facebook pages focused on these supporters to gain followers. They used tools like paid advertising to target supporters and tried to engage them by signing a petition to disqualify a presidential opponent.[15]

3. Amplifying and Distorting the Conversation[16]

Malicious actors often seek to distort debates in U.S. civil discourse by intentionally starting a fight or "trolling" people. Sometimes bots (fake accounts) are used to amplify this divided dynamic. The goal is to elicit strong emotions, create engagement and influence perception.

4. Making it Mainstream[17]

By creating division across conversations or issue areas, malicious actors intentionally elevate the extremes of arguments in a particular issue area to create controversy and attention. By effectively positioning accounts that engage with real people, the information shared is further spread until it gets to more legitimate information sources—even ultimately mainstream media, or moving offline into in-person activities, like the 2016 protests organized by Russian operatives. Going mainstream is the mark of a successful influence operation.[18]

15 Ibid, p. 14.

16 Cybersecurity and Infrastructure Security Agency (CISA) "War on Pineapple: Understanding Foreign Interference in 5 Steps."June 2019.

17 Cybersecurity and Infrastructure Security Agency (CISA) "War on Pineapple: Understanding Foreign Interference in 5 Steps."June 2019.

18 Michael Bennet. "Dividing America: How Russia Hacked Social Media and Democracy." July 2019.

Common Themes in IO Targeting Elections

Top Targets of Election Interference: The "Five Questions"

Key to combating mis/disinformation is early identification before it takes off in the public conversation. Disinformation targeting elections, and resulting misinformation, typically falls into one of the five questions of how elections run—the who, what, when, where, and how of the election process.

5 Questions of the Election Process:

Who? *The people who make elections run.*

What? *The machines, systems and ways that we vote.*

When? *The day(s), time, places and deadlines that help us come together to vote.*

Where? *Where we show up to exercise democracy.*

How? *How voting happens.*

As an election official, you can help counter mis/disinformation incidents by ensuring that you have provided clear, well publicized accurate information about each of these questions well in advance of election day. In addition, you can monitor and fact-check content shared online or by your constituents across any of these five categories. These efforts will enable you to identify mis/disinformation early and help you respond to it more effectively.

WHO?

Mis/Disinformation incidents often focus on the people that enable elections to run. This effort may involve impersonating or disparaging elections-related groups or individuals through hacked or fake social media accounts, websites and articles.

The most prominent targets include:

Election officials in your office, or in offices lateral to yours (e.g., county to county) or vertical to yours (e.g., county to state)

Poll workers and other volunteers, such as signature checkers or ballot counters

External staff, such as those who manage key external systems like Motor Voter

Vendors, including companies or individuals

Third party or special interest groups with access to large voter bases

WHAT?

Mis/Disinformation incidents may spread false allegations of disrupted election hardware, software, and infrastructure including vendor-managed systems. This includes allegations of bias, malfunctioning, or hacking.

The most common targets include:

Voter Registration Databases (VRDB)

E-poll books

Vote-casting Devices

Vote Tally Systems

Election Night Reporting Systems (ENR)

Contentious Political Issues

WHEN?

Mis/Disinformation incidents often misrepresent facts about key times and dates for elections. Elections can be catastrophically disrupted if voters do not know when they will occur, when to register to vote, or the times of other key events.

The most common targets include:

When election day is

When polls open and close

When you register to vote

When the deadlines are for early voting or absentee voting

WHERE?	**The most common targets include:**
Mis/Disinformation incidents can disrupt elections by reporting false information about locations involved in the elections process, including for voting, registration, or other events.	Where you vote on election day (or early voting in states that offer it) Where you register to vote Where you return an absentee (or "mail-in") ballot Where you vote on election day (or early voting in states that offer it)

HOW?	**The most common targets include:**
Mis/Disinformation incidents often misrepresent how key election events like voting or registration occur. This may involve suggesting that constituents can vote through a variety of unsanctioned methods (e.g., by Text Message, Twitter, Email).	Voting day processes that can involve mechanisms or procedures to do with functions of elections like mail-In or provisional ballots, Polling place processes, or absentee voting. Voter registration processes like where to register, online or in-person registration or same day registration

Common Disinformation Tactics

Malicious actors can use a wide array of tactics to spread mis or disinformation. This section highlights some of the top tactics bad actors are most likely to use.

False claims about incidents - Bots and trolls spread and amplify reports of false or embellished incidents. Individuals also do this. For example, state actors use state media and state channels, including embassies or ambassadors, to promote narratives around incidents. Individuals active on platforms may also express their own views on claims or incidents they encounter. Hostile actors will seize on messages issued in response to the incident, highlighting inconsistencies, to control the narrative of the incident and prolong public interest. These stories could be completely unsubstantiated or partially based on facts.

Stirring civil discontent - Hostile actors have used two, related, approaches to stir civil discontent:

1. **Direct activity -** Trolls have approached civil society groups to incite the group to conduct provocative and aggressive behavior.

2. **Indirect activity -** Trolls purporting to be followers or supporters of causes spread false, inaccurate, or misleading information targeted at civil society groups to inflame tensions.

Social media advertising - Highly targeted advertisements drawing on personal data available to social media platforms, is used to micro-target specific demographics or groups of voters. Examples of social media advertising include ads leading up to the 2016 election targeting voters in swing states on divisive issues such as second amendment rights and immigration.[19]

Search result manipulation and optimization - Use of techniques to push search results to the top of Google and other search engines. Results that appear higher in search results are significantly more likely to be clicked on and opened by users.[20] Platforms including Google continue to take steps to reduce search result manipulation.[21]

Misrepresentation and defamation - Creation of fake websites, Facebook pages, Twitter accounts to misrepresent the views or outputs of an organization or person. This includes websites and social media posts that detail false voter registration processes, therefore seeking to suppress votes.[22]

19 "How Russian Facebook Ads Divided and Targeted US Voters Before the 2016 Election." WIRED. April 2018. https://www.wired.com/story/russian-facebook-ads-targeted-us-voters-before-2016-election/.

20 "Google Organic CTR History." Advanced Web Ranking. May 2020. https://www.advancedwebranking.com/ctrstudy/

21 "Why keeping spam out of Search is so important." Google. June 2020.https://www.blog.google/products/search/how-we-keep-spam-out-of-search/

22 "Microsoft Foils Russian Security Threat, Seizes Fake Political Websites." SDXCentral. August 2018. https://www.sdxcentral.com/articles/news/microsoft-foils-russian-security-threat-seizes-fake-political-websites/2018/08/.

Memes - Photographs or short videos with captions or other text. These usually aim to be humorous and/or highly emotive, to make them more likely to be shared.[23]

Image source: "The Tactics & Tropes of the Internet Research Agency."

Edited visual content - Photographs and videos that have certain elements altered to make it look like something happened that did not. Videos of this kind are known as 'deep fakes', and, using modern technology, can even make it appear that someone said something they did not.[24]

Image source: The New York Times.

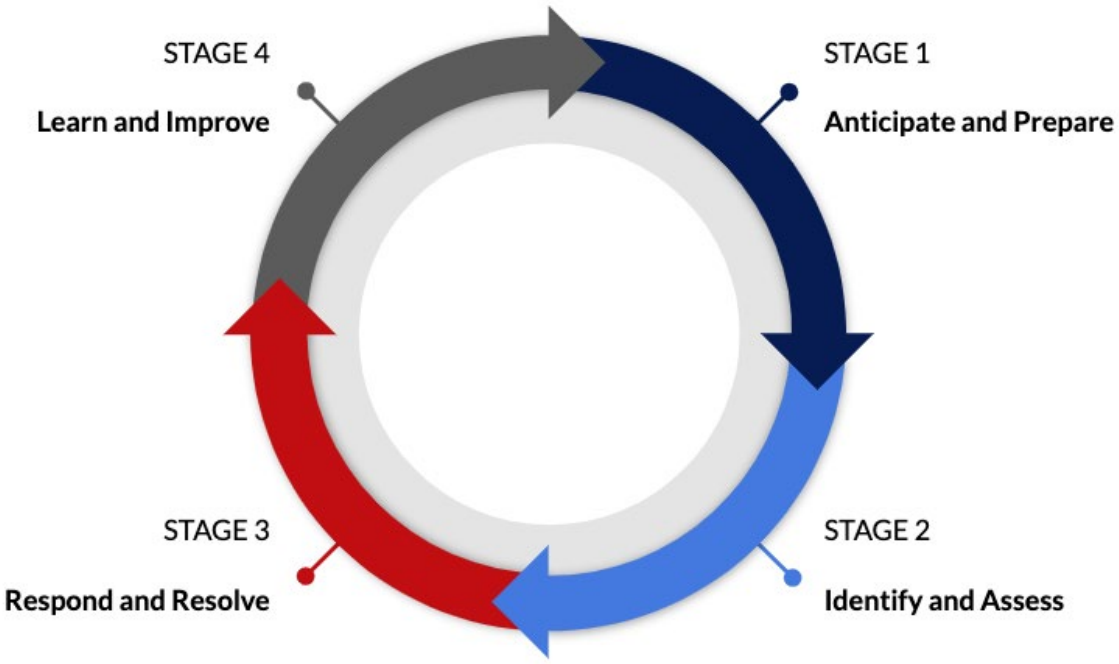
23 New Knowledge. "The Tactics & Tropes of the Internet Research Agency." Renee DiResta, et al. December 18, 2018.

24 New York Times,"We Asked for Examples of Election Misinformation. You Delivered." Kevin Roose. Nov 4, 2018. https://www.nytimes.com/2018/11/04/us/politics/election-misinformation-facebook.html

Steps to Counter Influence Operations

Mis/Disinformation incidents make public education and transparency even more important than it already is in your work to serve voters. Whether you are a small or large jurisdiction, your steps to help an efficient and quick response matter.

Part 2 of D3P's Election Influence Operations Playbook, The Mis/Disinformation Response Plan, focuses on actionable steps to respond to mis and disinformation incidents. In order to respond effectively, we suggest a 4-phased response that targets both the Operations and Incident Communications elements of your team to counter influence operations. This approach follows a cycle: **Anticipate & Prepare, Identify & Assess, Respond & Resolve, Learn & Improve**.



Mis/disinformation occurs before, during, and after elections. Each phase of this process and our baseline response plan will help you and your teams prepare, act, and respond through the continuous nature of these incidents to counter them effectively.

Appendix 1:
101 Overview of Social Media Platforms and Websites

Mis/disinformation content frequently spreads fastest and most effectively via social media and other online platforms. Below is a list with descriptions of some of the most significant platforms and websites on which mis/disinformation can spread. The popularity of these platforms changes rapidly, with new ones emerging and old favorites becoming less widely used.

Facebook: An extensive social network of individuals that can read, react to, and spread mis/disinformation at global scale. With large text and file size allowances, Facebook enables mis/disinformation campaigns to provide significant depth to misleading comments and posts.

- Who uses it: 2.4 billion users from all around the world. 220 million users in the U.S. Users are generally older than those on other platforms, with an average age of ~40.
- Features: Large suite of resources, including one-on-one messaging, public posts to all friends, interest pages, groups, businesses, and paid advertising.

Google: Google is the most widely used search engine worldwide. Relevant news stories appear at the top of Google search results for searches about current events.

- Who uses it: Google handles trillions of searches a year. Users come from all over the world.
- Features: Provides links to websites on the basis of user searches. Summaries of key information can appear alongside search results in knowledge panels or business profiles.

Instagram: Owned by Facebook, it offers a "curated" feed of photos and videos that users scroll through.

- Who uses it: 1 billion monthly active users around the world, with 120 million in the U.S. Users are typically younger, with 70% of users under 35 years old.
- Features: Public photo and video sharing platform with simple scroll-down functionality. Users can also share "stories" that briefly show a series of photos and videos. The 'Reels' feature, released in August 2020, allows accounts to publish short videos that can be viewed by people who are not followers of that account, potentially broadening accounts' reach. IGTV is a standalone video application by Instagram and stories can be viewed and saved with no time limitation.

Reddit: A minimally formatted platform made up of open forums called subreddits, whose subjects can cover any topic and content includes text, links, and images. The high volume of external links shared via Reddit can help a disinformation campaign spread undetected.

- Who uses it: 330 million users with 2.8 million comments a day, and 26.4 million U.S. users.
- Features: As a social sharing site, it is based on a voting system where the most popular content rises to the top, while downvoted content is less visible.

Snapchat: This platform provides an "expiring" photo, video, and/or message to users that can be viewed for a maximum of ten seconds. This format limits the viral potential of mis/disinformation campaigns on Snapchat, but it can still be used to reinforce disinformation spread on other platforms.

- Who uses it: 229 million daily active users, primarily in the U.S. and the E.U. Users are typically younger, with more than 50% of users under 35 years old.
- Features: Filters which alter users' appearance are popular. Businesses and other organizations can pay to display content in a separate Snapchat feed.

TikTok: Launched in 2016, TikTok has quickly risen to global popularity thanks to its short video format. It is owned by Beijing-based ByteDance. Although only 30 million of its users are in the U.S., it is growing here by almost 400% per year, and has frequently been close to the top of the monthly most downloaded apps rankings. At the time of publication, TikTok is facing the possibility of being closed down in the U.S. The company is also fielding offers by U.S. companies to acquire its U.S. operations.

- Who uses it: Over 800 million users worldwide, over half of which are in China. Over 60% of users are under 25.
- Features: Individual videos are restricted to 15 seconds. Lip syncing to songs and dance videos are popular. Videos can be downloaded and shared on other platforms.

Twitter: Provides a social platform that can solicit rapid response and reaction through "likes" and "retweets." Given text limits (140 or 280 characters) and limited video upload sizes, mis/disinformation campaigns on Twitter can be more concise, image, meme, and video-based, and targeted at a specific incident using hashtags ('#') to link related content together. When a topic is 'trending', it means that the hashtag of that topic is being widely used. Hashtags are now widely used across a range of other platforms.

- Who uses it: 166 million daily users, with most usage in U.S., Japan, and the E.U.
- Features: Public micro-blogging platform with each post limited to 280 characters. Videos, images and other web links can be shared.

WhatsApp: A direct messaging application owned by Facebook. It has been used in mis/disinformation campaigns across Asia, Latin America and elsewhere. Because WhatsApp is a closed peer-to-peer network, external parties cannot identify mis/disinformation independently.

- Who uses it: 70 million users in the U.S., and 1.5 billion users overall worldwide, mostly in Europe, Asia, and Latin America.
- Features: Private small-group messaging application, with text and phone call features, as well as short video (c.90 second limit), photo and other file (e.g. documents) sharing.

YouTube: Owned by Google, YouTube is a video sharing platform. Videos hosted on YouTube may be embedded on other sites and shared through other technologies and services.

- Who uses it: Every day, users from all over the world watch over a billion hours of YouTube videos.
- Features: Users can subscribe to the 'channel' of their favorite content creators to receive notifications every time new videos are uploaded. Comments sections under videos enable users to discuss content and share ideas and links.

4chan: This is an imageboard website that divides discussions into threads, each of which is governed by separate guidelines including expiration deadlines of content. The website is seen as a controversial forum that has helped the spread of disinformation.

- Who uses it: 4chan says it has 22 million unique monthly users, and that the majority of its users are young, college-educated males who primarily live in English-speaking countries.
- Features: 4chan preserves complete anonymity of its users. This anonymity can be a volitile factor for purposes of mis and disinformation.

Do you see a way to make this Playbook better?

IO threats are evolving, is there new information we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #IOplaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P