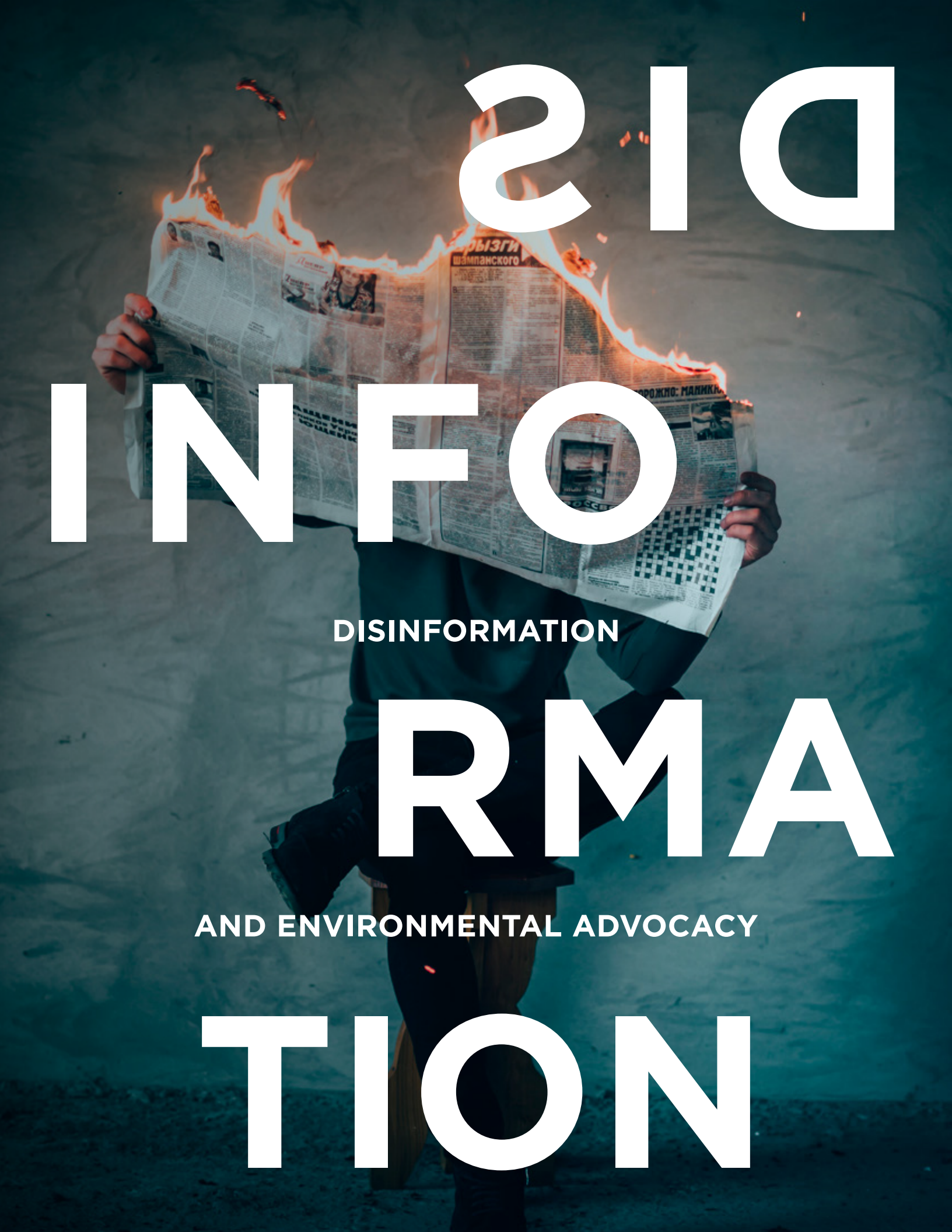

DISINFORMATION
AND ENVIRONMENTAL ADVOCACY

Disinformation and Environmental Advocacy

This report was written by **Melissa Ryan** with assistance from **Michael Khoo** and **Kevynn Gomez** of Friends of the Earth U.S.

Table of Contents

Acknowledgments

"Disinformation and Environmental Advocacy" cites research by:

Data and Society;
Equality Labs;
First Draft News;
HOPE not Hate;
Jan-Willem van Prooijen, André P. M. Krouwel and Thomas V. Pollet, University of Amsterdam;
Dr. Kate Starbird, University of Washington;
Media Matters; New Knowledge AI;
Oxford Internet Institute;
Pen America;
Pew;
Renee DiResta;
Securing Democracy Alliance;
Stop Online Violence Against Women;
Women's Media Center; and
Yochai Benkler, Robert Faris and Hal Roberts, Harvard University.

We are grateful for their work and coverage of these important topics.

We would like to thank the following organizations for their commitment to this topic and their support:

Defenders of Wildlife,
Environmental Defense Fund,
Greenpeace,
National Audubon Society,
Natural Resources Defense Council,
National Wildlife Federation,
Ocean Conservancy,
PAI,
Partnership Project,
Pew Research Center,
Sierra Club,
The Trust for Public Land and
Union of Concerned Scientists.

Executive Summary

Over the last few decades, disinformation in the environmental space has featured companies like Exxon quietly funding global warming denial or pesticide companies covering up health effects. In 2019, disinformation often looks like high-profile political figures like Sebastian Gorka, purposely and continually claiming the Democratic Party will take away Americans' hamburgers as part of a communist Green New Deal agenda, and using right-wing social media echo chambers to turn those lies into truth. The former represents insidious corporate power, the latter: just how blatant and weaponized disinformation has become.

While environmental groups continue to use technology like social media and email well, disinformation-spreading trolls and other bad actors are increasingly many steps ahead, using these same tools to further divide and derail conversations and reduce the power of activists. Multiple extensive studies documented how Americans were manipulated during the 2016 election by bad actors using social media. Disinformation is already a systemic societal problem, not merely a threat of the future, and if the history of power and control is any guide, environmental advocacy will be next.

This report highlights the existence of disinformation in the environmental community. From Russia's Internet Research Agency to harassment of Alexandria Ocasio-Cortez, we point to a few core examples of what environmental disinformation is evolving into in 2019. Disinformation can confuse and deceive your members and targets, misrepresent your message and damage your brand. It's an issue already plaguing other movements — notably immigration reform, racial justice and reproductive freedom.

"Disinformation and Environmental Advocacy" focuses on common disinformation tactics and how these connect (or in some instances, may one day connect) to the environmental community. We discuss studies, social media as an easily exploitable world of tools, right-wing trolls and their Trump connections, as well as the future of disinformation. We also take a look at a current example of manipulation by messaging and technology: the Green New Deal. Further, we offer practical strategies and tactics for organizations to prepare themselves and to be ready for an attack if and when it arrives.

Findings in this report are straightforward. Disinformation is a danger already at work. And as environmental topics, concerns and policies increasingly become linchpins in American society, we believe damaging disinformation incidents will grow in size and damage. Climate change, pollution and the shift to 2020 election policy are all ways environmental topics will continue to gain attention — and therefore become more at-risk from manipulating actors.

In the world of disinformation, cultural values, ideas and images are the primary fodder for bad actors. Gun rights, abortion and immigration have all been exploited by disinformation actors precisely because they are easy visual and cultural targets. There is reason to believe that as disinformation spreads, it will begin to take on topics like environmental policy by using cultural ideas, not policy facts, as a way to bridge the gap.

Protecting sacred lands is an issue already under attack, but when the activists are indigenous people of color, the disinformation takes on a racial tone. When a young member of Congress fights for environmental rights, the disinformation begins to take on a clear undercurrent of misogyny, racism and classism.

Disinformation campaigns through these bigoted filters are about something deeper: a struggle for power by far-right, white, patriarchal actors demanding to control the cultural landscape. These types of disinformation campaigns are, at their core, a cover by which to attack people of color, women, immigrants and other marginalized communities — they are a way to uphold white supremacist ideals.

Disinformation is therefore much more than simply damage to one's brand; it is an attempt to manipulate society into supporting oppressive beliefs.

It is our goal to bring these problems to light before they severely hit the environmental community. Our hope is that we may come together to identify disinformation threats, prepare, and of course, fight back. This problem is too large, and too novel, to handle alone. Through skills building and solidarity, the environmental community can take a stand against these toxic messages that will attempt to disrupt environmental campaigns.

CASE STUDY: Russian Troll Farm Spreads Enviro Disinformation

Russian trolls used climate change in an attempt to divide Americans in 2016 as part of their broader effort to influence American political discourse. The Russian organization Internet Research Agency exploited ideological differences through modern disinformation tactics in the U.S., exacerbating hot-button topics like oil pipelines and the validity of climate change.

The IRA notoriously influenced the 2016 U.S. presidential election, bombarding American social media with content supporting Trump and smearing Democratic candidate Hillary Clinton, and last spring Special Counsel Robert S. Mueller even indicted the troll farm and Russians working for it.

Yet the IRA still exists; their disinformation campaign hasn't ended.

Several federal government committees have investigated the IRA. The House Committee on Science, Space and Technology's investigation focused solely on the IRA's disinformation on energy topics. They found that the IRA infiltrated U.S. social media sites to manipulate Americans' opinions on the energy sector — such as pipelines, climate change and fracking. The end goal? To further sociopolitical divisions in the U.S., and maybe even control which industries we support and which we protest.

From 2015 to 2017, over 4,000 IRA-linked accounts were thought to exist between Twitter, Facebook and Instagram. Russian accounts pushed content in a variety of areas, not just energy and environment; the IRA troll farm worked on elections and racial issues as well. IRA actors fanned the flames of controversial issues with the intention of dividing Americans and influencing their beliefs. IRA accounts were dishonest, pretending to be American activists and social media users. These are all standard tactics of disinformation.

The accounts had blatantly partisan names like "Born Liberal," "_americafirst_" and "Native_Americans_United_." Their Instagram posts (featured) consisted of memes, i.e., photos with text added in, often with highly emotional language. Some posts were published on both Instagram and Facebook. These accounts targeted both sides of the aisle: some accounts posted content that was critical of the Dakota Access Pipeline and supportive of activists protesting it; others criticized environmental activists while supporting the energy industry. This was an attempt to create a divisive, false dichotomy pitting ideological groups against each other.

The Science, Space and Technology Committee believes the goal of these accounts was to influence the American energy industry by persuading social media users, playing upon ideological differences and exacerbating disagreement and tension. "The main focus of the Russian efforts centered on disruption of pipeline development or the advancement of climate change policies targeting fossil fuels," the report states. In some instances, the accounts directed viewers to links for protests and petitions — persuading the viewers to act on their newfound political stances, thereby influencing American policy or economy.

Despite journalists' coverage of the disinformation campaigns and the committees' investigations, the accounts still reached tens of thousands and sometimes hundreds of thousands of Americans. Buzzfeed News states that one account, Native_Americans_United_, had 33,000 followers. Facebook account "Stop A.I. (Stop All Immigrants)" had over six *million* likes.

Instagram
Account Name:
"_americafirst_"; "stand_for_freedom"
Likes: 3,076; 1,774
Comments: 57; 17
Posted: May 8, 2017; April 17, 2017

Facebook
Page Name:
"Born Liberal"
Shares: 5
Likes: 9
Comments: 0
Posted: May 11, 2017

Instagram
Account Name: "bornliberal"
Likes: 1,794
Comments: 96
Posted: May 11, 2017

These Russian actors were largely successful: they received millions of likes, comments and support from Americans and were even able to influence Americans to attend protests and events. Many of these accounts have since been blocked — though others are likely being created anew.

This underscores a disinformation campaign by bad actors feeding off already-controversial environmental topics. The IRA's infiltration of American social media is a prime example of disinformation, not just at large, but also within the niche environmental space. Instead of being a problem from the past, disinformation on such hot-button environmental topics will likely increase, especially as the United States heads toward a 2020 election year where climate and "green topics" remain a focal point.

Research and news reports on the IRA's expansive disinformation run deep, but the underlying message here is clear: Russians have manipulated Americans on topics of environmental import — and will try again if given the chance.

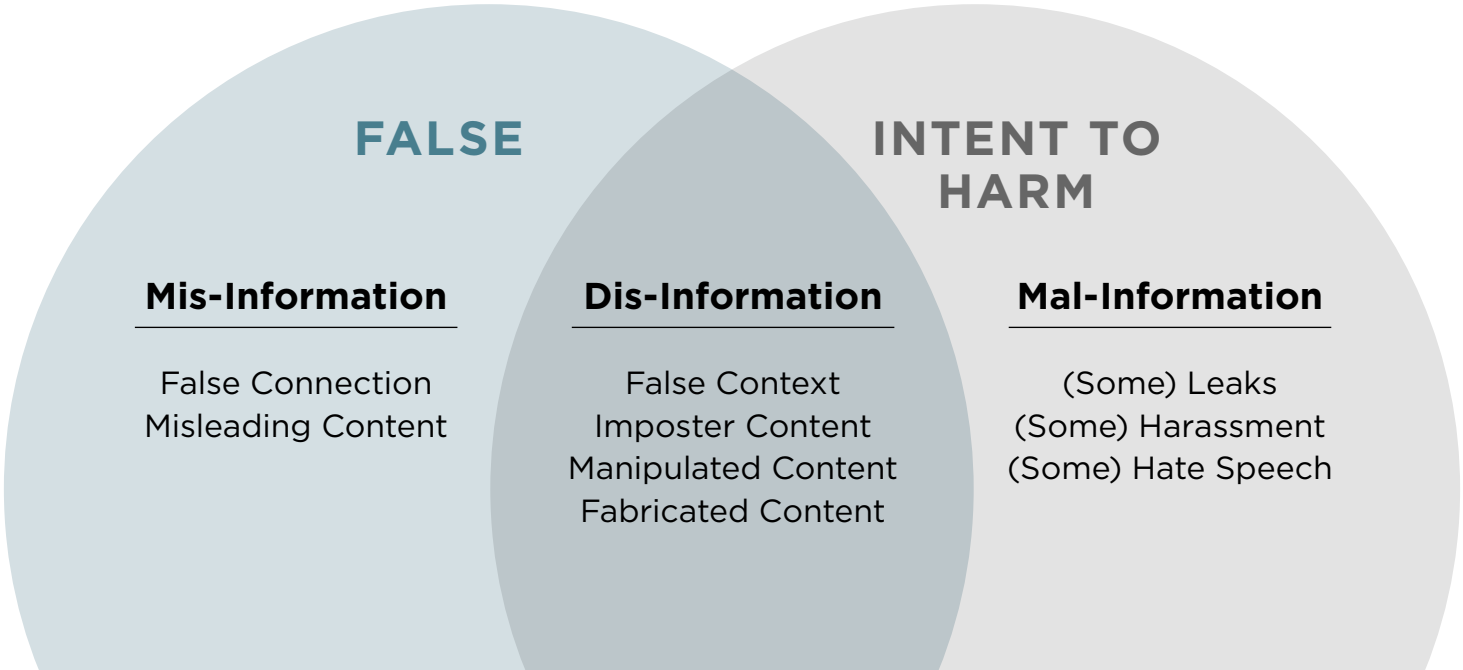
The Basics: Misinformation, Disinformation and Malinformation

Misinformation, defined by Oxford English Dictionary as "false or inaccurate information, especially that which is deliberately intended to deceive," is a helpful term when describing false information seen online. "Fake news," the popular term for misinformation that emerged after the 2016 election, is a problematic term. Whereas most of us would consider fake news to be false news, Donald Trump's base uses the term to describe news they believe is politically biased against them.

The organization First Draft News organizes what they term "information disorder" into three types: misinformation, disinformation and malinformation.

Information disorder

Source: firstdraftnews.com



Whereas misinformation can be accidental, disinformation is always intentional. Malinformation doesn't receive as much attention in the progressive movement as the first two, which is a vulnerability.

Most progressive organizations under attack will face a combination of mis-, dis- and malinformation. And, malinformation will almost certainly be a major part of the attack, as it was with the DNC hacking or ACORN attacks. Malinformation is particularly tricky in that the information released is likely to include at least some information that is true.

First Draft News also includes some hate speech and harassment in their definition of malinformation, but for this manual, we'll use a narrower definition and treat harassment and hate speech as separate tactics.

Further Reading

- Data & Society: Dead Reckoning Navigating Content Moderation After Fake News
- First Draft News: Information disorder: Toward an interdisciplinary framework for research and policy making
- Pacific Standard: How Trump Weaponized 'Fake News' For His Own Political Ends

Who does this and why? "Bad actors" and state-sponsored attacks

The first two questions to address are: who spreads disinformation and why? Disinformation often comes across as a mass of individuals with a particular opinion. But research shows that these people are often backed by institutions — the Russian government in the case of the IRA, or part of a formal grouping of racists, as in the case of right-wing extremism.

One way to explain the use of disinformation is to view it as a tool of power. The power of one group or institution to control another. Racist disinformation is an attempt to maintain its power over an evolving multicultural America. In another way, misogynistic trolling or revenge porn are tools used to fight the rising status of women in America.

As environmental groups challenge the corporate polluters that influence the White House or U.S. Congress, we can reasonably expect they will utilize these same technological tools to fight back to maintain their power.

Strategies and Tactics Used

Tech platforms and tools might change rapidly, but strategies and tactics deployed by bad actors waging information warfare have been fairly consistent over the past several years. Environmental groups need to become familiar with these tactics and be able to recognize them as they develop and expand.

BRIGADING

Know Your Meme defines brigading as "the practice of mobilizing a campaign within an online community to promote or undermine a targeted page, user or belief en masse through the user-voting system." #Release the Memo is probably the best-known example of this. Using Twitter, trolls were able to turn a political stunt from Rep. Devin Nunes into a front-page news story, keeping "release the memo" trending on Twitter and garnering days of media attention as a result.

During the net neutrality fight, a debate that had been occupied by nongovernmental organization activists on one side and telecom interests on the other was suddenly and repeatedly flooded by new "actors." In the public comments to the Federal Communications Commission, hundreds of thousands of fake names were submitted by the pro-telecom side. At an earlier FCC vote, the Twitter feed of #netneutrality was flooded by suspicious accounts posting unintelligible and erroneous information.

DISINFORMATION FLOODING

The goal of disinformation flooding isn't necessarily to change anyone's views, but to create confusion and potentially blunt a campaign's message. Reporters covering these events are forced into wild goose chases to debunk misinformation and social media users will have trouble telling truth from fiction. The disinformation that percolates from these floods often morph into conspiracy theories that remain in the online ether for years.

After any crisis breaking news event, disinformation spreads online like wildfire. During the Parkland mass shooting in 2018, posters on the message boards 4chan and 8chan spread false information about the shooter being linked to a white supremacist militia, the most widely reported of the multiple hoaxes about the massacre found online. After the Sandy Hook shooting, right-wing websites like Infowars spread conspiracies that the victims were "crisis actors" and that the shooting was a liberal plot for gun control.

Dr. Kate Starbird, a professor at the University of Washington, has done research on what she refers to as alternative narratives. She writes: "Over time, we noted that a similar kind of rumor kept showing up, over and over again, after each of the man-made crisis events—a conspiracy theory or 'alternative narrative' of the event that claimed it either didn't happen or that it was perpetrated by someone other than the current suspects." Starbird also highlights the role that botnets play in disseminating alternative narratives.

MALINFORMATION

As defined by First Draft News, malinformation is when "genuine information is shared to cause harm, often by moving private information into the public sphere." The most well-known examples are the leaked Democratic National Committee and John Podesta emails in 2016. The success of malinformation relies on traditional media to cover the released information on the basis that the info is true and now in the public record. The leaked information can result in weeks of negative news stories for the target.

Malinformation can also be a potent tool for sowing division. Leaked documents often contain gossip or discussion of others. It can also be used to add fuel to conspiracy theories online.

ORGANIZED ONLINE HARASSMENT AND DOXXING

Organized online harassment is a staple tactic of bad actors. Online harassment is an array of tactics including trolling, cyberstalking, doxxing, swatting and revenge porn. Most campaigns of organized harassment employ multiple attacks against their targets.

Women and people of color are disproportionately the targets of online harassment. The Women's Media Center Speech Project states that "women, the majority of the targets of some of the most severe forms of online assault – rape videos, extortion, doxing with the intent to harm – experience abuse in multi-dimensional ways and to greater effect." A Pew Research study on online harassment found that "although this harassment can take many forms, some minority groups more frequently encounter harassment that carries racial overtones. This is particularly true for black Americans, a quarter of whom say they have been targeted online due to their race or ethnicity, compared with 10% of Hispanics and 3% of whites."

Anyone is a potential target for online harassment — but those who threaten power structures or are attempting to change culture are the most at risk.

CONSPIRACY MONGERING

Conspiracy theories have long been a fixture of extremists and right-wing media, but have become mainstreamed in the era of Donald Trump, himself a conspiracy theorist. Extremist actors have continually used conspiracy theories as a way to galvanize Trump supporters online.

Conspiracy theory communities online can also serve as a recruitment tactic for trolls. Research suggests that people with extremist political views (left or right) are also likely to believe in conspiracy theories. The QAnon conspiracy theory, currently popular among Trump supporters, is the most prominent current example of this.

GAMING THE REFS AND CONSERVATIVE BIAS

Bad actors have adapted the frame that media is biased against conservatives for the social media era, and the mainstream conservative movement is aiding them.

Right-wing politicians, pundits and campaigns continually claim that Facebook and other tech platforms censor conservative content online. Donald Trump's campaign manager, Brad Parscale, frequently makes this argument.

Media Matters conducted an extensive six-month study into alleged conservative censorship on Facebook and found no evidence that conservative content is being censored on the platform or that it is not reaching a large audience.

Republicans continue to harp on the conservative censorship conspiracy theory as a way to rally their base, and in doing so, they give cover to disinfo disseminators who are constantly fighting suspension and expulsion from the platforms.

Further Reading

- PEN America: Defining "Online Harassment": A Glossary of Terms
- Women's Media Center Speech Project Online Harassment Report
- Dr. Kate Starbird: Information Wars: A Window into the Alternative Media Ecosystem
- Media Matters study debunking claims of conservative bias on Facebook

Social Media is Weaponized

The most important thing to understand about disinformation is that it's deliberate. Social media platforms that gained popularity by innocently sharing photos between friends and family have been weaponized against us. Hostile actors work overtime to amplify their message and make their movement seem larger than it is. They also run targeted harassment campaigns with the goal of silencing others, especially influencers and thought leaders.

These hostile actors — who always existed in political debates — now amplify their reach surreptitiously with technology. Bots are strategically programmed to blitz social media with links to right-wing content at key times. This often happened during the 2016 election at key moments for Trump. The bots' end products were millions of Twitter and Facebook posts carrying links to stories on conservative internet sites such as Breitbart and InfoWars, as well as on the Kremlin-backed RT News and Sputnik.

Twitter botnets are both foreign and domestic. They can be deployed to both amplify content and harass those they disagree with. The result of that amplification is that reporters and media see trending topics and report what people are saying on social media, further amplifying the message and normalizing extreme ideas.

What is weaponization, and am I doing it too?

Communicators and digital organizers often ask how to define the difference between legitimate online organizing and weaponization. It's a good question, especially as trolls continue to adopt traditional organizing and marketing tactics for their own purposes. The following is a proposed framework for determining the difference.

False amplification. **Attempting to make your view or movement seem larger than it is with fake accounts, bots or algorithmic manipulation.**

Spreading disinformation. **Knowingly spreading and amplifying false information online.**

Online harassment. **This includes bullying, doxxing or similar methods with the shared goal of intimidating others into silence.**

Fanning the flames. **Specifically trolling for the purpose of inciting outrage rather than pushing a particular political viewpoint.**

Most environmental groups do not do this, but it's an important question to periodically ask, as solutions are complicated.

For example, technology researcher Camille Francois recently posed the question to progressive activists on how to regulate bots. Should the focus be that they're automated? No — your website uses automation. Should the focus be that such use is not transparent? No. Most organizations' Twitter accounts post using scheduling software too. Or, that they tell lies? Again, no: you don't want the state adjudicating here. Bots, like other weaponized tools, cannot be easily regulated — though conversations on their inherent risks and impact, like Camille started, are necessary.

How platforms are gamed

This next section walks through the most popular social media platforms and how they're exploited to spread disinformation.

FACEBOOK

Facebook's role in the spread of disinformation is multi-faceted. Trolls utilize a network of real and fake profiles, pages and closed groups to create, workshop and disseminate disinformation and other toxic content. Right-wing meme pages outperform all other political content on Facebook. Facebook has been slow to respond to this weaponization, taking down some pages and closed groups but allowing others to remain.

Disinformation also spreads through Facebook ads. Facebook launched a public database of paid ads deemed "political" that ran on the platform. A review of the database found that the platform, in violation of its own policies, allowed ads featuring fake stories and conspiracy theories. Facebook has announced numerous initiatives to combat this, but a former journalist who participated in Facebook's third-party fact checking program called these efforts doomed, even as Facebook ignores calls for specific reforms from technologists working with communities of color.

TWITTER

Twitter is used to amplify messages knowing that a built-in audience of influencers including legacy media will see and absorb them. Memes and messages propagate on Twitter through the use of trolls, botnets and cyborg accounts, over-amplifying them to an audience with influence in media, politics and tech.

Over-amplification can include the brigading of the trending topics section.

Twitter is also the tech platform of choice for online harassment campaigns. Extremists have organized countless harassment campaigns against women, people of color, journalists and

verified users, to name a few. These campaigns are designed to silence influential voices and demobilize them from the public conversation online entirely. Twitter's CEO Jack Dorsey has admitted there is a link between Twitter harassment campaigns and those targeted often being put in real physical danger as a result.

YOUTUBE

YouTube functions as a hub for alternative media outlets, a network to mainstream extremist ideas, a conduit for conspiracy theories to spread and a source of income for several prominent extremist figures.

Right-wing media companies have built their businesses using YouTube's algorithm that autoplays and suggests similar content to users. The three main players are Rebel Media, PragerU and the recently merged CRTV and The Blaze. They monetize using YouTube's ad programs allowing them to sustain these activities over time.

Beyond YouTube's algorithm, right-wing figures use influencer marketing techniques to grow their audiences. A report on YouTube from Data and Society's Rebecca Lewis "presents data from approximately 65 political influencers across 81 channels to identify the 'Alternative Influence Network (AIN)'; an alternative media system that adopts the techniques of brand influencers to build audiences and 'sell' them political ideology."

YouTube has been prominent in the spread of conspiracies, from anti-vaxxers to Sandy Hook truthers. Recently, YouTube announced that it would no longer recommend conspiracy videos to users. But it remains to be seen how effective this change will be on the spread of conspiracies, as Facebook's current efforts to fight "fake news" are failing. Expect conspiracymongers to work overtime attempting to find creative ways to game the algorithms.

INSTAGRAM

Despite being owned by Facebook, Instagram often flies under the radar. Per a report on Russian propaganda from New Knowledge, Instagram was perhaps the most effective tool for IRA trolls looking to spread propaganda as part of Russia's efforts to influence Americans. Trolls also sell products using Instagram's ad program. Instagram also continues to be a platform for notable disinformers and extremists such as Milo Yiannopoulos and Alex Jones, despite the fact that other platforms — including Facebook — have banned or suspended them.

CROWDFUNDING

Digital ad platforms (e.g., search ads, display ads or social media ads), payment processors (e.g., credit card processors or services like PayPal) and crowdfunding platforms (e.g., Kickstarter, Patreon and GoFundMe to name a few) are an often overlooked piece of the tech platform puzzle. YouTube ran ads for hundreds of brands on conspiracy and extremist channels. Bad actors crowdfund their activities on a variety of platforms. Disinformation sites use Paypal to raise money from their misinformation and far-right personalities such as Alex Jones aggressively crowdfund from their audiences to support them.

Further Reading

- Wired: How Bots, Twitter, and Hackers Pushed Trump to the Finish Line
- Media Matters: How the Facebook right-wing propaganda machine works
- Media Matters: Under Facebook's new algorithm, conservative meme pages are outperforming all political news pages
- MisinfoCon: Cyborgs: Where is the line between man and misinformation machine?
- Data & Society: Alternative Influence: Broadcasting the Reactionary Right on YouTube
- Storyz: Google Adsense allows ads on extremist sites
- Media Matters: Multiple fake news sites are using Paypal to raise money, violating its terms of service

Russia and Disinformation

When most Americans think of disinformation from foreign actors, Russia's attempts to influence the 2016 election immediately comes to mind. Russia's attempts to manipulate public opinion in the U.S. began in 2014 and continue to this day. **A 2018 report from New Knowledge**, commissioned by the Senate Intelligence committee, illustrates how Russia gamed our social media platforms to pit Americans against one another. Russian operatives, working from the now notorious Internet Research Agency, preyed on American cultural vulnerabilities and racial tensions to fan the flames — first, to sow division, then, in support of Donald Trump. **African-American voters were targeted** with content meant to stoke racial tensions and with voter suppression ads.

Russia also targeted Americans with malinformation, namely the **DNC hacked emails** and the **Podesta email** leaks. A Russian state-sponsored hacking collective known as **Fancy Bear** was responsible for both of these attacks, which the American political press covered incessantly and gleefully in the weeks leading up to the 2016 election.

Disinformation attempts from Russia are ongoing but they are not the only foreign state actors attempting to manipulate Americans through mis-, dis- and malinformation. Recent news shows Facebook and Twitter's removal of what they term "inauthentic content" targeting Americans **included content originating** from Iran and Venezuela as well as Russia.

Disinformation and counter-terrorism expert Clint Watts **has predicted** that state-sponsored disinformation will become a common tactic if left unchecked, and that other entities seeking power will adopt Russian-style tactics. Watts says, "In the future, Russia and other authoritarians will continue their manipulation, but it will be ordinary candidates and their campaigns, lobbyists, and corporate backers that seek to exploit the manipulative advantages available on social media."

Russian disinformation is just the tip of the iceberg. Other entities and individuals can learn and deploy the strategies and tactics used by Russia and other state actors. Tech platforms are continually behind the curve in fighting the weaponization of their platforms. And troll armies for hire will almost certainly be utilized by state actors and corporations looking to spread disinformation for their own purposes.

Further Reading

Oxford Internet Institute: Computational Propaganda Worldwide

New Knowledge: The Disinformation Report

Stop Online Violence Against Women: Facebook Ads that Targeted Voters Centered on Black American Culture with Voter Suppression as the End Game

Culture Wars

Whether state-sponsored or domestic, trolls that traffic in disinformation are largely uninterested in pushing any specific legislative or policy agenda. In the Trump era, we've seen this with every policy fight from health care repeal to the deeply unpopular tax bill.

That's because cultural content is far more effective as an information warfare tactic. In a recent Media Matters study of memes and images from the most popular right-wing Facebook pages, the content that consistently went viral was either anti-immigration, pro-gun, pro-Trump, veteran clickbait or race baiting. (I suspect if the study was done again in 2019, anti-choice memes would be added to that list.) The only policy position that went viral with the right online were calls for voter suppression laws, and most of that content was explicit about whose right to vote they wanted to suppress.

The emphasis on cultural rather than policy fights might explain why the environmental movement has up until now been largely inoculated from large-scale disinformation campaigns on the same scale that other progressive movements have been forced to deal with.

A recent study from the Oxford Internet Institute Computational Propaganda Project offers some insight into this. They did a yearlong study mapping out the discourse around climate change on Twitter and Facebook and found that:

> **1.** most of the content and commentary shared on both platforms espouses the scientific consensus;
> **2.** the greatest share of content on Twitter (33%) and Facebook (49%) comes from professional news sources;
> **3.** businesses drive a lot of the conversation on Twitter, while civil society content gets more traction on Facebook;
> **4.** audiovisual content like YouTube videos plays an important part in polarizing and conspiracy content;
> **5.** on Facebook, accounts promoting skepticism seem significantly less integrated with the broader community than consensus accounts; and
> **6.** there is little evidence of automated tweeting.

It's tempting to read these findings and breathe a sigh of relief, but there are signs that the far-right are attempting to tie the environmental movement to cultural issues. In this next section, we'll cover emerging cultural issues that the right are exploiting around the Green New Deal and its champion, Rep. Alexandria Ocasio-Cortez.

Alexandria Ocasio-Cortez and Green New Deal Conspiracies

New York's Rep. Alexandria Ocasio-Cortez and her Green New Deal have rapidly become the GOP's new punching bag. Ocasio-Cortez has made waves for her unapologetically progressive politics — and this has led to a wave of lies, attacks, trolls and memes from the right wing.

In an interesting new combination, it appears AOC is being targeted for being a socialist, a woman, a person of color and an environmentalist. This confluence might be creating a dynamic where the furthest right echo chamber is now opposing environmentalism as a way to express its intrinsic racism and misogyny.

Ocasio-Cortez's Twitter account shows classic forms of disinformation at work. Harassment, spreading false and misleading information, false

amplification using bots and even imposter content all appear consistently. Dozens and sometimes hundreds of negative comments follow virtually every post she makes. Users (or bots) share doctored photos and memes to make her look bad.

Attacks on AOC use memes and bullying messages that attempt to discredit her professionalism, intelligence or simply make fun of her appearance. They connect Ocasio-Cortez with communism or Marxism, make her seem ditzy and unknowledgeable or deem her guilty of corruption or illegal acts such as money laundering.

Mainstream news outlets sometimes spread anti-AOC disinformation, such as the now-debunked Fox News claim that Ocasio-Cortez intended to get rid of farting cows. One common troll post in AOC's comments is a right-wing conspiracy video called "The Brains Behind AOC Alexandria Ocasio-Cortez" that claims she is a paid actor and a "puppet congresswoman." Right-wing news outlets, such as Long Room, Infowars and Canada Free Press, give the video free publicity too.

In keeping with disinformation tactics like imposter content, bad actors or bots created a number of fake look-a-like accounts of Alexandria Ocasio-Cortez. With names like "Alexandria Occasional Cortex" and "Alexandria Occasional Cortex fake," the accounts comment, post and like content just as anybody else would, using their accounts as a way to mock the congresswoman and potentially confuse users who don't look too closely at Twitter handles or account info.

Further Reading/Action Items

- Oxford Internet Institute: Climate Change Consensus and Skepticism: Mapping Climate Change Dialogue on Twitter and Facebook
- Quartz: Linguistic data analysis of 3 billion Reddit comments shows the alt-right is getting stronger
- Book: Troll Nation

The Pro-Trump Media Ecosystem

The current state of political media is built around supporting Trump. Just as far-right movements across the globe have coalesced around Trump, so have the activities of trolls spreading disinformation. This ecosystem impacts the traditional media in ways we haven't seen previously, and public relations agencies (corporate and nonprofit clients) are forced to adapt their strategies as well. Understanding this new ecosystem is key.

Here's how the network breaks down:

Message board communities including but not limited to 4chan and 8chan are a breeding ground of white supremacist and misogynist messages and memes, disinformation, conspiracy theories and organized harassment campaigns.

Narrative builders such as false news sites, YouTubers, podcasters and fringe right-wing media sites such as Breitbart amplified these messages to a larger audience.

Dissemination networks operating on popular platforms, mostly Facebook and Twitter, spread messages and ideas to a much larger audience through a combination of automation, false accounts and private groups for organizing.

Traditional right-wing media outlets like Fox News and talk radio broadcast a (usually) sanitized version of this content to their massive audiences once critical mass is reached online.

CASE STUDY:
The 4chan to Fox News to Trump Pipeline

Pro-Trump trolls often take advantage of the traditional media's propensity to mine social media for stories. The thinking seems to be: if it's trending on social media, viewers will care about it.

There are several examples of disinformation and extremist content making its way from 4chan to Fox News (where Trump often further amplifies Fox News programming via his Twitter account). A good example of how this happens can be seen in a debunked myth that there's a white genocide movement in South Africa.

As Vox reports, the white genocide myth actually began as corporate misinformation:

> AfriForum is a lobbying group based in South Africa that advocates for the rights and interests of a segment of the country's white minority known as Afrikaners. Formed in 2006, one of its biggest lobbying efforts in recent years has been aimed at convincing the international community that there is a widespread campaign of race-based killings targeting white farmers in South Africa.
>
> In addition to a huge digital media presence, its leaders travel around the world to meet with prominent politicians and other influential people and promote this horrifying story.

There's just one problem: The story isn't real. There is no evidence of a widespread campaign of violence and murder targeting white farmers in South Africa.

AfriForum used the pro-Trump online ecosystem to spread this untrue story. It became a popular topic on the chan message boards, the subreddit for Donald Trump fans, and with far-right personalities such as Richard Spencer, Lauren Southern and Ann Coulter. Breitbart and Russia Today picked up the story. Fox News' Tucker Carlson covered it on his primetime TV show. Trump tweeted demanding his secretary of state, Mike Pompeo, open an investigation not long after.

The South African myth shows not just how the pro-Trump network functions, but how easily it can be gamed by hostile actors, including corporations, who understand information warfare. Again, given that much of the disinformation the environmental movement currently deals with comes from corporate actors, it's helpful to have a working knowledge of this ecosystem.

Charlie Warzel's article outlining how pro-Trump media respond to a crisis can deepen your understanding of the ecosystem. For a deep dive into how this ecosystem works within the larger political media landscape, I'd recommend the book Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.

Further Reading/Action Items

- New York Times: YouTube, the Great Radicalizer
- Buzzfeed: How The Pro-Trump Media Responds To A Crisis In Just 4 Steps
- Book: Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics

Consultant hyper-partisan news networks (and email leads)

Republican candidates and consultants have embraced hyper-partisan news sites (largely modeled from false news sites) as a political strategy. GOP consultant Dan Backer has turned fake news into a moneymaker for his pro-Trump super PACs by using them to drive email sign-ups and donations. Reilly O'Neal, the CEO of Mustard Seed Media — which consulted on failed Alabama Senate candidate Roy Moore — purchased Big League Politics, a pro-Trump news site known for entertaining conspiracy theories. It seems likely that the site will cover Republican candidates O'Neal is working with favorably, considering his background as a political consultant. A recent study of Republican candidates in 2018 found that they were promoting fake news sites via their personal Facebook pages run by Liftable Media. Three of Liftable Media's websites have spun anti-Islam conspiracy theories.

Harris Media was caught running independent expenditure Facebook ads that were anti-Semitic in Florida. William Gheen, the head of an anti-immigrant political action committee, controls multiple Facebook pages that have repeatedly linked to hyper-partisan and fake news content from a handful of sites. Last election cycle, several GOP candidates paid to use Roger Stone's email list, including Rick Scott and Eric Brakey.

The line between campaign tactics and trolling has blurred to the point where it's difficult to tell where legitimate campaigning ends and trolling begins. Environmental groups can and should continue to call out traditional media when they fail to report political consultant trolling or fail to disclose hyper-partisan news sites they run that might cover their candidate favorably.

CASE STUDY: ACORN in 2009 vs. Sierra Club in 2018

The dismantling of ACORN in 2008 and 2009 is a prescient example of what bad actors spreading disinformation are capable of.

ACORN conspiracies and disinformation about alleged voter fraud began percolating in 2008 and were validated by losing presidential candidate John McCain and his vice presidential nominee Sarah Palin through the end of the 2008 presidential campaign.

Legacy media added fuel to the fire. According to an article in the Huffington Post, "U.S. newspapers published over 1,700 stories on ACORN during October – more than 10 times the average monthly total so far that year. More than three-fourths of these stories were devoted to allegations of "voter fraud."

In 2009, right-wing activist James O'Keefe released a series of undercover videos filmed in ACORN offices via Breitbart that were selectively edited. O'Keefe claimed the videos showed ACORN workers partaking in a variety of illegal activities, all of which would be proven untrue. ACORN was exonerated after criminal investigations in New York and California, but by then it was too late. Congress, despite holding a Democratic majority, had already voted to defund them.

Thanks to a troll campaign that included conspiracy mongering, harassment of staffers, disinformation and malinformation — amplified by legacy media every step of the way — ACORN was no more.

In 2018, the Sierra Club caught and exposed an infiltrator from O'Keefe's organization, Project Veritas. They were able to control the narrative and prevent the release of any potentially damaging information by proactively telling their own story in the Sierra Club magazine:

> [Veritas staff person] White also allegedly approached the campaign of Jon Tester, incumbent Democratic senator from Montana, presenting himself as the fundraising coordinator for the Sierra Club's Angeles Chapter. According to ThinkProgress, "He was so persistent in his requests for time with Tester's campaign staff that the campaign contacted the Sierra Club's national office to ask about him—a short time before the Sierra Club received a tip about his infiltration." That tip came via Windsor, who says it came from a second anonymous source: "I reached out to the Sierra Club and said, 'Hey, I got this tip; see if this is the guy.'"
>
> It was indeed, and White was quickly removed from his volunteer position. (The Club is now implementing new security procedures as a result.) "We assume he was recording everything," says Watland, although he knows of no sensitive conversations that the faux receptionist might have been involved in. California law prohibits most secret recordings. While targeting the Sierra Club would seem to be in line with Project Veritas's modus operandi, Watland and Windsor believe that this time he was using his involvement as a cover for a further infiltration of key political campaigns. "I think what is happening here is that they're doing a bank shot," Windsor says. "They're building up cover to go after candidates. It shows a rising level of sophistication in how they approach their targets."

The Sierra Club's proactive strategy also allowed them to frame any recordings Project Veritas might release. From a ThinkProgress article:

> The Sierra Club doesn't believe White obtained anything embarrassing about the organization or gained access to sensitive information or databases. But Kash emphasized the group is concerned he may have secretly videotaped or recorded conversations with individuals who thought they were having a private conversation. "That's Project Veritas's MO," she said.

ACORN had no template to help them prepare for O'Keefe's malinformation attack, but the Sierra Club's handling of a Project Veritas infiltrator shows how far the progressive movement has come since O'Keefe first appeared on the scene 11 years ago.

That doesn't mean we're out of the woods yet. The most effective troll campaigns isolate the target from their community, and ACORN's final blow came from former allies. Bad actors in 2020 will attempt to sow similar divisions within the broader progressive movement. Legacy media organizations can be counted on to aid their efforts via amplification. The environmental movement can help organizations facing attack by standing together in solidarity against mis-, dis- and malinformation and creating an information-sharing network so that groups see each other's attacks.

Communication Strategies For Nonprofits to Adapt

Benjamin Franklin, talking about fire prevention, said "an ounce of prevention is worth a pound of cure." The same is true for preventing attacks and inoculating the environmental movement from them. As we've laid out, the tools that trolls use might change, but the strategies and tactics for the most part do not. Environmental organizations have the opportunity to get ahead of attacks by assuming they're inevitable, assessing their organization's own vulnerability, gaming out potential threats and creating a decision tree for response ahead of time.

Now that we've outlined the potential problems facing the environmental movement, what can be done to combat them? This next section will walk through crafting an effective comms and digital strategy with an emphasis on preparation. We'll cover assessing threats, training staff, creating a crisis communications plan, as well as some suggestions for collective action.

Assessing Threats

At this point, you might be wondering if there is a way to assess whether an organization should ignore or respond to an attack of trolling or disinformation. If the attack hasn't spread beyond the dark corners of the internet, any organizational response risks amplifying it and reaching mainstream audiences that would otherwise have no idea the attack exists.

Advocacy organizations face a special challenge here. Advocacy groups are always seeking ways to keep their membership engaged, and an attack can be an excellent opportunity for fundraising and list building. The risk lies in elevating information that might not have spread otherwise.

Data and Society's Oxygen of Amplification report is a helpful resource for determining a course of action. The report is written with reporters and newsrooms in mind, but I find the criteria for response work just as well for advocacy organizations.

> **From the report:**
>
> 1. Determine if the story reaches the tipping point (drawing from Claire Wardle's definition, that it extends beyond the interests of the community being discussed)
> 2. Determine if there would be a public health takeaway (i.e. something worth learning) from the debunking; for example, explanations that identify and analyze manipulators' rhetorical strategies, including their use of humor
> 3. Determine if there is a political or social action point (i.e., something worth doing) related to the falsehood itself; for example, editorials that provide media literacy strategies for recognizing and resisting networked manipulation campaigns
> 4. Determine if the risk of entrenching/rewarding the falsehood in some stories is worth dislodging the falsehood in others
>
> If the answer to each of these questions is no, then the story isn't worth reporting at that time. If a story ultimately passes the tipping point and does become appropriate to report (because of clear risks to public safety, because of the underlying media systems the story unearths), reporters should be especially careful to follow established best reporting practices, with particular attention paid to the origins of the information, as well as its broader context— both of which should be discussed transparently in the article itself. Whenever possible, experts in the particular subject area should be recruited to write or consult on editorial pushback, to ensure the clearest and most informed refutations possible.

Environmental organizations will be well-served to use the same criteria when under attack. While no evaluation system is perfect, answering these questions before enacting a plan will help your organization potentially spread damaging dis- or malinformation to a larger audience than otherwise would have seen it.

Train Your Staff

It is essential to train staff to recognize potential threats, to understand the organization's processes when threats occur and to enact the crisis comms plan. There is a limited window of time in which a response can be effective, and the more prepared staff are, the better they'll be able to act with a clear head about the situation at hand. The manual and the accompanying training module can serve as resources for new staff and a refresher course for veteran staffers.

Make a Plan

When your organization is under attack, timing is everything. You have a limited window when you can push back and keep dis- and malinformation from spreading and sticking. It's important to make a plan ahead of time for if this happens. You can't plan for every variable, but you can answer some broad and basic questions ahead of time.

- **Who are your messengers online and off who can help stop the spread, tell your story and show support?**
- **Who are the friendly media outlets and reporters you'll contact to tell your story?**
- **Who will reach out to Facebook, Twitter and Google if content takedowns are necessary due to disinformation?**
- **Who are your trusted decision makers and/or outside advisers in crisis?**
- **Is a streamlined approval process for press statements and digital content necessary? If so, what does that process look like?**

We've included a worksheet as part of this manual to help your organization create a crisis plan of your own.

Outside of crisis planning, fostering a culture of awareness is essential. Social media monitoring needs to be someone's clear and stated responsibility. The amount of monitoring needed varies by organization (and available resources) but can be as simple as having staff search Twitter, Facebook and YouTube each day or as resource-intensive as purchasing a social listening tool.

Digital Security

An organizational commitment to digital security for both the organization's assets and staff's personal accounts is critical. And such work shouldn't fall only to your organization's IT department or security teams. Everyone from campaigners, organizers, communications and membership outreach to finance and administration staff could be targeted.

Staffers are oftentimes not targets on their own but *because* of their work for the organization, making dedication to staff's own security a workplace obligation. Time should be deliberately carved out for taking these matters seriously: organizations can educate staffers through workshops, meetings with IT, standardized rules such as password protection and even ensuring staffers understand the implications behind such threats.

Organizations should keep in mind that some employees may be targeted more than others. Women, people of color and community activists are oftentimes more vulnerable, and companies would do well to protect them accordingly — and in turn — protect the information and materials these staff members have access to. The more prominent and successful your campaigns or campaigners, the more they could become a target of your opposition.

As many organizations have learned the hard way, one simple mistake from an unknowing staffer can become an organizational nightmare. The following guides can help you come up with a plan for your organization as a whole and for individual staff professional and personal accounts.

- **Organizing for Action:** 10 things you and your grassroots organization can do to improve your digital security
- **Equality Labs:** Anti-Doxing Guide For Activists Facing Attacks From The Alt-Right

The Importance of Solidarity

Trolls look to sow division. They win by dividing us against one another. If one environmental organization falls, the others are more vulnerable to future attacks because the strategy has worked. Presenting a united front against attacks is essential. Solidarity with one another makes it more difficult for the attacks to succeed.

Sharing information and best practices will also aid the environmental movement in improving the movement's response to attacks. The Sierra Club was able to employ learned best practices from several groups who have been infiltrated by Project Veritas since ACORN. The sooner others learn about a tactic that trolls are using, the sooner they can inoculate their organizations from facing a similar line of attack.

Action Items

- Read The Oxygen of Amplification Report
- Using the provided worksheet, create a preemptive crisis communications plan for your organization.

Pressuring the Tech Platforms

There's no doubt that negligence by tech platforms (Facebook, Google and Twitter in particular) played a significant role in the current rise of troll armies and their exploitation of the digital ecosystem. The platforms have allowed themselves to be gamed, and until they were pressured via public outcry and congressional hearings, they took little action to curb being abused by bad actors. By allowing bad actors to game tech platforms, the tech companies have also failed to protect the human and civil rights of their consumers who are targeted with misinformation at minimum — or with attacks and threats via organized harassment.

Lack of racial diversity in tech company staff continues to be a core issue that the platforms must address. The teams building products, deploying algorithms and monitoring harmful content don't reflect the diversity of users on their platforms. The lack of cultural competency has given bad actors an advantage because tech companies are slow to recognize when content is inauthentic.

Moving forward, the tech platforms must enact ad policy changes, algorithmic transparency and work with one another across platforms to better fight bad actors. Disinformation is a systemic problem and all too often, individuals and organizations are left to deal with it on their own with no assistance or recourse from the platforms who have allowed it to fester online for years.

Environmental organizations have the opportunity to use their collective power to better pressure the tech platforms on these issues. Collectively, the environmental movement can join efforts to hold platforms accountable for extremism and/or disinfo, sign on to issues like net neutrality, liaise with groups like Free Press and others that oppose mergers of media companies and lend their support to civil rights groups advocating for the safety of users online.

Additional Resources

External Organizations

The following organizations provide original research and other resources related to extremism and online toxicity on their websites.

Center for Humane Technology
Dedicated to reversing the digital attention crisis and realigning technology with humanity's best interests.

Center for Media Justice
Creates media and cultural conditions that strengthen movements for racial justice, economic equity and human rights.

Data & Society
Research institute focused on the social and cultural issues arising from data-centric technological development.

Equality Labs
A South Asian community technology organization dedicated to ending caste apartheid, gender-based violence, Islamophobia and religious intolerance.

First Draft News
Fights mis- and disinformation through fieldwork, research and education.

HOPE not Hate
Uses research, education and public engagement to challenge mistrust and racism.

Media Matters for America
Dedicated to comprehensively monitoring, analyzing and correcting conservative misinformation in the U.S. media.

Oxford Internet Institute
A multidisciplinary research and teaching department of the University of Oxford, dedicated to the social science of the internet.

Political Research Associates
Produces investigative research and analysis on the U.S. right to support social justice advocates and defend human rights.

Southern Poverty Law Center
Dedicated to fighting hate and bigotry and to seeking justice for the most vulnerable members of our society.

Stop Online Violence Against Women
Raises awareness and funding to stop online harassment.