The Media Manipulation Casebook

Code Book

Last updated: October 26, 2020

Version 1.0

Table of Contents

About the Media Manipulation Casebook

The Media Manipulation Casebook (the Casebook) is a research repository consisting of documented attempts to manipulate on- and offline media ecosystems. It is intended for researchers, journalists, policymakers, and other members of civil society to better understand how sociotechnical information ecosystems can be gamed and manipulated and the outcomes of such actions. It is led by Dr. Joan Donovan and developed and maintained by the Technology and Social Change Project at the Harvard Kennedy School Shorenstein Center for Media, Politics, and Public Policy.

Each case study is coded according to a set of predefined variables and includes a chronological description of the campaign in question using the Media Manipulation Life Cycle model.

The Casebook is still in its expansion phase and welcomes collaboration. For further inquiry, please contact us at manipulation@hks.harvard.edu.

What is Media Manipulation?

We define media manipulation as a process where actors leverage specific conditions or features within an information ecosystem in an attempt to generate public attention and influence public discourse through deceptive, creative, or unfair means. Media is a reference to *artifacts of communication* and not simply a description of news. Although much has been written about the harmful effects of media manipulation and is often attributed or linked to so-called “bad actors,” it is not inherently good or bad. Activists, constrained by heavy censorship in traditional media, for example, may rely on media manipulation in the digital space to circumvent such information controls. However, violent extremists may likewise use the same platforms and tactics to mainstream hateful or dangerous speech. Furthermore, media manipulation is a broad term in that it can be used to define a variety of other terms, such as disinformation, information operations, or influence operations. This is intentional as it allows for a wider variety of cases to be analyzed.

Note that we differentiate media manipulation from media control, which occurs at the top-level by the state and private sector. Media control would instead refer to activity like ISP-level content blocking, government censorship agencies, media ownership, or distribution and licensing regimes.

Selection Criteria

The Casebook aims to provide users with a wide range of cases from around the world that illustrate how specific conditions and features of technology and society can be used to manipulate the information ecosystem with the goal of generating wider press coverage for issues or events that would otherwise go uncovered or to create a false perception of an issue. With this in mind, cases are selected based on three main criteria: their *novelty* of tactics and strategies; the *scale* of the operation and its resulting outcomes and institutional responses; and whether there is enough high-quality *empirical evidence*. To identify whether or not a case should be included we ask the following questions:

Novelty

Goal: To increase diversity of information within the Casebook

- Does this case expand the diversity of cases with regard to strategies and tactics?
- Does this case introduce a new tactical mix in executing a strategy?
- Are the social and technical vulnerabilities being exploited in new or different ways?
- Are the targets or campaign operators or participants involved in the case novel?
- Did the campaign operators or participants adjust their tactics in response to institutional actions (ex. user ban, content removal, account suspension)?

Scale

Goal: To include cases with observable outcomes and reach

- Does this case stand out because of the scale of media coverage?
- Does this case stand out because of high engagement (ex. retweets, comments, likes)?
- Does this case span multiple platforms?
- Did this case invoke institutional response (ex. political response, civil society response, change in platform governance)?

Evidence

Goal: To ensure cases are backed by high-quality sources and multiple indicators

- Is there enough evidence to support analyses of the tactics and strategies employed?
- Are the secondary sources reliable or drawn from high-quality investigations? (ex. academic research or credible investigative reporting)
- Is the data collection and analysis repeatable by other researchers?

Contributors

Cases are researched, written, and coded by members of the Technology and Social Change Project at the Harvard Kennedy School's Shorenstein Center on Media, Politics, and Public Policy. In addition, researchers and scholars from a wide range of experiences and backgrounds, including the fields of sociology, political science, and science and technology studies, have also contributed to the Casebook.

The Casebook is still in its expansion phase and welcomes future contribution and collaboration. For further inquiry, please contact us at manipulation@hks.harvard.edu.

Cautionary notes and limitations

Firstly, media manipulation campaigns are difficult to detect, trace, and attribute, due largely to their ephemeral and covert nature of their planning and execution. Depending on the availability of evidence, some stages will be thinner in description than others. This does not imply there was no activity in that stage, but rather there was no credible evidence available. For example, Stage 1, which documents campaign planning, is often conducted in private. Researchers who primarily rely on open source means of gathering data may therefore be unable to ascertain what actually happened during this period. Similarly, some cases' variables will be coded with "Unclear" where there is not enough evidence. For example, attribution, which is notoriously difficult to pinpoint, will often be coded as "Unclear," implying there is not enough evidence to ascertain with a high-level of confidence who the operators of a campaign are.

Secondly, the casebook is neither an exhaustive nor representative collection of media manipulation and disinformation. Therefore, statistical analyses that take the case as the unit of analysis may not be robust to selection biases. Analyses that attempt to extrapolate trends or quantify elements or features of media manipulation are not advised.

Lastly, as with many cases of media manipulation, new and emerging evidence may change a case's analysis and findings. Any errors should be brought to our attention at manipulation@hks.harvard.edu and will be greatly appreciated. Changes made to a case will be identified with a note explaining why and the date of the change.

Methodology and Theory

Research methods

The means for documenting case studies require a variety of methods in order to establish a chronological account of a campaign, the tactics and strategies employed, the actors involved, and the outcomes. As such, a variety of indicators from different sources (ex. commercial threat reporting, platform reporting, independent research, investigative journalism, website scraping, etc.) is used to triangulate the findings. In addition, each case study varies in the methods used to detect and document the operations, depending on the availability of evidence. Methods may therefore include a mix of quantitative content analysis, network mapping, and ethnographic studies. Where original research and analysis was undertaken, source material is presented and cited, if practicable.

Examples of evidence include:

- Screenshots (ex. JPG, PNG)
- Archived links (ex. Web Archive, Archive.is, Perma.cc, Local HTML Archives)
- Graphs and charts (ex. Graphml files, Gephi files and images, Tableau files)
- Larger datasets (ex. API-drawn data, Factiva or Lexis Nexis exports, other scraped platform data)
- Internet infrastructure (ex. WHOIS information, IP addresses)
- Digital forensics (ex. Malware analysis)
- Credible and well-researched external sources (ex. investigative journalism, peer-reviewed article, research paper)

Coding process

The variables and values used to code each case are emergent from the existing cases and have been developed after multiple rounds of review. They were determined by identifying the most salient traits that are also applicable to all the cases. These codes function as a way to organize and filter case studies based on a common feature while offering comparability and nuance across the different cases.

Each case goes through a minimum of two rounds of coding to ensure each code corresponds to the evidence and text in the description of the life cycle. The initial round is conducted by the primary author of the case, followed by a member of the TaSC team. Any discrepancies in codes are discussed after between the two coders. If there are still any outstanding discrepancies, a third round of coding by a different member of the TaSC team is conducted, and any differences resolved between all three coders.

To view all the variables and values used, see the **Variables** section below.

The media manipulation life cycle

The media manipulation life cycle (MMLC) forms the basis of the Casebook. Patterned after data life cycle models that describe how data should be gathered and used,[1] the MMLC model was developed to give a common framework for journalists, researchers, technologists, and members of civil society to understand the origins and impacts of disinformation and its relation to the wider information ecosystem.[2] It is the product of three years of digital ethnography and field research by Dr. Donovan and her team on how journalists, civil society groups, and technologists grapple with media manipulation and disinformation campaigns.[3] Situated in the emerging field of Critical Internet Studies,[4] this research methodology combines social science and data science to create a new framework for studying sociotechnical systems and their vulnerabilities.[5]

Each case is written according to the five stages defined in the MMLC (details below), allowing researchers to analyze the order, scale and scope of the campaign in question, as well as the actors involved, platforms used, vulnerabilities (both social and technical) exploited, and outcomes. This semi-structured format allows for comparability across cases while providing any necessary context and nuance.

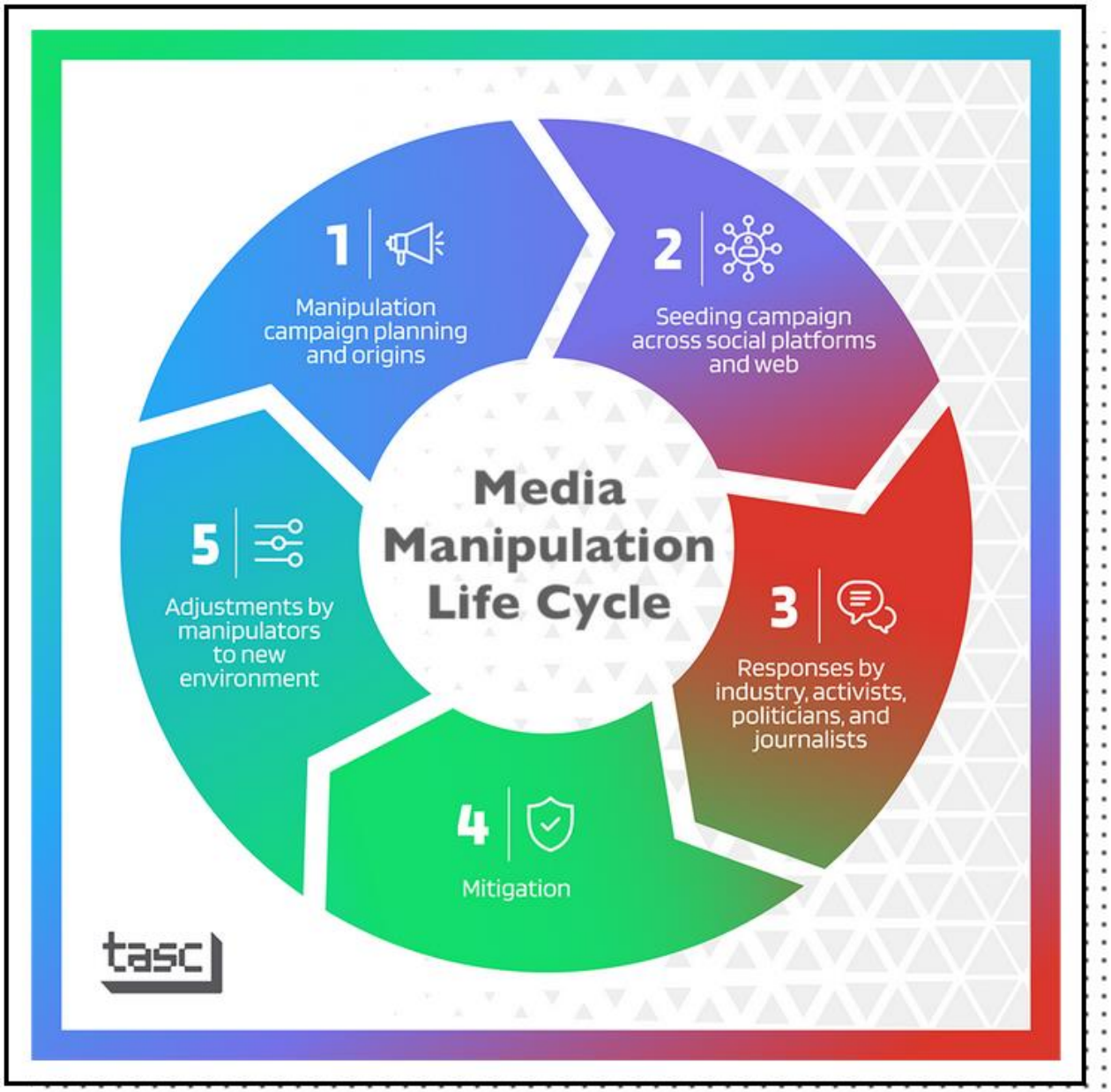
[1] Joan Donovan, "The Lifecycle of Media Manipulation," in *Verification Handbook for Disinformation and Media Manipulation*, ed. Craig Silverman (European Journalism Centre, 2020), https://datajournalism.com/read/handbook/verification-3/investigating-disinformation-and-media-manipulation/the-lifecycle-of-media-manipulation.

[2] Donovan, "The Life Cycle of Media Manipulation."

[3] Joan Donovan and danah boyd, "Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem," *American Behavioral Scientist* (September 29, 2019), https://doi.org/10.1177/0002764219878229.

[4] Amelia Acker and Joan Donovan, "Data Craft: A Theory/Methods Package for Critical Internet Studies," *Information, Communication & Society* 22, no. 11 (September 19, 2019): 1590–1609, https://doi.org/10.1080/1369118X.2019.1645194.

[5] Matt Goerzen, Elizabeth Anne Watkins, and Gabrielle Lim, "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework," in *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI)* (Santa Clara, CA, 2019), https://www.usenix.org/conference/foci19/presentation/goerzen.



Stages of the Media Manipulation Life Cycle

Stage 1: Manipulation campaign planning and origins

Stage 1 documents the campaign planning process and its origins. Depending on the availability of source materials and evidence, this stage would typically describe the platforms and technologies used by campaign operators to plan and coordinate, as well as the social and technical circumstances that facilitated the campaign's genesis. This may include evidence from private and semi-private chat applications (ex. WhatsApp or Telegram), less popular platforms (ex. Discord, 4chan, other message boards), and more mainstream platforms (ex. Twitter or Facebook). Due to the clandestine nature of campaign planning, it is not always feasible, ethical, or legal for researchers to obtain such evidence. However, when it is possible, available evidence that elucidates the campaign planning stage should be included.

Stage 2: Seeding the campaign across social platforms and web

Stage 2 documents the tactics and relevant technologies used to execute the campaign. It details the dissemination and propagation of content relevant to the operation. Typically, this stage involves the execution of campaign plans, when narratives, slogans, images, videos, or other materials are strategically spread on fringe news websites, social media, or video broadcasting platforms. Campaign participants will attempt to dominate conversations on platforms where they believe they can reach a target audience. This can sometimes be on a single platform, such as the closed environment of WhatsApp, in Facebook pages, a particular Twitter hashtag, or across the open web through the strategic use of keywords. The rationale is often to reach as many individuals as possible so as to achieve a critical mass in conversation that will lead to a campaign becoming newsworthy, result in a false perception of massive public concern, sway public opinion, recruit followers, or a number of other off- and online responses.

Stage 3: Responses by industry, activists, politicians, and journalists

After content has been seeded, the campaign moves on to Stage 3, which documents how institutional actors (ex. civil society organizations, politicians, political parties, mainstream media outlets) amplify, adopt, or extend the campaign. The third stage of the operation is usually a turning point indicating whether the campaign was effective in gaining attention through amplification or if led to an observable outcome. Responses may include public statements by representatives from social media platforms, activist campaigns drawing attention to malicious behavior by campaign participants, official political statements, critical reporting in the mainstream press, or political adoption of an idea or narrative pushed by the campaign.

Stage 4: Mitigation

The fourth stage of a manipulation campaign documents actions by tech companies, government, journalists, or civil society to mitigate the spread of a campaign's content and messaging and its effects. This may include actions from civil society (ex. debunking and research), technology companies (ex. user ban, account deletion, content removal), media

organizations (ex. fact-checking and investigative reporting), or the government (ex. draft bills, regulatory changes, take down orders).

Stage 5: Adjustments by manipulators to new environment

The fifth stage of a manipulation campaign involves how the operators and campaign participants adapt according to mitigation efforts described in Stage 4 and the resulting changes in the information ecosystem. While certain content may be banned, or accounts spreading disinformation removed, manipulators will often find ways to circumvent these changes, including by creating new accounts, adapting coded language, altering audio/visual material, and iterating on narratives already identified as objectionable by platforms.

Note that while there may be no evidence of tactical or strategic adaptation, that does not imply the operators did not adapt. Media manipulation campaigns are often covert and as such the operators may have evolved to become better at hiding their tracks. However, if Stage 5 includes successful tactical adaptation or redeployment, a new cycle may begin (i.e. Stage 5 actions turn into Stage 1).

Variables

The following variables and values are used to code each case study. They are emergent from the cases and determined after multiple rounds of review. As new cases are included in the Casebook, the variables and values may change. In this case a new version of the Codebook will be released, and any changes noted.

Case Name

Type: Text

Descriptive case title.

Region

Type: Text

The geographical location where the campaign was most likely carried out based on the evidence available regarding the campaign's origins, participants, or audience. If evidence is inconclusive or unavailable, "Unclear" may be used.

Date

Type: Numerical

Date or date range the campaign was carried out based on available evidence.

Strategy

Type: Categorical (multiple selection allowed)

The plan of action or series of actions designed to achieve an overall goal as observed by the available evidence. Multiple selection is allowed as there may be several strategies in play or working in tandem with one another.

Trading up the chain - Gaining exposure by placing information or disinformation artifacts in locations that will be taken up and amplified by other systems, individuals, or publications. Typically, information may be introduced on smaller blogs or social media before being reported by mainstream media outlets or politicians and other influential individuals.

Targeted harassment - Coordinated and organized online harassment of an individual or groups of individuals to threaten, censor, or upset them or to disrupt their operations or behavior.

Muddy the waters - Distribution of conflicting information to cloud public perception of an individual, group or topic, making the target subject more complex or confusing.

Butterfly attack - Butterfly attacks occur when imposters mimic the patterns of behavior of a social group (usually a group that has to fight for representation). Imposters pretend to be part of the group in order to insert divisive rhetoric and disinformation into popular online conversation or within the information networks used by these groups. Distinct from astroturfing, which tries to falsify grassroots support for an issue, butterfly attacks are designed to infiltrate existing communities, media campaigns, or hashtags to disrupt their operations and discredit the group by sowing divisive, inflammatory, or confusing information.

Coined by Patrick Ryan to describe a series of manipulation campaigns he claims to have orchestrated in 2013, the term butterfly attack is inspired by the mimicry behavior of certain species of butterflies, who impersonate the fluttering patterns of other species to confuse predators.[6]

Astroturfing - Astroturfing occurs when campaign operators attempt to create the false perception of grassroots support for an issue by concealing their identities and using other deceptive practices, like hiding the origins of information being disseminated or artificially inflating engagement metrics.

Gaming an algorithm - Attempting to manipulate an algorithm in order to gain attention. This may include tactics that elevate content into a platform's trending list, being recommended to other users, or placing in the top ten of a search engine's results.

Meme war - The intentional propagation of political memes on social media for the purpose of political persuasion, community building, or to strategically spread narratives and other messaging crucial to a media manipulation campaign.

Unclear strategy - There is no discernible strategy based on the available evidence.

Tactics

Type: Categorical (multiple selection allowed)

Actions employed in service of the strategy as observed by the available evidence.

[6] Patrick Ryan, "The Butterfly War," October 13, 2017, https://cultstate.com/2017/10/13/The-Butterfly-War/.

Viral sloganeering - Repackaging of provocative, revolutionary or reactionary talking points into a short, catchy, and memorable format for social media and press amplification.

Trolling - Engaging in inflammatory, divisive, or distracting behavior in an online community with the goal of provoking readers or viewers into an emotional, often negative, response (ex. anger, outrage, offense).

Bots - Social media accounts that are automated and deployed for deceptive purposes, such as artificially amplifying a message, to game a trending or recommendation algorithm, or inflate an account's engagement metrics. These accounts are typically centrally controlled or at least in coordination with each other.

Swarming - When loosely organized online groups come together for specific objectives or campaigns.

Forgery - The creation of a fake document with intent to deceive via distribution.

Leak - The unauthorized release of sensitive materials or documents.

Evidence collage - Compiling information from multiple sources into a single, shareable document, usually as an image, to persuade or convince a target audience.

Recontextualized media - Media (image, video, audio) that has been taken out of its original context and reframed for an entirely different purpose or narrative frame.

Cheap Fake - The use of conventional editing techniques like speeding, slowing, or cutting, footage or images to create a false impression of an individual or an event.

Keyword squatting - The strategic domination of unique or under-used keywords on a social media platform or search engine that will return search results and content in favor of the campaign operators' goals.

Impersonation - Pretending to be another person or member of a social identity group, either by mimicking their behavior or creating a falsified online presence.

Misinfographic - Infographics with false or misleading information. In some cases, they may also be classified as a forgery when they borrow an existing organization's brand aesthetics and logo in order to make it seem as if the content was coming from the organization.

Typosquatting - The intentional registration of a domain name that incorporates typographical variants of the target domain name in order to deceive visitors. This may involve misspelling a

domain or using a different top-level domain. Typosquatting is a form of cybersquatting, or an attempt to mislead users by fraudulently posing under someone else's brand or copyright.

Memes - Memes, a term coined by Richard Dawkins (1976), are “units of culture” that spread through the diffusion of ideas. Memes are particularly salient online because the internet crystallizes them as artifacts of communication and accelerates their distribution through subcultures. Within media manipulation they typically take on the form of images, gifs, or videos.

Phishing - Fraudulently posing as a trustworthy entity in a malicious attempt to access confidential information such as usernames, passwords and credit card details, usually by the means of email.

Distributed amplification - A call to participants to rapidly and widely spread campaign materials, including propaganda or disinformation.

Network terrain

Type: Categorical (multiple selection allowed)

The digital platforms and technologies used to carry out the campaign.

4chan - 4chan.org

8chan - 8ch.net. Rebranded as 8kun since November 2019.

Twitter - twitter.com

Reddit - reddit.com

Facebook - facebook.com

Instagram - instagram.com

YouTube - youtube.com

Gab - gab.com

Google - google.* Includes all other top-level domains owned by Google (ex. Google.ca, google.com, google.co.uk).

Vimeo - vimeo.com

Discord - discord.com (includes web app, desktop app, and other means of use)

Media outlets - Independent and mainstream media outlets.

Blogs - Self-published websites or web pages, with no editorial oversight, that are usually run by an individual or small group and are regularly updated with new content.

Open editorial platforms - Platforms that have both an editorial arm and a self-publishing arm for users to publish and post their own articles and other content. Examples include Medium and Buzzfeed Community.

Vulnerabilities

Type: Categorical (multiple selection allowed)

The social and technical conditions being exploited by the campaign.

Wedge issue - Political or social issues that are divisive in nature and divide social groups. They typically split along partisan lines and are often presented as binary positions – for or against. Politicians, political influencers, and those running for office will often amplify these wedges in popular discourse, in mainstream press, and on social media.

Prejudice - A bias that can result in an injury or detriment to another individual's legal rights or claims, wellbeing, or participation in society. Such preconceived judgements are not informed by facts and often target an individual or group based on race, religion, sexual orientation, age, class, or other demographic identifier.

Active crisis - A period of time when the normal state of affairs is interrupted by unforeseen events that are troubling and potentially dangerous. Active crises trigger confusion and require urgent action and immediate attention. Due to the increased media attention and importance of any decisions made during this time, active crises are vulnerable to being exploited by media manipulation.

Breaking news event - Periods of heightened attention to current events of local, national, or international importance in mass media and on social media. During these moments of mass attention, legitimate information and misinformation may be indistinguishable until facts are established and vetted by official bodies. This period of confusion creates opportunities to sow confusion, target individuals, or shape certain narratives.

Public directory - Publicly available information pertaining to individuals, organizations, companies, or any other entity that has been aggregated into an accessible, searchable, and organized format.

Election period - Refers to the time leading up to an election when candidates have begun campaigning. Depending on the country, there may be legal limits to what constitutes a campaign period.

Lax security practices - A lax security practice is anything that makes the user more vulnerable to security attacks or scams, like phishing. An example of a lax security practice is having a password that can be guessed easily or is repeated across multiple accounts.

Data void - Coined and theorized by Michael Golebiewski and danah boyd (2018), this refers to unique topics or terms that result in minimal, low quality, or manipulative information from search engine queries. Data voids are social or technical securities risks depending on the subject matter of the query.

Attribution

Type: Categorical (multiple selection allowed)

The individuals or groups responsible for planning, carrying out, or participating in the campaign based on the available evidence.

Prankster - Individuals who engage in activity designed to elicit a reaction from a target purely for fun or mischief.

Networked faction - Tacit coalitions or groups of people who share some, but not all, political positions, primarily congregate online (though not exclusively), and often come together as a swarm to act in unison as a political force. Networked factions maintain these coalitions using shared phrases, hashtags, memes, or similar media. These factions can form and dissolve according to the political context.

Extremists (right wing) - Groups or individuals that espouse right-leaning radical or violent positions, often associated with organized white supremacy or other prejudice-driven ideologies.

Partisans - A strong supporter or committed member of a party, cause, or person.

Influencers - Visible pundits, journalists, or public figures who drive conversation around particular topics in broadcast media and online networks.

Conspiracists - Individuals or groups that actively propagate unfounded or unverified narratives and frames. This often includes speculation, unsubstantiated claims, and explanations predicated on secretive and powerful actors scheming with malicious intent.

Unclear attribution - Attribution, whether referring to the campaign planners or participants, is unclear based on available evidence.

Targets

Type: Categorical (multiple selection allowed)

The individual or group the campaign intended to discredit, disrupt, criticize, or frame in a negative light based on available evidence.

Political party - A group of people sharing similar ideology or political positions who participate in elections by fielding candidates that will then carry out their goals and policies.

Social identity group - Groups defined by some social, physical, or mental characteristics. Examples include race, ethnicity, gender, social class, sexual orientation, or religious beliefs.

Politician - A person engaged in party politics or occupying public office.

Activist group - Individuals or groups that campaign for social, political, or legal change. They may be formally organized (ex. registered non-governmental organization) or loosely affiliated (ex. advocacy networks).

Individual - A single person.

Scientific and medical community - Individuals or groups involved in scientific research, medicine, or healthcare.

Observable outcomes

Type: Categorical (multiple selection allowed)

The results (intended or unintended) of the campaign as observed by available evidence.

Media exposure - Coverage and reporting by journalists in popular or mainstream media.

Political adoption - When a political party or politician adopts or co-opts a phrase, term, or idea for politically motivated purposes.

Recognition by target - When a target of a media manipulation or disinformation campaign acknowledges and responds to the campaign's activities or the operators.

Harassment - Targeted and repeated behavior towards an individual or group of people that causes mental, physical or emotional distress. Harassment includes but is not limited to unwanted threats, insults, touching or offensive language.

Dox - The act of publishing on the internet private or identifying information about a specific individual against their wishes and usually with malicious intent (i.e. retaliation, punishment).

Misidentification - Erroneously identifying an individual as someone else, intentionally or accidentally.

Mitigation

Type: Categorical (multiple selection allowed)

Attempts, measures, and other actions taken by the private sector, government, media organizations, and civil society in an attempt to contain or prevent the continuation of a campaign.

Critical press - Press coverage that is critical of a manipulation campaign. Articles may debunk false claims or investigate the origins and motivations of a campaign.

Civil society response - Civil society response refers to actions taken by members or groups of civil society in an attempt to mitigate a campaign's harms or spread. We define civil society as groups or organizations engaged in advocating for certain issues, educating the wider public, holding the government accountable, or promoting civil and human rights. They may be formally organized or loosely coordinated and include non-governmental organizations (NGOs), community groups, labor unions, educational organizations, faith-based organizations, professional associations, non-profit think tanks, and foundations.

Debunking - Exposing and correcting false or misleading claims. Debunking includes fact-checking efforts, research and investigation, exposés, and other critical content or actions that attempt to correct the false claims.

Account suspension - Accounts that have been suspended by a platform or company, preventing the user from log in or using the account.

Content removal - Content removal is the act of platforms taking down specific pieces of content, like videos, tweets, posts, etc. The platform's terms of service are often a guideline for what can be removed, though these are rarely enforced uniformly or consistently.

Deplatforming - The removal of individuals or groups from a platform, preventing them from using the platform’s services even if they try to create new accounts.

Flagging - Reporting harmful or offensive content to an online social media platform or company. Content can be flagged by an algorithm, content moderator, or another user.

Research and investigation - Individual or coordinated group efforts to establish the origins and impact of a manipulation campaign.

Civil/Private lawsuit - A legal proceeding by a private party or parties against another in a civil court of law that seeks remedy for a wrongdoing or harm.

Counterspeech - A tactic used for countering hate speech and misinformation by advancing alternative narratives and challenging information.

De-indexing - Removing a link or other content from search results. The content or website in question is still available but will not be included in a search engine's, website's, or platform's results.

Media blackout - Self-imposed or state mandated censorship of a certain news topic.

Blocking - User-instigated action that prevents another account from interacting with them or viewing their content.

Criminal investigation - All activities involved in the process of investigating and prosecuting a crime including collecting evidence or information pertaining to a crime, apprehending a suspect, and any subsequent related proceedings such as a trial or sentencing.

Campaign adaptation

Type: Categorical (multiple selection allowed)

Actions taken by campaign operators and participants in response to the observable outcomes and mitigation attempts. Details of campaign adaptations will be described in case studies when applicable.

Tactical redeployment - The redeployment of a media manipulation or disinformation campaign's tactics.

Tactical adjustment - The continuation of a media manipulation or disinformation campaign with adjustments to the tactics or new tactics altogether.

Unclear or no adaptation - There is no adaptation or redeployment of tactics based on the available evidence.