|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |

|  |  |
| --- | --- |
|

|  |
| --- |
| Forwarded this email? [Subscribe here](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1lbWFpbCZ1dG1fY2FtcGFpZ249ZW1haWwtc3Vic2NyaWJlJnI9d2tlMXQmbmV4dD1odHRwcyUzQSUyRiUyRnJ3bWFsb25lbWQuc3Vic3RhY2suY29tJTJGcCUyRnRhY3RpY3Mtb2YtZGlzaW5mb3JtYXRpb24iLCJwIjoxMzc4OTU0MjUsInMiOjU4MzIwMCwiZiI6dHJ1ZSwidSI6NTQ2OTkwNDEsImlhdCI6MTY5NzEyNzg0NSwiZXhwIjoxNjk5NzE5ODQ1LCJpc3MiOiJwdWItMCIsInN1YiI6ImxpbmstcmVkaXJlY3QifQ.ILJbj1-k0bwNqQzem6kBEN4flF2jBK5hiL0zdB-iJqk) for more |

 |

[**Upgrade to paid**](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1wb3N0JnV0bV9jYW1wYWlnbj1lbWFpbC1jaGVja291dCZuZXh0PWh0dHBzJTNBJTJGJTJGcndtYWxvbmVtZC5zdWJzdGFjay5jb20lMkZwJTJGdGFjdGljcy1vZi1kaXNpbmZvcm1hdGlvbiZyPXdrZTF0JnRva2VuPWV5SjFjMlZ5WDJsa0lqbzFORFk1T1RBME1Td2lhV0YwSWpveE5qazNNVEkzT0RRMUxDSmxlSEFpT2pFMk9UazNNVGs0TkRVc0ltbHpjeUk2SW5CMVlpMDFPRE15TURBaUxDSnpkV0lpT2lKamFHVmphMjkxZENKOS5NRU1TRTlKSzgwOXFBNUtMalB6dWwtZHI2ZmRCNmZfZS00dGg5cDB4Z21jIiwicCI6MTM3ODk1NDI1LCJzIjo1ODMyMDAsImYiOnRydWUsInUiOjU0Njk5MDQxLCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTAiLCJzdWIiOiJsaW5rLXJlZGlyZWN0In0.ZEBtw6S5D0MoO-mUQthUlX6yoAcT3oBKDWLcow7SgME?&utm_medium=email&utm_source=subscribe-widget&utm_content=137895425)[**Tactics of Disinformation**](https://substack.com/app-link/post?publication_id=583200&post_id=137895425&utm_source=post-email-title&utm_campaign=email-post-title&isFreemail=true&r=wke1t&token=eyJ1c2VyX2lkIjo1NDY5OTA0MSwicG9zdF9pZCI6MTM3ODk1NDI1LCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTU4MzIwMCIsInN1YiI6InBvc3QtcmVhY3Rpb24ifQ.Vk1WnIIXdGVg_jZ7SbzKChW-58dG7CFoVF-pbhFTsDU)An amazing self-own from the US Government's Cybersecurity and Infrastructure Security Agency (CISA)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|

|  |
| --- |
| [Robert W Malone MD, MS](https://substack.com/redirect/c48b653c-c711-4014-918c-b2b4ef3ea616?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) |

 |
|

|  |
| --- |
| Oct 12 |

 |

 |

|  |
| --- |
|  |

 |

|  |
| --- |
|   |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
|  |

 |  |

|  |
| --- |
|  |

 |  |

|  |
| --- |
|  |

 |  |

|  |
| --- |
|  |

 |

 |

|  |  |
| --- | --- |
|

|  |
| --- |
| [READ IN APP](https://open.substack.com/pub/rwmalonemd/p/tactics-of-disinformation?utm_source=email&redirect=app-store) |

 |

 |

 |
|   |
|  |  |  |

**Background and Context**In this essay I provide an overview of disinformation tactics summarized on the US Government's Cybersecurity and Infrastructure Security Agency (CISA) CISA.gov website, and have modified that document for use by individuals and organizations wishing to counter the mis-mal-disinformation (MDM) constantly emanating from governments, corporations - such as big pharma, non-governmental organizations (such as the Gates foundation), astroturf organizations (such as the Center for Countering Digital Hate). For more information on CISA, please see our prior Substack essay titled ["HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS": THE WEAPONIZATION OF CISA - Interim staff report for the Committee on the Judiciary and the Select Subcommittee.](https://substack.com/redirect/77a91ba0-32d9-41ac-8f4d-9db2b60ed746?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo)In addition to the various organizations, the information summarized below also applies to individuals spreading MDM, including those who are working for these agencies or as individuals, with their own, personal agendas.All of the disinformation tactics described below are being used against the health sovereignty movement, the freedom (or liberty) movements, those pushing back against UN Agenda 2030 and the approved climate agenda, the WEF, the UN, and the resistance against globalization movement (NWO). **Tactics of Disinformation**Disinformation actors include governments, commercial and non-profit organizations as well as individuals. These actors use a variety of tactics to influence others, stir them to action, and cause harm. Understanding these tactics can increase preparedness and promote resilience when faced with disinformation.Disinformation actors use a variety of tactics and techniques to execute information operations and spread disinformation narratives for a variety of reasons. Some may even be well intentioned but ultimately fail on ethical grounds. [Using disinformation for beneficial purposes is still wrong](https://substack.com/redirect/342bf5ef-6f71-4a08-97b7-dba127e99a32?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo). Each of these tactics are designed to make disinformation actors’ messages more credible, or to manipulate their audience to a specific end. They often seek to polarize their target audience across contentious political or social divisions, making the audience more receptive to disinformation.These methods can and have been weaponized by disinformation actors. By breaking down common tactics, sharing real-world examples, and providing concrete steps to counter these narratives with accurate information, the Tactics of Disinformation listed below are intended to help individuals and organizations understand and manage the risks posed by disinformation, Any organization or its staff can be targeted by disinformation campaigns, and all organizations and individuals have a role to play in building a resilient information environment. All of this is yet another aspect of the Fifth Generation Warfare (or propaganda/PsyWar) technologies, strategy, and tactics which are being routinely deployed on all of us by our governments, corporations, and various non-state actors.**Disinformation Tactics Overview****Cultivate Fake or Misleading Personas and Websites**: Disinformation actors create networks of fake personas and websites to increase the believability of their message with their target audience. Fake expert networks use inauthentic credentials (e.g., fake “experts”, journalists, think tanks, or academic institutions) to lend undue credibility to their influence content and make it more believable.**Create Deepfakes and Synthetic Media**: Synthetic media content may include photos, videos, and audio clips that have been digitally manipulated or entirely fabricated to mislead the viewer. Artificial intelligence (AI) tools can make synthetic content nearly indistinguishable from real life. Synthetic media content may be deployed as part of disinformation campaigns to promote false information and manipulate audiences.**Devise or Amplify Conspiracy Theories**: Conspiracy theories attempt to explain important events as secret plots by powerful actors. Conspiracy theories not only impact an individual’s understanding of a particular topic; they can shape and influence their entire worldview. Disinformation actors capitalize on conspiracy theories by generating disinformation narratives that align with the conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience.**Astroturfing and Flooding the Information Environment**: Disinformation campaigns will often post overwhelming amounts of content with the same or similar messaging from several inauthentic accounts. This practice, known as astroturfing, creates the impression of widespread grassroots support or opposition to a message, while concealing its true origin. A similar tactic, flooding, involves spamming social media posts and comment sections with the intention of shaping a narrative or drowning out opposing viewpoints.**Abuse Alternative Platforms:** Disinformation actors may abuse alternative social media platforms to intensify belief in a disinformation narrative among specific user groups. Disinformation actors may seek to take advantage of platforms with fewer user protections, less stringent content moderation policies, and fewer controls to detect and remove inauthentic content and accounts than other social media platforms.**Exploit Information Gaps:** Data voids, or information gaps, occur when there is insufficient credible information to satisfy a search inquiry. Disinformation actors can exploit these gaps by generating their own influence content and seeding the search term on social media to encourage people to look it up. This increases the likelihood that audiences will encounter disinformation content without any accurate or authoritative search results to refute it.**Manipulate Unsuspecting Actors:** Disinformation actors target prominent individuals and organizations to help amplify their narratives. Targets are often unaware that they are repeating a disinformation actor’s narrative or that the narrative is intended to manipulate.**Spread Targeted Content:** Disinformation actors produce tailored influencer content likely to resonate with a specific audience based on their worldview and interests. These actors gain insider status and grow an online following that can make future manipulation efforts more successful. This tactic often takes a “long game” approach of spreading targeted content over time to build trust and credibility with the target audience.**Actions You Can Take**Although disinformation tactics are designed to deceive and manipulate, critically evaluating content and verifying information with credible sources before deciding to share it can increase resilience against disinformation and slow its spread. * **Recognize the risk.** Understand how disinformation actors leverage these tactics to push their agenda. Be wary of manipulative content that tries to divide.
* **Question the source.** Critically evaluate content and its origin to determine whether it’s trustworthy. Research the author’s credentials, consider the outlet’s agenda, and verify the supporting facts.
* **Investigate the issue.** Conduct a thorough, unbiased search into contentious issues by looking at what credible sources are saying and considering other perspectives. Rely on credible sources of information, such as government sites.
* **Think before you link.** Slow down. Don’t immediately click to share content you see online. Check the facts first. Some of the most damaging disinformation spreads rapidly via shared posts that seek to elicit an emotional reaction that overpowers critical thinking.
* **Talk with your social circle.** Engage in private, respectful conversations with friends and family when you see them sharing information that looks like disinformation. Be thoughtful what you post on social media.

**The next sections discuss common disinformation technologies, tactics and strategies in more detail.****Cultivate Fake or Misleading Personas and Websites****Description:** Disinformation actors create networks of fake personas and websites to increase the believability of their message with their target audience. Such networks may include fake academic or professional “experts,” journalists, think tanks, and/or academic institutions. Some fake personas are even able to validate their social media accounts (for example, a blue or gray checkmark next to a username), further confusing audiences about their authenticity. Fake expert networks use inauthentic credentials to make their content more believable.Disinformation actors also increase the credibility of these fake personas by generating falsified articles or research papers and sharing them online. Sometimes, these personas and their associated publications are intentionally amplified by other actors. In some instances, these materials are also unwittingly shared by legitimate organizations and users. The creation or amplification of content from these fake personas makes it difficult for audiences to distinguish real experts from fake ones.Adversaries have also demonstrated a “long game” approach with this tactic by building a following and credibility with seemingly innocuous content before switching their focus to creating and amplifying disinformation. This lends a false credibility to campaigns.Example: During the course of the COVIDcrisis, I have had a number of misleading personas and websites (including substack authors) target me. It is extremely disturbing to see fragments of my CV, my life, my peer-review papers dissected, re-configured, even modified to target me. Evidently, because some government and/or organization perceives my ideas to be dangerous.There is one person on Twitter with almost 100,000 followers who has literally posted thousands of posts targeting me. At one point, Jill took screen shots of all of these posts and placed in a summary document. She gave up the project at around page 1500. The file was too big to handle easily. Everyday for years, this disinformation actor posts two to three hit pieces on me - mixed with other content. He has used every single one of these tactics outlined above. Clearly, he is being paid by an organization or government. He self-defines as an independent journalist, and has a long and well documented history of cyberstalking and spreading falsehoods. Many of his followers do not question his authenticity. One of the followers recently even attacked me for having worked on development of the Remdesivir vaccine! These posts get passed around as authentic information, and there is nothing I can do. These fabricated fake information fragments then gets spread as if they are true information, and other influencers report on these posts as if they were real. The cycle goes around and around. The end result is not only intentional damage to myself and my reputation, but also that the whole resistance movement (whatever that is) gets delegitimized.Which is a “win” for those chaos agents who are pushing this disinformation.**Create Deepfakes and Synthetic Media**Synthetic media content may include photos, videos, and audio clips that have been digitally manipulated or entirely fabricated to mislead the viewer. *Cheapfakes* are a less sophisticated form of manipulation involving real audio clips or videos that have been sped up, slowed down, or shown out of context to mislead. Sort of like how the corporate media will often take limited quotes out of context and then weaponize them. In contrast, *deepfakes* are developed by training artificial intelligence (AI) algorithms on reference content until it can produce media that is nearly indistinguishable from real life. Deepfake technology makes it possible to convincingly depict someone doing something they haven’t done or saying something they haven’t said. While synthetic media technology is not inherently malicious, it can be deployed as part of disinformation campaigns to share false information or manipulate audiences.Deepfake photos by disinformation actors can be used to generate realistic profile pictures to create a large network of inauthentic social media accounts. Deepfake videos often use AI technology to map one person’s face to another person’s body. In the case of audio deepfakes, a “voice clone” can produce new sentences as audio alone or as part of a video deepfake, often with only a few hours (or even minutes) of reference audio clips. Finally, an emerging use of deepfake technology involves AI-generated text, which can produce realistic writing and presents a unique challenge due to its ease of production.**Devise or Amplify Conspiracy Theories**Conspiracy theories attempt to explain important events as secret plots by powerful actors. Conspiracy theories not only impact an individual’s understanding of a particular topic; they can shape and influence their entire worldview. Conspiracy theories often present an attractive alternative to reality by explaining uncertain events in a simple and seemingly cohesive manner, especially during times of heightened uncertainty and anxiety.Disinformation actors capitalize on conspiracy theories by generating disinformation narratives that align with the conspiracy worldview, increasing the likelihood that the narrative will resonate with the target audience. By repeating certain tropes across multiple narratives, malign actors increase the target audience’s familiarity with the narrative and therefore its believability. Conspiracy theories can also present a pathway for radicalization to violence among certain adherents. Conspiracy theories can alter a person’s fundamental worldview and can be very difficult to counter retroactively, so proactive resilience building is especially critical to prevent conspiratorial thinking from taking hold. Furthermore, conspiracy theories can also be used to divide groups as well as bad jacket individuals within a movement. Conspiracy theories can also be used to discredit a movement. Conspiracy theories that are not based in reality, that can be linked to a movement or organization can be used to smear that group as a “fringe element.” Not to be taken seriously or to drown out expert voices.**Astroturfing and Flooding the Information Environment**Disinformation campaigns will often post overwhelming amounts of content with the same or similar messaging from several inauthentic accounts, either created by automated programs known as bots or by professional disinformation groups known as troll farms. By consistently seeing the same narrative repeated, the audience sees it as a popular and widespread message and is more likely to believe it. This practice, known as astroturfing, creates the impression of widespread grassroots support or opposition to a message, while concealing its true origin.A similar tactic, flooding, involves spamming social media posts and comment sections with the intention of shaping a narrative or drowning out opposing viewpoints, often using many fake and/or automated accounts. Flooding may also be referred to as “firehosing.”This tactic is used to stifle legitimate debate, such as the discussion of a new policy or initiative, and discourage people from participating in online spaces. Information manipulators use flooding to dull the sensitivity of targets through repetition and create a sense that nothing is true. Researchers call these tactics “censorship by noise,” where artificially amplified narratives are meant to drown out all other viewpoints. Artificial intelligence and other advanced technologies enable astroturfing and flooding to be deployed at speed and scale, more easily manipulating the information environment and influencing public opinion.**Abuse Alternative Platforms**Disinformation actors often seek opportunities for their narratives to gain traction among smaller audiences before attempting to go viral. While alternative social media platforms are not inherently malicious, disinformation actors may take advantage of less stringent platform policies to intensify belief in a disinformation narrative among specific user groups. These policies may include fewer user protections, less stringent content moderation policies, and fewer controls to detect and remove inauthentic content and accounts than some of the other social media platforms.Alternative platforms often promote unmoderated chat and file sharing/storage capabilities, which is not inherently malicious but may be appealing for actors who want to share disinformation.\* While some alternative platforms forbid the promotion of violence on public channels, they may have less visibility into private channels or groups promoting violence. Disinformation actors will recruit followers to alternative platforms by promoting a sense of community, shared purpose, and the perception of fewer restrictions. Groups on alternative platforms may operate without the scrutiny or detection capabilities that other platforms have. Often, groups focus on specific issues or activities to build audience trust and disinformation actors can, in turn, abuse this trust and status to establish credibility on other platforms.**Exploit Information Gaps**Data voids, or information gaps, occur when there is insufficient credible information to satisfy a search inquiry, such as when a term falls out of use or when an emerging topic or event first gains prominence (e.g., breaking news). When a user searches for the term or phrase, the only results available may be false, misleading, or have low credibility. While search engines work to mitigate this problem, disinformation actors can exploit this gap by generating their own influence content and seeding the search term on social media to encourage people to look it up.Because the specific terms that create data voids are difficult to identify beforehand, credible sources of information are often unable to proactively mitigate their impacts with accurate information. Disinformation actors can exploit data voids to increase the likelihood a target will encounter disinformation without accurate information for context thus increasing the likelihood the content is seen as true or authoritative. Additionally, people often perceive information that they find themselves on search engines as more credible, and it can be challenging to reverse the effects of disinformation once accepted.Of course, recognize that the “Googlenet” and other search engines place government websites and “trusted sources” before other sources of information. Remember, just because it is the first term found on Google does not make it true.The Googlenet does not like data voids. So when Google does not like the analytics of a search term or encounters a datavoid, they fill the gap with information they do like. The Googlenet has even been caught manipulating search results by hand. This is what happened with the search term “mass formation psychosis” was used to describe the public response to the COVIDcrisis. As this term went against the COVID narrative, its legitimacy was quickly snuffed out by the Googlenet.**Manipulate Unsuspecting Actors**Disinformation campaigns target prominent individuals and organizations to help amplify their narratives. These secondary spreaders of disinformation narratives add perceived credibility to the messaging and help seed these narratives at the grassroots level while disguising their original source. Targets are often unaware that they are repeating a disinformation actors’ narrative or that the narrative is intended to manipulate. The content is engineered to appeal to their and their follower’s emotions, causing the influencers to become unwitting facilitators of disinformation campaigns.**Spread Targeted Content**Disinformation actors surveil a targeted online community to understand its worldview, interests, and key influencers and then attempt to infiltrate it by posting tailored influence content likely to resonate with its members. By starting with entertaining or non-controversial posts that are agreeable to targeted communities, disinformation actors gain “insider” status and grow an online following that can make future manipulation efforts more successful. This tactic may be used in combination with cultivating fake experts, who spread targeted content over time, taking a “long game” approach that lends false credibility to the campaign. Targeted content often takes highly shareable forms, like memes or videos, and can be made to reach very specific audiences by methods such as paid advertising and exploited social media algorithms.**In Conclusion**The distribution of mis- dis- or mal- information is currently defined as domestic terrorism by the US Department of Homeland Security (for receipts, please see prior Substack essay [“DHS: Mis- dis- and mal-information (MDM) being caused by "Domestic Terrorists"](https://substack.com/redirect/c20ce5cf-eac4-4b2b-9ef1-5708afd983ad?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo)). The [2010 DoD Psychological Operations manual](https://substack.com/redirect/aba4b6c9-805f-4b64-b4f0-c74d085fb5f5?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo), signed off by current Secretary of Defense Lloyd Austin, includes the following clause: “When authorized, PSYOP forces may be used domestically to assist lead federal agencies during disaster relief and crisis management by informing the domestic population”. In other words, any time a disaster or crisis occurs - as loosely defined by any component of the Federal administrative state, the DoD is authorized to deploy military grade PSYOP (otherwise known as PsyWar) technologies and capabilities on US citizens. A key aspect of PSYOP or PsyWar capabilities involves distribution of [grey and black propaganda](https://substack.com/redirect/d07cbe1a-0260-4a20-81a0-1b6db558bc4c?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) into a targeted population. The methods used to accomplish this (summarized above) are clearly defined by CISA on its own website, and the congressional [Interim staff report for the Committee on the Judiciary and the Select Subcommittee](https://substack.com/redirect/77a91ba0-32d9-41ac-8f4d-9db2b60ed746?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) titled “[HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS": THE WEAPONIZATION OF CISA](https://substack.com/redirect/77a91ba0-32d9-41ac-8f4d-9db2b60ed746?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) provides a summary road map of how CISA has acted as a key coordinating agency for the Federal administrative state as it has deployed these technologies, tactics and strategies on United States citizens.In an article published in USA Today on October 03. 2023 titled “[Federal appeals court expands limits on Biden administration in First Amendment case](https://substack.com/redirect/a51f6663-c8fc-46ad-82c0-58b424fc6675?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo)”, journalists Jessica Guynn and John Fritze summarize current standing of the key legal case which is revealing the weaponization of CISA against the American populace.The nation’s top cybersecurity defense agency likely [violated the First Amendment](https://substack.com/redirect/8f29da3f-3d1f-4291-b359-2decbf3b3811?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) when lobbying Silicon Valley companies to remove or suppress the spread of online content about elections, a federal appeals court ruled Tuesday.The 5th Circuit Court of Appeals expanded an injunction issued in September to include the Cybersecurity and Infrastructure Security Agency, ruling that it used [frequent interactions with social media platforms](https://substack.com/redirect/58bcaaef-0b3d-402c-b50f-e97411158f1e?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) “to push them to adopt more restrictive policies on election-related speech.”The previous decision from a panel of three judges – nominated by Republican presidents – concluded that the actions of the Biden White House, FBI and other government agencies likely violated the First Amendment but that CISA – which is charged with securing elections from online threats – attempted to convince, not coerce.Republican attorneys general, who brought the case, asked for a rehearing. In Tuesday’s order, the 5th Circuit judges ruled that CISA facilitated the FBI’s interactions with social media companies. The order bars CISA and top agency officials including director Jen Easterly from taking steps to [“coerce or significantly encourage”](https://substack.com/redirect/37a9a1d4-0496-42e7-b47d-3a16c4c6eb96?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo) tech companies to take down or curtail the spread of social media posts.The Justice Department declined to comment. CISA, which is part of the Department of Homeland Security, said it does not comment on ongoing litigation, but executive director Brandon Wales said in a statement that the agency does not censor speech or facilitate censorship.The lawsuit was filed by the attorneys general of Missouri and Louisiana as well as individuals who said their speech was censored.“CISA is the ‘nerve center’ of the vast censorship enterprise, the very entity that worked with the FBI to silence the Hunter Biden laptop story,” Missouri Attorney General Andrew Bailey tweeted. CISA knew precisely what it was doing and how to accomplish the censorship and propaganda agenda of the Obama/Biden administration. There are three key questions remaining at this point1. What will the Supreme court do about CISA and Biden Administration violations of the First Amendment?
2. Which is the greater risk, mis- dis- and mal- information deployed on US Citizens by the USG Administrative State, or US Citizens discussing information and ideas that the USG Administrative State does not want discussed, and therefore defines as misinformation.
3. What do you intend to do about this?

Please keep in mind where this all started. And also remember that in Fifth Generation Warfare, otherwise known as PsyWar, the battle is for control of your mind, thoughts, emotions, and all information you are exposed to. The only way to win at PsyWar is not to play. As soon as you engage with either corporate or social media, you enter the battlefield. So be careful out there. Know the technology, tactics and strategy of your opponents. The PsyWar battlefield terrain is tortuous, bizarre, constantly shifting, and dangerous to your mental health. Our opponents make no distinction between combatant and non-combatant, and they recognize no moral boundaries to what they will do to achieve their objectives. *“Who is Robert Malone” is a reader supported publication. Please consider subscribing and sharing my articles.*[***Upgrade to paid***](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1wb3N0JnV0bV9jYW1wYWlnbj1lbWFpbC1jaGVja291dCZuZXh0PWh0dHBzJTNBJTJGJTJGcndtYWxvbmVtZC5zdWJzdGFjay5jb20lMkZwJTJGdGFjdGljcy1vZi1kaXNpbmZvcm1hdGlvbiZyPXdrZTF0JnRva2VuPWV5SjFjMlZ5WDJsa0lqbzFORFk1T1RBME1Td2lhV0YwSWpveE5qazNNVEkzT0RRMUxDSmxlSEFpT2pFMk9UazNNVGs0TkRVc0ltbHpjeUk2SW5CMVlpMDFPRE15TURBaUxDSnpkV0lpT2lKamFHVmphMjkxZENKOS5NRU1TRTlKSzgwOXFBNUtMalB6dWwtZHI2ZmRCNmZfZS00dGg5cDB4Z21jIiwicCI6MTM3ODk1NDI1LCJzIjo1ODMyMDAsImYiOnRydWUsInUiOjU0Njk5MDQxLCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTAiLCJzdWIiOiJsaW5rLXJlZGlyZWN0In0.ZEBtw6S5D0MoO-mUQthUlX6yoAcT3oBKDWLcow7SgME?&utm_medium=email&utm_source=subscribe-widget&utm_content=137895425)Thank you for reading Who is Robert Malone. This post is public so feel free to share it.[**Share**](https://substack.com/app-link/post?publication_id=583200&post_id=137895425&utm_source=substack&utm_medium=email&utm_content=share&utm_campaign=email-share&action=share&triggerShare=true&isFreemail=true&r=wke1t&token=eyJ1c2VyX2lkIjo1NDY5OTA0MSwicG9zdF9pZCI6MTM3ODk1NDI1LCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTU4MzIwMCIsInN1YiI6InBvc3QtcmVhY3Rpb24ifQ.Vk1WnIIXdGVg_jZ7SbzKChW-58dG7CFoVF-pbhFTsDU)[**Give a gift subscription**](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1wb3N0JnV0bV9jYW1wYWlnbj1lbWFpbC1jaGVja291dCZuZXh0PWh0dHBzJTNBJTJGJTJGcndtYWxvbmVtZC5zdWJzdGFjay5jb20lMkZwJTJGdGFjdGljcy1vZi1kaXNpbmZvcm1hdGlvbiZyPXdrZTF0JnRva2VuPWV5SjFjMlZ5WDJsa0lqbzFORFk1T1RBME1Td2lhV0YwSWpveE5qazNNVEkzT0RRMUxDSmxlSEFpT2pFMk9UazNNVGs0TkRVc0ltbHpjeUk2SW5CMVlpMDFPRE15TURBaUxDSnpkV0lpT2lKamFHVmphMjkxZENKOS5NRU1TRTlKSzgwOXFBNUtMalB6dWwtZHI2ZmRCNmZfZS00dGg5cDB4Z21jIiwicCI6MTM3ODk1NDI1LCJzIjo1ODMyMDAsImYiOnRydWUsInUiOjU0Njk5MDQxLCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTAiLCJzdWIiOiJsaW5rLXJlZGlyZWN0In0.ZEBtw6S5D0MoO-mUQthUlX6yoAcT3oBKDWLcow7SgME?&gift=true)

|  |  |  |
| --- | --- | --- |
|  |  |  |

You're currently a free subscriber to [Who is Robert Malone](https://substack.com/redirect/bb1ee7b1-599d-4f7a-8f46-1b000da7da17?j=eyJ1Ijoid2tlMXQifQ.SE-VFIDjmL6q3IZJzeaahaqLNZ_82-S4L0hJ6yHiBmo). For the full experience, [upgrade your subscription.](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1wb3N0JnV0bV9jYW1wYWlnbj1lbWFpbC1jaGVja291dCZuZXh0PWh0dHBzJTNBJTJGJTJGcndtYWxvbmVtZC5zdWJzdGFjay5jb20lMkZwJTJGdGFjdGljcy1vZi1kaXNpbmZvcm1hdGlvbiZyPXdrZTF0JnRva2VuPWV5SjFjMlZ5WDJsa0lqbzFORFk1T1RBME1Td2lhV0YwSWpveE5qazNNVEkzT0RRMUxDSmxlSEFpT2pFMk9UazNNVGs0TkRVc0ltbHpjeUk2SW5CMVlpMDFPRE15TURBaUxDSnpkV0lpT2lKamFHVmphMjkxZENKOS5NRU1TRTlKSzgwOXFBNUtMalB6dWwtZHI2ZmRCNmZfZS00dGg5cDB4Z21jIiwicCI6MTM3ODk1NDI1LCJzIjo1ODMyMDAsImYiOnRydWUsInUiOjU0Njk5MDQxLCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTAiLCJzdWIiOiJsaW5rLXJlZGlyZWN0In0.ZEBtw6S5D0MoO-mUQthUlX6yoAcT3oBKDWLcow7SgME?&utm_source=substack&utm_medium=email&utm_content=postcta)[**Upgrade to paid**](https://substack.com/redirect/2/eyJlIjoiaHR0cHM6Ly9yd21hbG9uZW1kLnN1YnN0YWNrLmNvbS9zdWJzY3JpYmU_dXRtX3NvdXJjZT1wb3N0JnV0bV9jYW1wYWlnbj1lbWFpbC1jaGVja291dCZuZXh0PWh0dHBzJTNBJTJGJTJGcndtYWxvbmVtZC5zdWJzdGFjay5jb20lMkZwJTJGdGFjdGljcy1vZi1kaXNpbmZvcm1hdGlvbiZyPXdrZTF0JnRva2VuPWV5SjFjMlZ5WDJsa0lqbzFORFk1T1RBME1Td2lhV0YwSWpveE5qazNNVEkzT0RRMUxDSmxlSEFpT2pFMk9UazNNVGs0TkRVc0ltbHpjeUk2SW5CMVlpMDFPRE15TURBaUxDSnpkV0lpT2lKamFHVmphMjkxZENKOS5NRU1TRTlKSzgwOXFBNUtMalB6dWwtZHI2ZmRCNmZfZS00dGg5cDB4Z21jIiwicCI6MTM3ODk1NDI1LCJzIjo1ODMyMDAsImYiOnRydWUsInUiOjU0Njk5MDQxLCJpYXQiOjE2OTcxMjc4NDUsImV4cCI6MTY5OTcxOTg0NSwiaXNzIjoicHViLTAiLCJzdWIiOiJsaW5rLXJlZGlyZWN0In0.ZEBtw6S5D0MoO-mUQthUlX6yoAcT3oBKDWLcow7SgME?&utm_source=substack&utm_medium=email&utm_content=postcta) |