MYTH 1:

PREPARATIONS FOR DISINFORMATION ATTACKS SHOULD TAKE PLACE IN THE IMMEDIATE MONTHS LEADING UP TO AN ELECTION

REALITY:
MYTH 1:

PREPARATIONS FOR DISINFORMATION ATTACKS SHOULD TAKE PLACE IN THE IMMEDIATE MONTHS LEADING UP TO AN ELECTION

REALITY:

MYTH CAUSED BY: MEDIA FRENZY OVER DISINFORMATION CAMPAIGNS IN IMMEDIATE LEAD-UP AND DAY-OF TO ELECTIONS

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
EXAMPLE: WIRED (ELECTION DAY - NOV 6TH 2018)

Alert: Track midterm election day misinformation right here

© AARON P. BERNSTEIN/GETTY IMAGES

ELECTION DAY is a perfect environment for misinformation to spread, whether it's through coordinated campaigns or honest error—or a mix of both. The stakes are high, there's a lot of breaking news, and the US voting system isn't always the most intuitive. Social media didn't create misinformation, but as Emily Dreyfuss wrote last...
Here’s A Running List Of Hoaxes And Misleading Information About The Midterm Elections

Attempts to confuse voters have already started circulating across social media.

BuzzFeed News is tracking and debunking the dubious rumors, memes, and falsehoods related to the midterm elections. If you see something we haven’t covered, get in touch through email (jane.lytvynenko@buzzfeed.com) or Twitter (@handystef). This post will be updated through Election Day 2018.
MYTH 1:

PREPARATIONS FOR DISINFORMATION ATTACKS SHOULD TAKE PLACE IN THE IMMEDIATE MONTHS LEADING UP TO AN ELECTION

REALITY:

PREPARATION IS A 365 DAY ISSUE. ADVERSARIAL GOAL IS TO SOW DISCORD, FEUD HYSTERIA, AND CAUSE POLITICAL CONFUSION

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
MYTH 1:

PREPARATIONS FOR DISINFORMATION ATTACKS SHOULD TAKE PLACE IN THE IMMEDIATE MONTHS LEADING UP TO AN ELECTION

REALITY:

PERMANENT ELECTION TEAMS BEING ESTABLISHED
FBI, DHS task forces to address election security are now permanent

FBI director Christopher Wray called attempts to impact US elections a ‘365-day a year’ issue.
Critical Infrastructure Sectors

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The Elections Infrastructure Information Sharing and Analysis Center (ISAC) was announced Thursday, giving the nation’s 8,800 state and local jurisdictions a dedicated venue to share information about cyberthreats and vulnerabilities specific to election systems and remote security monitoring capabilities.

The Designation of Election Systems as Critical Infrastructure

Prior to the 2016 federal election, a series of cyberattacks occurred on information systems of state and local election jurisdictions. Subsequently, in January 2017 the Department of Homeland Security (DHS) designated the election infrastructure used in federal elections as a component of U.S. critical infrastructure. The designation sparked some initial concerns by state and local election officials about federal encroachment of their prerogatives, but progress has been made in overcoming those concerns and providing assistance to election jurisdictions.

What Led to the Designation?

In August 2016, the Federal Bureau of Investigation (FBI) announced that some state election jurisdictions had been the victims of cyberattacks aimed at infiltrating data from information systems in those jurisdictions. The attacks appeared to be of Russian-government origin. That same month, DHS contacted state election officials to offer cybersecurity assistance for their election infrastructure. Most states accepted the offer. Although the cyberattacks did not appear to affect the integrity of the election infrastructure, some observers began calling for it to be designated as critical infrastructure (CI). On January 6, 2017, the Secretary of Homeland Security announced that designation.

What Is Critical Infrastructure?

Under federal law, CI refers to systems and assets for which “incapacity or destruction would have a debilitating impact on security, national economic security, national chemical and transportation systems. It serves as SSA for several, including the EIS.

The components of the EIS as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results). It does not include infrastructure related to political campaigns.

Does the Designation Permit Federal Regulation of Election Infrastructure?

DHS does not have regulatory authority over EIS. Five other agencies have significant roles with respect to federal elections, but none has claimed regulatory authority over the EIS:

- The Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA, P.L. 107-252), provides a broad range of assistance to states, including development of voluntary technical standards for voting systems, voluntary guidance on implementing HAVA requirements, and research on issues in election administration. It also has statutory authority for administering formula payments to states to assist them in meeting HAVA requirements and improving election administration, including $380 million appropriated in FY2018 in response to security concerns.
The Census Bureau is trying to head off any possible disinformation efforts aimed at disrupting the 2020 count.

It's asking major tech companies and online platforms to help stave off rogue actors.

Disinformation plus Americans' growing distrust of government could result in a staggering undercount.

The results of the once-in-a-decade count determine political representation and distribution of nearly $700 billion in federal funds every year. (While the Census Bureau conducts many surveys based on sampling, the decennial census is the only program to actually count all U.S. residents.)
MYTH 2: 

TRANSPARENCY IN POLITICAL ADS BY PLATFORMS IS EFFECTIVE

REALITY:
MYTH 2: TRANSPARENCY IN POLITICAL ADS BY PLATFORMS IS EFFECTIVE

REALITY: WE ARE STILL A LONG WAY AWAY. MANY LOOPOHLES EXPLOITED BY ADVERSARIES.

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
Facebook’s Ad Archive API is Inadequate

Facebook’s tool meets only two of experts’ five minimum standards. That’s a failing grade.

Facebook pledged in February to release an ad archive API, in order to make political advertising on the platform more transparent. The company finally released this API in late March — and we’ve been doing a review to determine if it is up to snuff.

While we appreciate Facebook following through on its commitment to make the ad archive API public, its execution on the API leaves something to be desired. The European Commission also hinted at this last week in its analysis when it said that “further technical improvements” are necessary.

The fact is, the API doesn’t provide necessary data. And it is designed in ways that hinders the important work of researchers, who inform the public and policymakers about the nature and consequences of misinformation.
**EXAMPLES: FACEBOOK AD ARCHIVE ISSUES**

[1] ×

**Researchers’ guideline:** A functional, open API should have comprehensive political advertising content.

**Facebook’s API:** It’s impossible to determine if Facebook’s API is comprehensive, because it requires you to use keywords to search the database. It does not provide you with all ad data and allow you to filter it down using specific criteria or filters, the way nearly all other online databases do. And since you cannot download data in bulk and ads in the API are not given a unique identifier, Facebook makes it impossible to get a complete picture of all of the ads running on their platform (which is exactly the opposite of what they claim to be doing).

[2] ×

**Researchers’ guideline:** A functional, open API should provide the content of the advertisement and information about targeting criteria.

**Facebook’s API:** The API provides no information on targeting criteria, so researchers have no way to tell the audience that advertisers are paying to reach. The API also doesn’t provide any engagement data (e.g., clicks, likes, and shares), which means researchers cannot see how users interacted with an ad. Targeting and engagement data is important because it lets researchers see what types of users an advertiser is trying to influence, and whether or not their attempts were successful.

[3] ×

**Researchers’ guideline:** A functional, open API should have up-to-date and historical data access.

**Facebook’s API:** Ad data will be available in the archive for seven years, which is actually pretty good. Because the API is new and still hasn’t been properly populated, we cannot yet assess whether it is up-to-date, whether bugs will be fixed, or whether Facebook will support long-term studies.

[4] ×

**Researchers’ guideline:** A functional, open API should be accessible to and shareable with the general public.

**Facebook’s API:** This data is now available as part of Facebook’s standard GraphAPI and governed by Facebook Developers Terms of Service. It is too early to determine what exact constraints this will create for public availability and disclosure of data.

[5] ×

**Researchers’ guideline:** A functional, open API should empower, not limit, research and analysis.

**Facebook’s API:** The current API design puts huge constraints on researchers, rather than allowing them to discover what is really happening on the platform. The limitations in each of these categories, coupled with search rate limits, means it could take researchers months to evaluate ads in a certain region or on a certain topic.
Facebook Political Ad Collector

How Political Advertisers Target You

by Jeremy B. Merrill, Ally J. Levine, Ariana Tobin, Jeff Larson and Julia Angwin.
July 17, 2018. Updated hourly.

To shine a light on targeted political advertising on Facebook, ProPublica built a browser plugin that allows Facebook users to automatically send us the ads that are displayed in their News Feeds, along with their targeting information. Use this database to search for political ads based on who was meant to see them. Methodology | Install the plugin →

<table>
<thead>
<tr>
<th>Trait</th>
<th>Total Political Ads Collected</th>
<th>How Political Ads Target You in city or state, age, custom or “lookalike” audiences</th>
<th>Who’s Helping?</th>
</tr>
</thead>
<tbody>
<tr>
<td>181,364 (total)</td>
<td></td>
<td>22,076 contributors</td>
<td></td>
</tr>
</tbody>
</table>

Or see who is targeting a:

- 65-year-old man living in Washington, D.C. who is conservative
- 45-year-old woman living in California who is liberal
- 18-year-old man living in Wisconsin who is neither liberal nor conservative
- 30-year-old woman living in North Dakota who is conservative

The following ads are the most recent ads submitted to our database. Select traits above to filter based on how they were targeted. Search by keyword →

Seth Moulton
Sponsored · Paid for by Seth Moulton for America · 🅱️
As president, I’m asking all 33 million young Americans to consider civilian national service. And if you invest in our country, we’ll invest in you—through tuition assistance and job training benefits. If you want this message represented on the debate stage, chip in $1 right now!

Kirsten Gillibrand
Sponsored · Paid for by Gillibrand 2020 · 🅱️
The DNC’s debate qualification rules put my chances of guaranteeing my spot in jeopardy. If you want to guarantee that a voice for women’s rights is on the debate stage, I need your help to hit the 85,000-donor goal. Chip in today!
Facebook Moves to Block Ad Transparency Tools — Including Ours

Our tool had let the public see exactly how users were being targeted by advertisers. The social media giant urged us to shut it down last year.

by Jeremy B. Merrill, special to ProPublica, and Ariana Tobin, Jan. 28, 4:29 p.m. EST
EXAMPLES OF LOOPHOLES

“PAID FOR BY A FREEDOM LOVING AMERICAN CITIZEN EXERCISING MY NATURAL LAW RIGHT, PROTECTED BY THE 1ST AMENDMENT AND PROTECTED BY THE 2ND AMENDMENT.”

(SOURCE: JENNIFER WEXTON NY TIMES)
MYTH 3:

 THERE IS CLEAR PUBLIC UNDERSTANDING AND AWARENESS OF HOW DISINFORMATION WORKS IN ELECTIONS.

REALITY:
MYTH 3:

There is clear public understanding and awareness of how disinformation works in elections.

REALITY:

There are several methods of election interference.
MYTH 3:

1. Disinformation
2. Political Ads
3. Sentiment Amplification
4. Identity falsification
5. The theft of emails or documents through hacking or phishing operations, followed by their strategic public release,
6. Hacking operations against state institutions or publicly influential orgs (NGOs, Think tanks)
7. Cyber Disruption
8. Grooming The cultivation of favorable relationships with key public- and private-sector elites.
9. Campaign Financing
10. The use of hard power to intervene in a country’s political developments and democratic process,

SOURCE: EU VS DISINFO APRIL 2019

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
MYTH 3:

Securing Voter Registration

U.S. Electoral Process Infographic (386).

SOURCE: EU VS DISINFO APRIL 2019

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
MYTH 4:

WE MUST START WITH EDUCATION—IT IS ONLY IMPORTANT TO EDUCATE KIDS WITH CRITICAL THINKING

REALITY:

CLARA TSAO | MOZILLA FELLOW | @TWEETCLARITA
MYTH 4:

WE MUST START WITH EDUCATION—IT IS ONLY IMPORTANT TO EDUCATE KIDS WITH CRITICAL THINKING

REALITY:

WE MUST PUT EQUAL EDUCATIONAL FOCUS ON ELECTION OFFICIALS, SENIORS, MARGINALIZED AND MINORITY GROUPS
“11 PERCENT OF USERS OLDER THAN 65 SHARED A HOAX, WHILE JUST 3 PERCENT OF USERS 18 TO 29 DID. FACEBOOK USERS AGES 65 AND OLDER SHARED MORE THAN TWICE AS MANY FAKE NEWS ARTICLES THAN THE NEXT-OLDEST AGE GROUP OF 45 TO 65, AND NEARLY SEVEN TIMES AS MANY FAKE NEWS ARTICLES AS THE YOUNGEST AGE GROUP (18 TO 29).”

(SCIENCE ADVANCE STUDY)
MYTH 5:

POLICY AND CONTENT REPORTING ALONE WILL SOLVE THIS PROBLEM

REALITY:
MYTH 5:

HOW THE AI WAS TRAINED TO HUNT FOR FAKE ACCOUNTS

One of the most important, given the way Facebook’s platform was exploited during the 2016 presidential election, is to try to identify—and shut down—fake accounts. Rosen says the company uses AI to identify and block millions of such accounts every day, usually at the point of creation and before the people behind them are able to use them for any kind of harm. And last month, Rosen adds, the company deployed a new AI technique that has been hunting for fake accounts tied to various financial scams. He says the AI systems have already taken down more than half a million scam accounts.

To do so, Rosen says Facebook trained the AI systems to look for the kinds of signals that would indicate illegitimacy: an account reaching out to many more other accounts than usual; a large volume of activity that seems automated; and activity that doesn’t seem to originate from the geographic area associated with the account.
MYTH 5:

POLICY PRESSURE AND CONTENT REPORTING ALONE WILL SOLVE THIS PROBLEM

REALITY:

- NEED FIX THIS THROUGH A MORE INTENTIONAL PRODUCT FOCUS
- DEVELOPING CLASSIFIERS FOR AUTOMATIC DETECTION TO SOLVE THIS AT SCALE
- TUG OF WAR BETWEEN POLICY AND PRODUCT TEAMS AT PLATFORMS
QUESTIONS

Clara Tsao | Mozilla Fellow | @tweetclarita
clar@mozillafoundation.org