World Without Truth

How Business Must Confront the AI-Powered Disinformation Supply Chain

Dave Aron | Andrew Frank | Richard Hunter

Gartner

1st Edition – September 2025

First published September 2025 by

Gartner Inc.
56 Top Gallant Road
Stamford, CT
USA

Contact: WorldWithoutTruth@gartner.com

For my wife, my daughter, and in memory of my parents,
who ignited my love of learning.
Dave Aron

For my wife, my daughter, my mother and all
the friends and colleagues who helped along the way.
Andrew Frank

This is for my grandchildren, who will live
their lives in the world we have created,
and my mother, who has been a source of
strength and wisdom all my life.
Richard Hunter

Foreword

In the last few decades, we have seen, wondered at, and benefited from the seemingly continuous rise in the power of digital technology and the value of information. We have witnessed the transition from poor quality audio transmission to high resolution immersive video communication. And the availability of digital information moving from the landline anchored at home to the smartphone on the move, and more recently to planes, trains, automobiles and now space. Digital technology has invaded our offices, our homes, our cars, and even our bodies and our pets.

Like every innovation, these digital technology evolutions have a dark side. Every new technology capability opens multiple new threat vectors and uncovers before unknown weaknesses in existing systems. Every day we read about new and innovative attacks affecting individuals, companies, critical infrastructure, societies and governments. Cyber-security has become even more important than physical security in many cases.

But now, as the authors of "World Without Truth" point out, there is a third layer of security we need: disinformation security. Even if a business has perfect physical and cyber-security, it would be still vulnerable to disinformation campaigns. Bad information that can skew our perceptions, cause us to make bad decisions or damage our reputation.

We all know that disinformation is not a new topic; it has been around since societies began. Propaganda was a more familiar term in the past, but it all boils down to the same thing – bad information by bad actors to achieve their goals.

So why now? Why is this attention to disinformation so important and so different. It is really a question of scale, scope and capability. A couple of hundred years ago, I might have been able to print flyers with disinformation and spread them around physically to a limited number of

people. Fifty years ago, with sufficient funds, I could have used TV and radio to broadcast a message to millions.

Now I can reach billions over social media, apps and other digital channels. What's more, I can execute a campaign for a fraction of a cost compared to previous mean. And I can even mass customize the content for each consumer based on demographic and psychographic data. Moreover, the content is no longer a simple text message or a picture. It could be a video of each consumer's loved ones speaking a message in their voice.

This issue is hiding in plain sight. We all hear the stories of disinformation attacks, but we are not yet prepared for the huge deluge of disinformation that is coming our way. The title "World Without Truth" captures the world that is coming beautifully.

In this book, Dave, Andrew and Richard make this clear, but fortunately they don't just admire the problem. They propose solutions. In terms of both the broad-brush levers that we have at hand as societies to meet disinformation head on, and the disciplines each organization can adopt to master disinformation detection and countermeasures. For the latter, they have coined the term *TrustOps*, short for trust operations.

As you read this excellent treatise on the topic of disinformation and its countermeasures, I encourage you to consider where disinformation will be in the next few years, and how ready you, your organizations, governments and societies are for the onslaught of disinformation.

Jeffrey L. Sampler
Professor of Practice, Hong Kong University Business School

"Those who can make you believe absurdities can make you commit atrocities."

Voltaire, 1765.

Introduction

Welcome to a World Without Truth

The temperature in the boardroom was rising. The chairman held up his phone and addressed the CEO. "*My inbox was swamped this morning. Did you see this video? Who is this guy? And why's he repeating these lies about us?*" The CEO looked calm. "*It looks like one of our lobbyist friends in Washington. But it could be a deepfake. In any case, the PR team is on it. It'll be debunked by the end of the day. And we're expecting no impact on next week's earnings call.*" The chairman was unimpressed. "*No impact? Have you looked at our stock price? This disinformation campaign has been building for almost a month. We know it's being orchestrated by someone with resources who is intent on framing us as traitors. We have to get out in front of this. I need to see your plan for a new approach…*"

This book is about the threats that a rising flood of disinformation poses to businesses, industries, and the world at large. It is about how generative and agentic artificial intelligence are joining social networks, advanced analytics and other digital innovations to deliver power to parties ruthless enough to exploit these new capabilities against their adversaries. And most importantly, it's about what companies should do about it.

This is not a book about politics. Although political polarization figures prominently in the design of disinformation, its motives are more often commercial: to persuade people that scientific consensus is wrong when it threatens an industry, or to undermine the claims and reputation of disruptive competitors.

Of course, using false information for political gain is as old as civilization itself. In Rome in 44 B.C.E., after Julius Caesar's assassination, his nephew Octavian engaged in a systematic disinformation campaign against Marc Antony, his rival. Octavian publicly claimed to have obtained Antony's will, which he claimed contained plans to bequeath Roman territories to Antony's children with Cleopatra, the Egyptian queen of whom the Romans were suspicious. He read this fake will in the Senate, successfully

swaying public opinion against Antony, which led to Antony's downfall and eventual suicide. This is one of the first documented examples of disinformation.

Those wanting to mislead have always had a wide variety of tactics available to them. Table 1 outlines ten categories of disinformation stratagem.

Table 1. Disinformation Stratagems

Stratagem	Explanation
Deceive	Deliberately create and/or propagate wrong information.
Distort	Introduce biases in information that skew perceptions.
Divide	Create and/ propagate multiple conflicting narratives to sow discontent.
Deluge	Overwhelm consumers with too much information.
Distract	Flood the channel with other pressing matters that capture consumers' attention.
Deaden	Silence, suppress or censor content and sources that conflict with disinformers' messages.
Deny	Conduct campaigns to deny information that is known to be true.
Discredit motive	Spread information to make it seem that sources have ulterior motives.
Discredit method	Spread information to make it seem that sources' information is unreliable.
Demotivate	Change actual/ perceived incentives and disincentives for producers and/ or consumers of information.

More generally, let's reflect for a moment on the question, "*Why is information so important?*" The answer is that all societies and organizations require good information to function well. It is impossible to know everything you need to know in a country, city or company with more than a handful of people. People need good sources of information to make

good decisions about their health, their work, their families. Related, but not exactly the same, is the need to have shared information and confidence about sources of information to create social cohesion and trust, the glue that binds us together.

Availability of reliable information is specifically important for companies, public sector agencies, non-governmental and all other organizations in three ways:

1. *Consumption*. Organizations need to be confident that they are using good information to make decisions. This includes information about customers and their needs, competitors, markets, governments and regulations.

2. *Production*. Organizations must ensure that the information they share, both externally and internally, including commercial information, is accurate. This includes being sure of the provenance of information, and specifically whether its source is trustworthy or not.

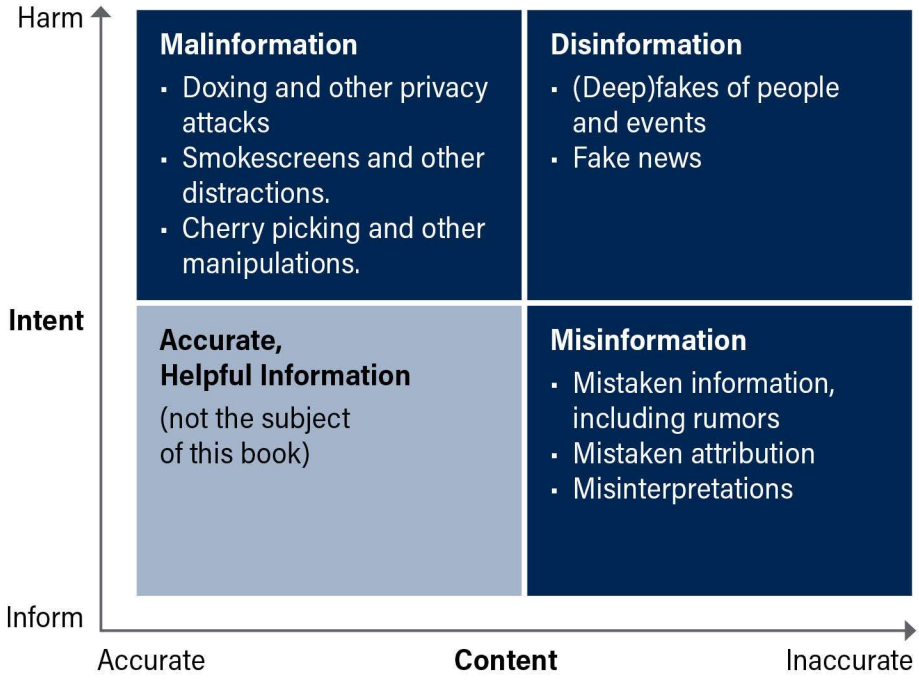
3. *Reputation.* Organizations must ensure that information circulating in the market about them is accurate, and if not, take appropriate action to address it. This includes accidental misinformation and deliberate disinformation.

If disinformation has always been with us, why worry about it now? The reason is that twenty-first century technology is transforming disinformation into something new. Social media has given it instant, low-cost global reach. Generative AI is arming it with tools to convincingly simulate reality. AI-powered analytics are tailoring it to maximize its persuasive power over individuals. And agentic AI is allowing the whole thing to happen without the need for human oversight or intervention. As prevalent as disinformation has become in recent years, emerging technologies threaten a vast escalation. The need to address accidental *misinformation* and deliberate *disinformation* now is rising to a top concern in the boardroom.

Throughout this book, the words misinformation, disinformation and on occasion malinformation will be used. Figure 1 positions them, in terms of

accuracy of content, and harmfulness of intent and the callout contains definitions on these and other important terms used in the book.

Terms for Harmful Information Intent and Content



Source: Gartner

Figure 1. Terms for Harmful Information Intent and Content

A Few Useful Definitions

For this book, *facts* are defined as empirically verifiable data points, and *truth* as an accurate description of reality based on facts. Two news reports could have the same number of facts, but one may be true and the other false. (Philosophers have debated the meaning of truth for centuries and will continue for centuries to come. The authors beg the reader to accept this brief definition as functional for the purposes of this book.)

Misinformation is defined as the act of creating or distributing information that is accidentally erroneous. The provider of this wrong information has no intent to harm their target, but this can lead to harmful conclusions about products, people, and institutions. Misinformation has become an exponentially larger global issue because of the rise of influencers on social media. For example, medically and scientifically uneducated and uninformed influencers often post definitive positions related to the safety and efficacy vaccines that they erroneously believe are correct.

Disinformation is defined as the act of deliberately creating or distributing false information with the intention of harming its chosen target. A goal of a disinformer might be to make targets believe something specific about an adversary. Sometimes disinformers are working on a metalevel to change the way people think, in a sense turning their targets into agents and promoters of disinformation. For example, if a disinformer can influence people to believe that big pharmaceutical companies routinely suppress information about the harmful effects of their medications, they can boost the market for pseudoscientific treatments and maybe even recruit consumer advocates to peddle their disinformation for them.

It is worth noting that on occasion disinformation campaigns may be conducted with benevolent, rather than destructive, intentions. For example, a government may exaggerate a health threat to try to improve citizens' safety and health. However, this book focuses on disinformation with negative intentions and outcomes.

A Few Useful Definitions (continued)

Malinformation is defined as information that is technically accurate but deliberately taken out of context, framed in a misleading way, or used inappropriately. Malinformers will often use elements of truth to confound fact-checkers and disarm their opponents. For example, a malinformer might assert that a food company's products contain chemicals associated with cancer, omitting the crucial detail that these chemicals are present in quantities far below the safety thresholds set by health authorities. (Note that, in this example, even if a fact-checker points out the omission, suspicions will linger among people who are already skeptical about food safety.)

Throughout this book, for the sake of brevity, the term *disinformation* will be used to mean "dis- and mal-information" as both represent the attempt to deliberately mislead.

Sometimes mis-, dis- and mal-information are collectively known by the acronym *MDM*. (For those in the technology world, this can be slightly confusing since the same acronym is also used for something completely different, that is Master Data Management.)

Industrial disinformation (IDI) is defined as the systematic, large-scale production and dissemination of false or misleading information funded by governments, industries, corporations, NGOs or powerful individuals, often to protect their interests, harm competitors, or manipulate public opinion and policy outcomes. Unlike the image of a hacker in a hoodie in their bedroom generating occasional untruths, this type of disinformation is typically well-funded and strategically executed, leveraging various media channels and platforms to reach a wide audience. Historical examples include efforts by certain industries to downplay scientific evidence about the harmful effects of their products, such as the tobacco industry's campaigns to cast doubt on the link between smoking and cancer, and fossil fuel companies' attempts to undermine the scientific consensus on climate change. While IDI has been around for over a century, the advanced version described in this book utilizes the latest technology, particularly generative AI, to deliver customized messages to individuals

A Few Useful Definitions (continued)

Generative AI (GenAI) describes technologies that can generate new, derived versions of content, strategies, designs and methods by learning from large repositories of original source content. A GenAI model trained on publicly available content can be customized (poisoned) by a disinformer to incorporate false information into its representation of the world. *Deepfakes* are a particular type of GenAI output that consists of very realistic images, video, or audio recordings that depict incidents that never happened or recognizable people doing or saying things they never did in a realistic manner. GenAI can also personalize experiences based on context and observations about individual users and their mental models.

Agentic AI refers to goal-driven software entities that have been granted rights by an organization or individual to act on their behalf by autonomously making decisions and taking action on its behalf. These entities use AI techniques, combined with components such as memory, planning, sensing, tooling, and guardrails, to complete tasks and achieve objectives. Unlike another term, robotic process automation (RPA), agentic AI doesn't require explicit inputs and doesn't produce predetermined outputs. In the context of disinformation, agentic AI could autonomously conduct narrative attacks on a target over a sustained period of time using a variety of media, adapting its tactics along the way without need for human oversight or intervention.

A ***mental model*** is a person's internal representation of external reality, consisting of a collection of assumptions about the way the world works in particular domains. People need mental models to make sense of the world and to achieve a stable relationship with it. However, although they are used as a navigational tool, they may not have a high degree of fidelity to reality. A mental model appears consistent to the person who has it even if it's incomplete, contains logical inconsistencies, or contradicts mental models they have in other domains. Mental models may be slow and painful to change, even when confronted with facts – a human quality that IDI producers rely upon.

Appendix 5 contains a more complete glossary of terms related to the various information disorders.

The World Economic Forum's 2025 Global Risks Report[1] survey of almost 1500 business, government, academic and other experts identified misinformation and disinformation as the top global risk, in terms of likely impact in the next two years. To put that in perspective, the next five risks that followed misinformation and disinformation were extreme weather events, societal polarization, cyber insecurity, interstate armed conflict and lack of economic opportunity. And these experts don't believe this will change appreciably any time soon. In that same survey, experts agreed that misinformation and disinformation will remain as one of the five top global risks for the next ten years.

Global Risks Ranked by Severity Over the Short Term

1st	**Misinformation and disinformation**
2nd	Extreme weather events
3rd	State-based armed conflict
4th	Societal polarization
5th	Cyber espionage and warfare
6th	Pollution
7th	Inequality
8th	Involuntary migration or displacement
9th	Geoeconomic confrontation
10th	Erosion of human rights and/or civic freedoms

n = "nearly 1,500 global experts" per report.

Q. "Please estimate the likely impact (severity) of the following risks over a 2-year [...] period."

Source: World Economic Forum Global Risks Perception Survey 2024-2025.

Figure 2. Global Risks Ranked by Severity of Impact

Other measures also suggest the world is facing a crisis. For instance, Google's nGram Viewer, which reveals word frequencies in printed materials, found that the use of misinformation and disinformation is now at its highest level in at least the past two centuries, and has been on a steep upward trajectory in the twenty-first century.

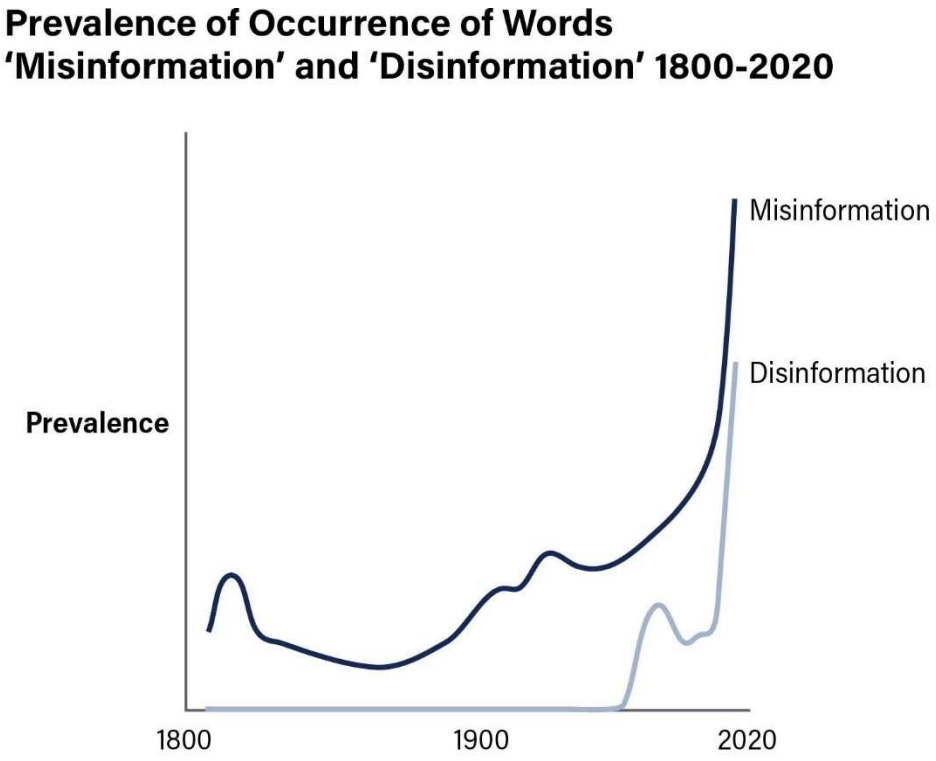
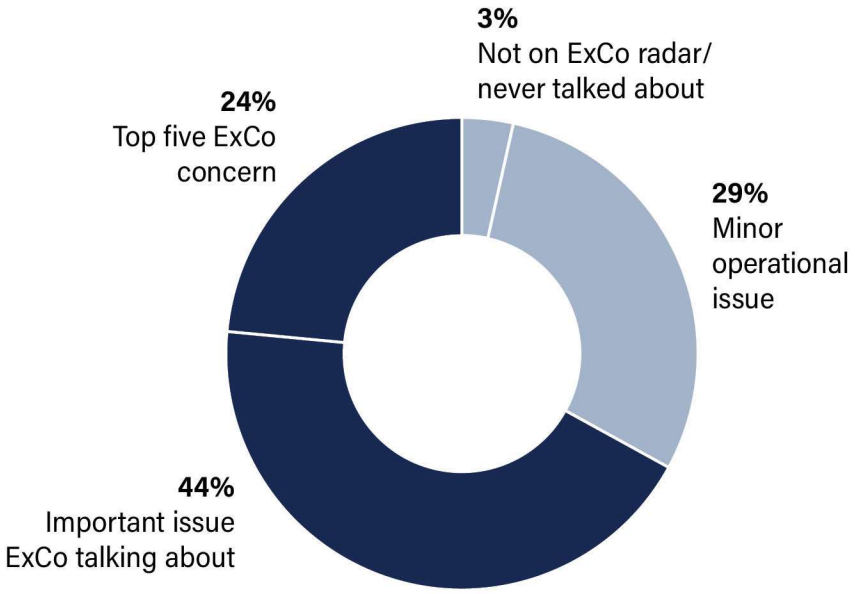


Figure 3. Prevalence of Occurrence of Words 'Misinformation' and 'Disinformation' 1800-2022

Executive leaders of organizations are becoming more and more sensitized to these issues and the need to address them. In a recent Gartner survey of 200 C-level leaders, 68% of them told us that misinformation, disinformation, and malinformation (MDM) was an important issue being talked about by their executive committees. Thirty percent said it was a top five concern for their executive committee. (Note: This survey will be referenced throughout the book. The survey is described in detail in Appendix 6.) With the increasing prevalence of AI, social networking and other digital technologies, these numbers are only likely to increase.

CxOs Are Talking About MDM in the Executive Committee

Executive committee viewpoint regarding mis/dis/mal Information (MDM)



n = 200 senior business and technology executives

Q. Please tell us which of the following most closely represents your executive committee viewpoint regarding Mis/Dis/Mal Information?
Source: 2025 Gartner Readiness for World Without Truth Survey

Figure 4. CxOs are Talking About MDM in the Executive Committee

What's driving these executives to talk about harmful information? Gartner asked in the same survey, and as you can see in Figure 5, the most important driver is whether the organization has already experienced these issues. Sixty-five percent were driven by having experienced MDM issues, and for thirty percent, this was the sole reason cited. Fifty eight percent said their executive committee was driven by market news about MDM, and thirty percent by the results of risk assessments.

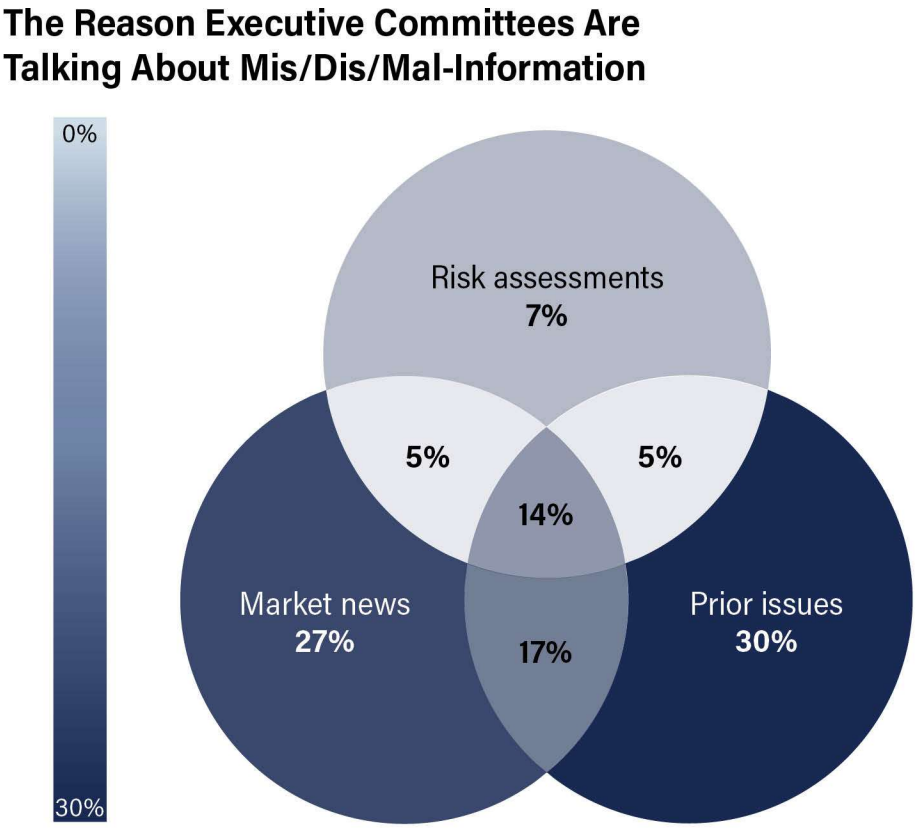


Figure 5. The Reason Executive Committees are Talking About MDM

But as aware and alarmed as organizations are already about the issue of misinformation and disinformation, they don't go far enough. The lack of reliable information needs to be seen as a *meta-issue* that compromises everyone's ability to understand and deal with all other issues. In a world without truth, how can society decide how big a concern climate change is, what its causes are, and how to address them? How can society address global health challenges?

And at the corporate level, how can companies maintain relationships with their customers, employees, investors, and other stakeholders in a world where people feel they can no longer believe what they read, see, or hear?

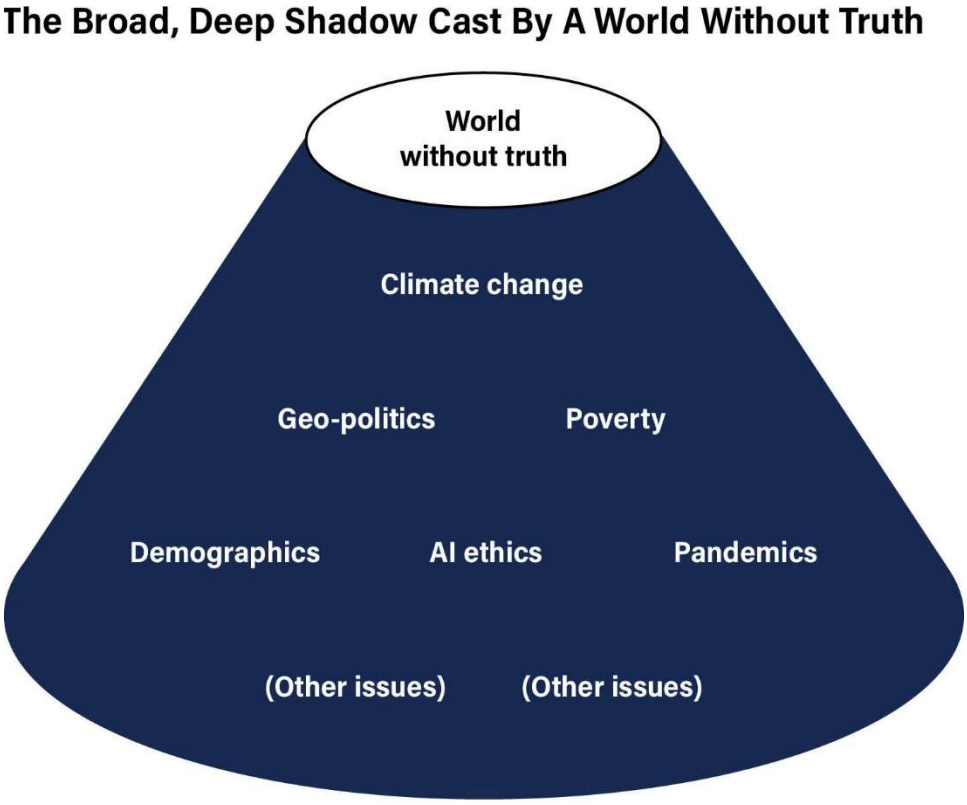


Figure 6. The Broad, Deep Shadow Cast by a World Without Truth

In retrospect, this escalation of disinformation seems inevitable. In 2002, one of the authors of this book, Richard Hunter, wrote *World Without Secrets: Business, Crime, and Privacy in the Age of Ubiquitous Computing*. He highlighted the effects of all information being available digitally, to anyone who wanted it badly enough. This book proved to be prescient, predicting many of the phenomena showing up today, such as *network armies* and the meteoric rise in importance of influencers. (Appendix 1 contains a summary of the findings and messages from *World Without Secrets*.)

Twenty-three years later, the digital world has democratized our ability to analyze data, target individuals and corporations, create fake content and disseminate it, all at scale and relatively low cost.

This book is about how today's digitally accelerated wave of misinformation and disinformation will challenge our world, and the steps companies need to take now to mitigate its reach and damage. The first half (chapters 1-6) describes the industrialization of disinformation, its emerging supply chain and the problems it causes. The second half (chapters 7-12) offers concrete steps organizations can take to combat it, in all its stages, on both organizational and societal levels. Each chapter includes a 30-second summary and key take-aways to allow busy executives to select which chapters to skim and which to read in detail.

Welcome to a *World Without Truth*.

Introduction Endnotes

[1] Elsner, M., Atkinson, G., & Zahidi, S. (2025, January 15). *Global risks report 2025.* World Economic Forum. Retrieved from https://www.weforum.org/publications/global-risks-report-2025

Chapter 1

Industrial Disinformation Threatens Truth and Trust

30-Second Summary

The digital world has massively expanded our ability to create and distribute information. Distressingly, a growing share of this information is harmful. The power of digital dis- and malinformation to influence public behavior has given rise to an entire industry dedicated to its production and spread. This industry, which operates under the protection of free speech laws in liberal democracies, victimizes businesses with direct losses and indirect corruption of markets. As breakthroughs in AI enable powerful new strains of harmful information, the problem will rapidly worsen if left unaddressed.

In 2019, the CEO of a UK energy firm picked up the phone. His boss, the CEO of his firm's German parent company, was on the line, asking him to transfer €220,000 (over US $240,000) to a Hungarian supplier. Only later would he learn that the voice didn't belong to his boss and the bank account did not belong to their supplier. He had been scammed, the victim of the world's first reported AI-generated deepfake frauds.

Fast forward to early 2024. On a video conference call with a number of senior officers of Arup, the global engineering and design firm, a member of the finance staff in Hong Kong was asked to transfer HK$ 200 million (about US $25 million)—only to learn later that all the other participants on the call were digital fakes.[1]

From $240k to $25 million, from fake audio to fake videoconferencing—all in just five years. What next? Almost certainly much more, and much worse.

Estimates of the rising cost of digital disinformation vary, but they all point to very large numbers. Consider the following:

- In 2019, a study by University of Baltimore Economist Professor Roberto Cavazos and AI and cybersecurity company CHEQ estimated the economic damage caused by digital mis- and dis- information to be $78 billion.[2] This included $49 billion in stock market losses, $17 billion in financial misinformation, $9.5 billion related to reputation management, $9 billion from health misinformation, and $3 billion in online platform safety. This was before the introduction of ChatGPT in November 2022, and the subsequent explosion and democratization of generative AI capabilities.

- A 2021 study by Johns Hopkins Center for Health Security estimated that after vaccines were available in May 2021, the economic costs arising from people refusing vaccination in the US because of misinformation and disinformation were between $30 and $500 million per day[3] from May to October 2021. This was based on the cost of hospitalizations, the valuation of lives lost and long-term morbidity due to COVID-19. The higher end of that range translates to an annualized rate of $180 billion.

- Gartner predicts that by 2028, enterprise spend on battling misinformation and disinformation will surpass $30 billion, cannibalizing 10% of marketing and cybersecurity budgets to combat a multifront threat.[4]

- Markets estimate that the deepfake AI market will grow more than 40% compound annual growth rate from $564m in 2024 to $5.1billion in 2030.[5]

All of this points to mis-, dis- and mal-information representing roughly a trillion dollar problem for the global economy. And of course, the damage done by disinformation is not only financial. Bad information can result in loss of quality of life, health and life itself.

Even history is not safe from digital disinformation. Consider an experiment conjured up with the GenAI image generator Midjourney and posted on a Reddit thread: a collection of realistic images of an imaginary plague of blue flowers that supposedly blanketed the Soviet Union in the 1970s.

It was relatively easy to create. In one Reddit post, the developer explained how they made the *Blue Plague* images by prompting Midjourney, a generative AI graphics tool, with a 140-word description detailing the context and photographic specifications of the desired content. Why stop there?

Since the Blue Plague experiment, high quality AI-generated video has become more commonplace. Today, the same creator could conjure up videos of the Blue Plague, reported by famous TV newsreaders from the 1970s. Then, the creator could instruct AI-powered agents (so-called *agentic AI*) to create thousands of fake news articles on fake news websites, all talking about the blue plague, and all linked to and corroborating each other.

For good and ill, the authors expect to see many such ongoing advances in quality, range of media channels incorporated, and degree of personalization – not to mention the size of the prize for a successful impersonation.

Progress in Technologies Favors Disinformation

Put simply, the digital world, including AI, accelerates the challenge of disinformation exponentially in multiple directions.

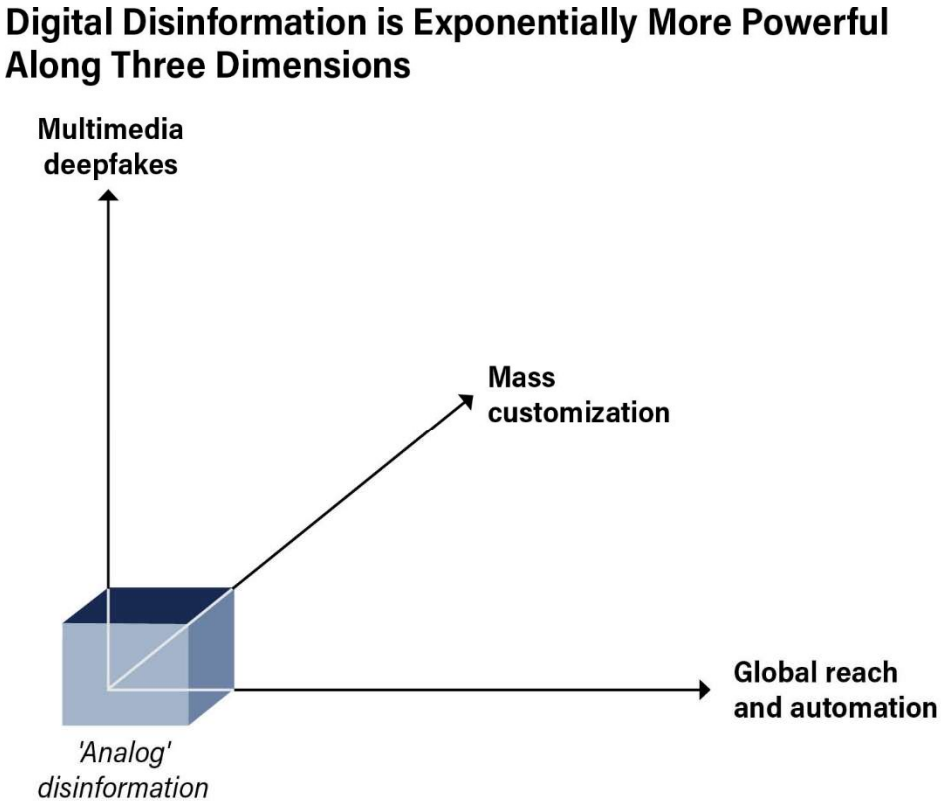


Figure 7. Digital Disinformation is Exponentially More Powerful Along Three Dimensions

- First, generative AI powers the creation of more and more convincing deepfake texts, audio, video, or any other content.
- Second, data, analytics and machine learning allow content and dialogs to be customized for each target, based on learned inferences about their habits, hopes, fears, dreams, worldviews and preferences. Widespread ability to conduct mass customized disinformation campaigns.
- Third, digital channels have made it extremely cheap and easy to engage almost anyone on earth with very high frequencies of contact. Agentic AI is now making it possible to automate the use of those channels to build narratives across media and over time.

Right or Wrong, Mental Models Carry the Day

What makes these advances frightening is that their target – the human mind – has not changed. Humans still navigate through life using mental models that are often grounded in a blend of fantasy and fact.

Mental models are internal representations that individuals use to reason and make sense of the world.[6] They influence how people interpret information, make decisions, and interact with others. What makes the emerging strain of disinformation techniques especially dangerous is their ability to exploit weaknesses in people's mental models of reality, which often rest on inaccurate or incoherent beliefs. Such models are shaped continuously over time, making them ideal targets for conversational AI agents. These talking bots can generate increasingly immersive and compelling content – not just fake board meetings, as noted above, but even fake speeches.

Advances in natural language processing and generative AI now make it possible for bots to:

- Present human-like expressions of emotion, context and understanding to engender empathy and trust, even where it's unwarranted.
- Draw out people's motivations and shape their mental models at scale.
- Make timing, channel and content decisions for media campaigns based on real-time feedback.

Apps that can be used to create these kinds of fakes are now readily available. Deepfakes Web β, a Web service, can construct deepfake videos in a few hours. Wombo is an app that takes a face you provide and lip syncs singing. Reface and Jiggy allow you to apply your face to gif memes. MyHeritage's Deep Nostalgia feature allows animation of old photos. DeepFaceLab is a PC-based tool. Face Swap allows the user to 'swap faces' with their friends. Apps like these will come and go, and get ever more sophisticated.

Most of these use techniques that are relatively easy to recognize. Providers such as Amped Software, Cognitech, DuckDuckGoose, Google, Intel, Reality Defender, Sensity, and Sumsub offer products designed to detect deepfakes and other forms of synthetic disinformation. Ultimately, however, the game is tilted in favor of fakers with access to more sophisticated technology and skills, and less need to conform to laws and regulations. Open-source models and fine-tuning techniques available to dedicated developer communities provide capabilities to produce assets almost impossible to distinguish from authentic content. GitHub, Stability AI, HuggingFace, and civit.ai are enabling thousands of developers to hone these skills and tools.

Distrust Is on the Rise

One reason to be confident that the damage caused by deepfakes will continue to grow is that even as the production values of fakery rise, the height of the bar needed to sow doubt continues to decline. Over the past decade, society's level of trust in organizations has plummeted, a phenomenon RAND analysts Jennifer Kavanagh and Michael D. Rich have dubbed *truth decay*.[7] A 2024 Gallup study of Americans' trust in various institutions concluded that:

> "*The United States continues to suffer from a crisis in confidence in many institutions, including the federal government, its three branches, and those who either hold or are running for public office. In addition, trust in the fourth estate – the mass news media – is at a new low. Local and state governments and the American people as a whole are the only entities garnering trust from more than half of US adults.*"[8]

People are aware this is happening. A majority in 15 of 26 countries agree that their country is more divided than in the past. Sixty-two percent agree "the social fabric that once held this country together has grown too weak to serve as a foundation for unity and common purpose" and 65% agree "*The lack of civility and mutual respect today is the worst I have ever seen.*" [9]

Declining trust doesn't just apply to media and government. Gartner research indicates that brands as well have experienced a sharp decline in trust since 2021.

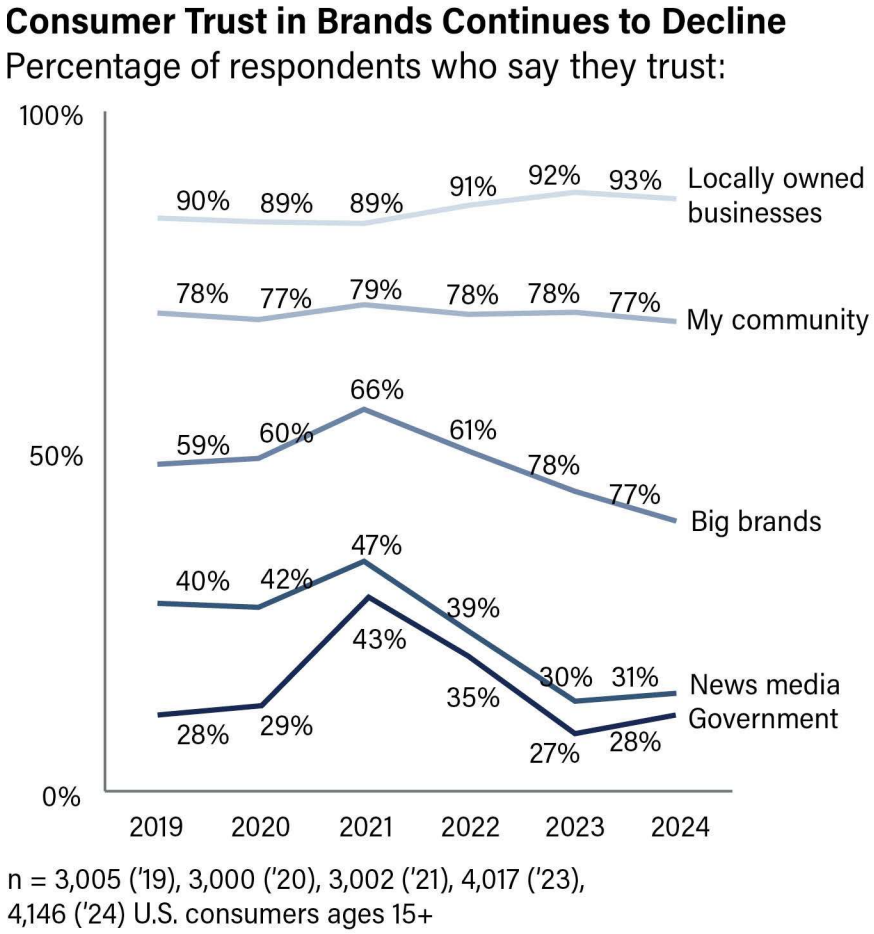
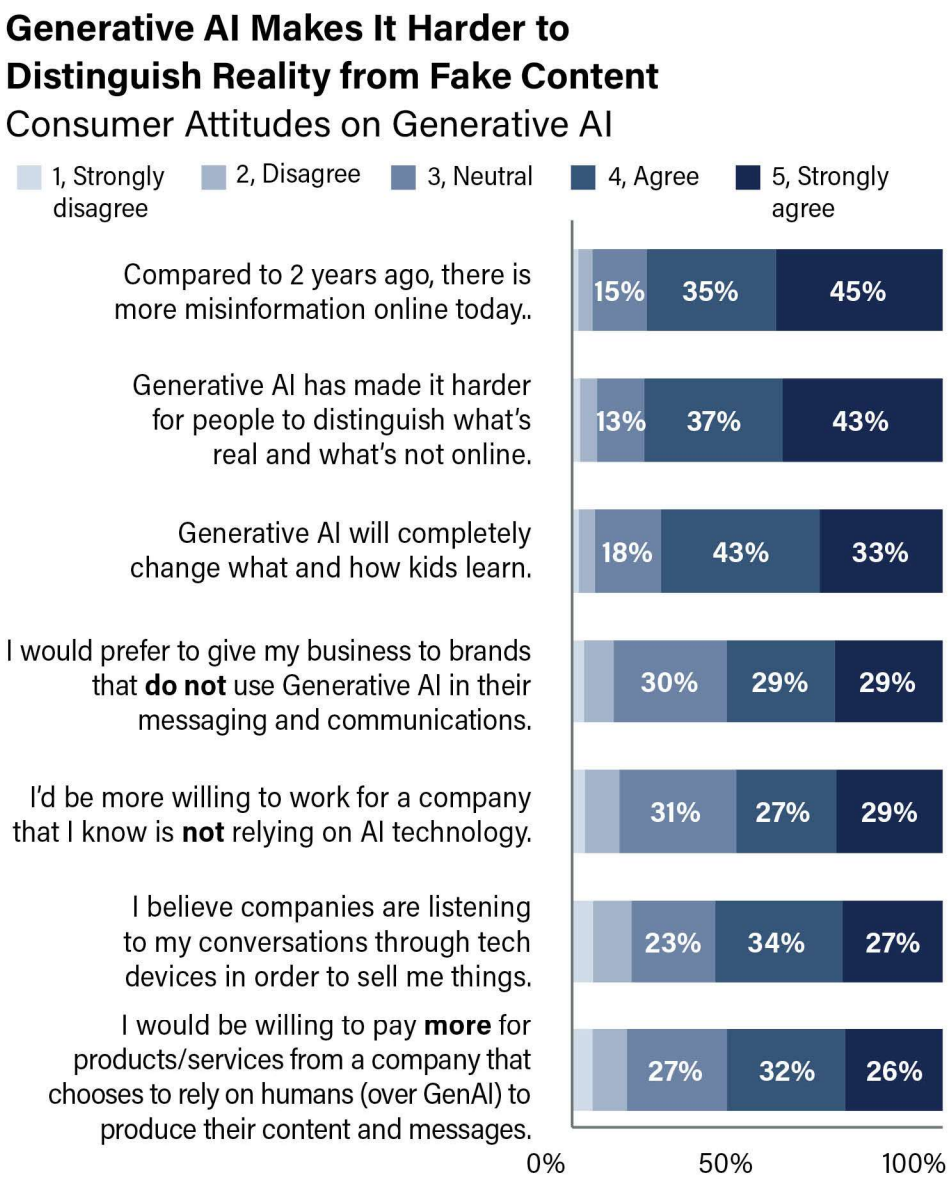


Figure 8. Consumer Trust in Brands Continues to Decline

Kavanagh and Rich argue that the public feels increasingly skeptical about the reliability of facts and analytical interpretation of facts and data. The situation is exacerbated by a blurring of the lines between opinion and fact, increasing volume (and corresponding influence) of accounts of personal experiences and opinions over fact in the media, and declining belief in formerly respected sources of information. Why else is trust declining? Consumers blame Generative AI.



n = 2,001 U.S. Consumers age 18+.

Q. GEN_AI_2. How much do you agree with each of the following statements?
Source: 2024 Gartner Consumer Omnibus Survey
Note: percentage less than 5% is not shown

Figure 9. Generative AI Makes It Harder to Distinguish Reality from Fake Content

Skepticism in the face of a torrent of unreliable stories and images might seem like a good thing, but the result tends to be that people choose those stories that best align with their prior prejudices—or the stories are chosen for them.

> "*Mental models are more powerful than facts*," said Viktor *Mayer-Schönberger, a professor of Internet Governance and Regulation at the Oxford Internet Institute. "Facts alone don't tell you much. You have to contextualize facts with mental models to create meaning. Mental models are incredibly persistent*."

It's not only stubbornness that makes us this way. Psychologists also point to a cognitive bias called the Dunning-Kruger effect: a tendency to overestimate your knowledge of a topic, particularly when your knowledge is sparse. As society continues to confront more complex challenges, this effect contributes to the likelihood that our mental models will fail to assess the true nature of issues that threaten us.

Sticking with an inaccurate mental model can have serious consequences. You may think you hear your boss on the telephone and on that voice's instructions, send millions of dollars to a con-artist's account. Or worse, your customers may read a fake news report that fits with something they thought they knew about your organization. Worst of all, some of your relatives may see a lecture on YouTube that reinforces a false idea they have about vaccines, to the detriment of their health and the health of millions of others—a phenomenon of the COVID-19 pandemic.

Mayer-Schönberger warns that the risks posed by inaccurate mental models will only continue to grow as the technology improves. "*The more immersive nature of the digital world makes us even more vulnerable…the idea that a significant portion of some people's time may be spent in synthetic environments amplifies the dangers of mental model manipulation*," he said.

Opinion Dynamics Describes How Disinformation Spreads

In addition to being a good way to influence mental models, social media and other digital platforms have given social scientists a tremendous new resource for understanding how opinions form, evolve, and spread. Over the past few decades, the study of opinion dynamics emerged as a pivotal

area of research, merging insights from social psychology, computational modeling, and network theory.

One key insight has been a theory called the *Bounded Confidence Model (BCM)*.[10] The BCM posits that individuals are influenced only by others whose opinions fall within a certain "confidence bound" or threshold of similarity to their own.

Individuals with rigid mental models may have narrow confidence bounds, making them less susceptible to external influence and more prone to polarization.

The BCM and its variants have been instrumental in simulating the conditions under which consensus, polarization, or fragmentation occur within a population. They aid in understanding, predicting, and controlling how social media activities shape opinions in social media environments. Researchers have found that algorithmic filtering and user-driven content curation reinforce existing mental models, leading to the formation of *echo chambers* where like-minded individuals congregate and further polarize each other's beliefs and related behaviors.

Empirical Validation: Twitter Firehose Data and Social Media Dynamics

These insights have been applied to a variety of real-life cases regarding the spread of misinformation. In 2016 Alessandro Bessi and Emilio Ferrara, researchers at the University of Southern California, utilized Twitter data to analyze the spread of misinformation during the 2016 US presidential election.[11] Their study highlighted how disinformation could spread rapidly through retweet networks, often bypassing traditional media gatekeepers. It also detailed the effects of bots on social media dynamics, estimating that about 400,000 bots had engaged in the political discussion leading up to the Presidential election. They were responsible for roughly 3.8 million tweets, about one-fifth of the entire conversation hosted by Twitter.

Bessi and Ferrara's work demonstrated how social media platforms, by design, amplify certain types of content through algorithms that prioritize engagement. Research by Vosoughi, Roy, and Aral demonstrated that false news spreads more rapidly on Twitter than true news, largely due to its

novelty and emotional appeal.[12] This finding aligns with theoretical predictions from opinion dynamics models, which suggest that novel information can break through bounded confidence thresholds, especially when it resonates with pre-existing biases. This helps explain the prevalence of conspiracy theories in social networks, as they're often the basis for the disproportionate spread of emotionally charged or novel information.

Leveraging Opinion Dynamics for Disinformation

Producers of disinformation exploit the mechanisms of opinion dynamics to achieve their goals. Disinformation campaigns often target specific segments of the population with tailored messages designed to reinforce existing beliefs and exploit mental models. By applying the principles of bounded confidence and mental models, they can craft messages that are more likely to penetrate their target audiences' cognitive defenses, increasing the likelihood of acceptance and dissemination.

Industrial Disinformation Exploits and Inflames Culture Wars

Bounded confidence and mental models also help explain social media's amplification of culture wars: the deep ideological and political conflicts that are polarizing communities, especially in the US and Europe. Cultural values and beliefs form the core of people's identities, so it follows that disinformers seek motivation by appealing to a targeted social group's most fundamental principles while describing how they're being violated by other groups in shocking and outrageous ways. Reinforcing core beliefs is not enough: to motivate action, disinformation needs to position an adversary as an existential threat to those beliefs, sparking outrage to reinforce ideological divisions and create visceral associations.

Figure 10 from Edelman's Trust Barometer shows how stark this has become among people who feel strongly about issues.

Figure 10. Ideology Becomes Identity

Communication specialists know that what matters most to people are not facts but emotional resonance. Since people are most likely to share and engage with information that triggers strong emotions and confirms their mental models, disinformers embed false claims in an emotional narrative that describes a threat to the target group's sense of identity, including religion, race, sexuality, security, heritage and sense of community.

This means that regardless of a company's size, market, or lack of any political affiliation, it must be prepared to hold back substantial subgroups of a globally polarized society that disinformers are adept at mobilizing against it for any grievance. Companies can be caught off-guard when a campaign uses polarization to escalate a small, concocted political association into an existential threat.

Consider two examples, one where agents mobilized the political right against a small target, and another which mobilized the political left against a much larger one.

Backed by major venture capital funds, Beyond Meat and Impossible Foods were the leaders of an emerging industry of plant-based products that mimic the taste, texture, and nutritional value of meat, without the environmental and ethical impact.

As with many other industrial disinformation campaigns, the campaign against them was funded by a business sector that felt threatened by an innovation. In this case, the livestock industry saw synthetic meat makers as a potential threat to their industry, so they reportedly enlisted the help of groups like Berman & Company's Center for Consumer Freedom (CCF, now known as the Center for Organizational Research and Education, or CORE) and The CLEAR Center of the University of California at Davis.[13]

These organizations took on synthetic meat with a three-pronged attack.

First, they raised apparently legitimate concerns about the quantity and safety of synthetic ingredients and processing that went into producing these foods. CCF spent over $5 million to run a 2020 Super Bowl ad highlighting and mocking their chemical composition and ran full-page ads in The New York Times and Wall Street Journal, claiming "*fake meats*" are full of "*real chemicals*."[14] One ad asked, "Should Fake Meat Have a Cancer Warning?"[15] despite lack of evidence of a link with cancer. Mainstream media outlets such as Bloomberg, Forbes, and the Guardian eventually picked up this narrative and began publishing articles questioning the health and viability of these products.

Second, the anti-synthetic group fostered visceral revulsion by comparing the products to dog food and eating bugs. CCF ran a series of "*Fake Meat or Dog Food?*" ads in prominent newspapers while CLEAR began circulating quizzes comparing Beyond and Impossible burgers to dog food.

Third, they played the culture wars card by linking the industry to toxic themes of elitist conspiracies and threats to traditional masculinity and freedom. CCF blogged that people like Bill Gates were trying to get you to eat bugs and shift away from all-American meat consumption for their own profit making.[16]

Beyond Meat's stock price dropped from $178 in January 2021 to around $3.50 in July 2025. Its CEO, Ethan Brown, initially took a relatively passive approach to responding to attacks but has recently stepped up the company's efforts to promote a stronger counternarrative. The company has cited health studies affirming its claims of health[17], launched product

upgrades and leaned into environmental benefits.[18] Time will tell if these efforts are effective.

While politically right-oriented attacks frequently rely on cultural caricatures and *dog whistle*[19] associations, left-oriented attacks are often more specifically cause-related and directed at corporate practices. One of the most prominent corporate antagonists is the Boycott, Divestment and Sanctions Movement (BDS), which has launched impactful boycotts of major brands, including Coca-Cola, Intel, McDonald's, Starbucks and others based on their perceived support for Israel's role in the conflict in Gaza. Whatever share of their business involves Israel, BDS accuses these brands of "supporting genocide," and complicity in war crimes. Their campaigns have had "meaningful business impact", in the words of McDonald's CEO.

Large companies tend to respond with curt public statements labeling these attacks as "*disinformation*", "*misrepresentation*" and "*misperceptions*", and certain inflammatory claims have been debunked by independent fact-checkers. For example, after a McDonald's franchisee in Israel announced in October 2023 that it would be donating free meals to the Israeli army, McDonald's attempted to distance itself from the move on social media by pointing out that the decision was made independently by a local licensee and asserting its neutrality on the issue. In March 2024, fake customer notice stickers were seen in the windows of McDonald's restaurants in Glasgow suggesting the brand was congratulating the Israeli military for killing civilians in Gaza. The posters were debunked in April 2024, by Reuters which identified an activist group called "*Art Workers For Palestine Scotland*" claiming credit on Instagram. Reuters quoted a McDonald's executive: "*We are dismayed by the disinformation and inaccurate reports regarding our position in response to the conflict in the Middle East. McDonald's Corporation is not funding or supporting any governments involved in this conflict*."[20]

The posters were fake but the passions they stirred were real. Such activism has led to substantive changes in business operations, such as McDonald's decision to buy out its Israeli franchisees. The danger of polarized political mobilization to organizations warrants defensive preparations beyond assertions of political neutrality.

The Best Defense

Opinion dynamics research reveals how any brand or organization can be attacked from either side by a motivated detractor, regardless of its stated position on any specific issue or value. If a brand emphasizes sustainability or diversity and inclusion in its products, a right-flank attack will tag the brand as infected with the *woke virus* while a left-flank one frames the claims as hypocritical *virtue-signaling*. If the brand opts for neutrality and distances itself from any position on a charged issue, the right-flank detractor suggests the brand is hiding its true affiliations and nefarious connections while the left-biased one spotlights its omissions as complicit.

From a communication perspective, BCM suggests that it is generally more effective to shift the narrative toward exposing attack groups and raising questions about their motives, tactics and affiliations than to focus on refuting their claims. Impeaching the source redirects an individual's suspicion back on the motives of the originator.

Addressing the World Without Truth is a Prerequisite to Addressing Other Critical Issues

Disinformation may not seem as urgent and scary to businesses as a product recall or a major lawsuit. But deceptive communication makes it harder for us to agree on how to solve issues and even makes us question whether they are problems at all. This applies to both global problems such as pandemics or climate change, and corporate issues such as shifts in demand or competition.

When it comes to our understanding of many crucial issues, reality continues to outpace our mental models. Take global warming, for example. In July 2023 the world endured its highest temperatures in 125,000 years. In the first week of June 2024 temperatures in Delhi reached 52.2 degrees Celsius (126 degrees F).[21] There is good reason to believe that temperatures will go higher as the processes that took the climate to this point continue. But before it can address that reality, society will have to acknowledge the validity and severity of the issue, and that will only be possible once disinformation has been brought under control.

The next chapter looks at the Industrial Disinformation supply chain to understand how deliberate half-truths and outright lies are being

conveyed in ways calculated to persuade us individually and yet at scale, to our collective harm.

Key Takeaways

- **Deepfake fraud is rapidly evolving.** The progression from early deepfake scams in 2019 to sophisticated video-based frauds in 2024 illustrates the rapid advancement and increasing threat of AI-generated disinformation.
- **Economic impact of disinformation is massive.** Disinformation's economic toll is substantial, with studies pointing to a trillion dollar problem to the global economy. As dire as this seems, the greater impact of devolving into society that lacks any ability to trust in the integrity of information is incalculable.
- **Mental models are exploited by disinformation.** Disinformation campaigns target human mental models, which are often based on a mix of fact and fantasy. They increasingly use AI to manipulate perceptions and reinforce biases, making individuals more susceptible to false narratives.
- **Trust in institutions is declining.** The phenomenon of truth decay describes how public trust in institutions and media is eroding, making societies more vulnerable to disinformation and complicating efforts to address critical global issues like climate change.
- **Commercial disinformation exploits culture wars.** Disinformation campaigns often politicize messages for impact, even when their donors' motives are commercial. Innovative businesses and non-profits that challenge large, established markets are especially vulnerable.

Chapter 1 Endnotes

[1] The Guardian. (2024, May 17). *UK engineering firm Arup hit by £20m deepfake scam in Hong Kong*. Retrieved from https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video

[2] Cavazos, R., & CHEQ. (2019). *The economic cost of bad actors: Influencers.* Retrieved from https://info.cheq.ai/hubfs/Research/THE_ECONOMIC_COST_OF_BAD_ACTORS_Influencers.pdf

[3] Johns Hopkins Center for Health Security. (2021, October 20). *Misinformation and disinformation in the COVID-19 pandemic: The economic cost.* Retrieved from https://centerforhealthsecurity.org/sites/default/files/2023-02/20211020-misinformation-disinformation-cost.pdf

[4] Gartner. (2023, November 23). *Gartner's top strategic predictions for 2024 and beyond – Living with the year everything changed.* Retrieved from https://www.gartner.com/document-reader/document/4964231

[5] MarketsandMarkets. (2024). *Deepfake AI market report.* Retrieved from https://www.marketsandmarkets.com/Market-Reports/deepfake-ai-market-256823035.html

[6] Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference, and consciousness.* Harvard University Press.

[7] Kavanagh, J., & Rich, M. D. (2018). *Truth decay: An initial exploration of the diminishing role of facts and analysis in American public life.* RAND Corporation. Retrieved from

https://www.rand.org/pubs/research_reports/RR2314.html

[8] Gallup. (2024). *Americans' trust in media remains at trend low.* Retrieved from https://news.gallup.com/poll/651977/americans-trust-media-remains-trend-low.aspx

[9] Edelman. (2023, March). *2023 Edelman trust barometer global report.* Retrieved from https://www.edelman.com/trust/2023/trust-barometer

[10] Deffuant, G., Neau, D., Amblard, F., & Weisbuch, G. (2000). *Mixing beliefs among interacting agents*. Advances in Complex Systems, *3*(01n04), 87–98. https://doi.org/10.1142/S0219525900000078

[11] Bessi, A., & Ferrara, E. (2016). *Social bots distort the 2016 US presidential election online discussion*. First Monday, 21(9). Retrieved from

https://firstmonday.org/ojs/index.php/fm/article/view/7090/5653

[12] Vosoughi, S., Roy, D., & Aral, S. (2018). *The spread of true and false news online*. Science, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

[13] Changing Markets Foundation. (2024, January). *Truth, lies and culture wars: The industrial disinformation campaign against plant-based foods.* Retrieved from https://changingmarkets.org/wp-content/uploads/2024/01/Truth-lies-and-culture-wars-final.pdf; Changing Markets Foundation. (2024, February). *What do the meat industry, far-right and major internet conspiracy theories have in common?*, Changing Markets Foundation. Retrieved from https://changingmarkets.org/op-ed-what-do-the-meat-industry-far-right-and-major-internet-conspiracy-theories-have-in-common/

[14] Center for Consumer Freedom. (2019 October). *Ad: What's Hiding Inside Plant-Based Meat*. Retrieved from https://consumerfreedom.com/2019/10/ad-whats-hiding-inside-plant-based-meat/

[15] MDPI. (2024). *Sustainability.* Retrieved from https://www.mdpi.com/2071-1050/16/11/4457

[16] Center for Consumer Freedom. (2021, February). *Bill Gates wants you to eat ultra-processed goop.* Retrieved from

https://consumerfreedom.com/2021/02/bill-gates-wants-you-to-eat-ultra-processed-goop/

[17] Stanford University Medicine. (2024). *SWAP-MEAT study.* Retrieved from https://med.stanford.edu/nutrition/research/completed-studies/SWAPMEATstudy.html

[18] WIRED. (2024, December 26). *Beyond Meat says being attacked has just made it stronger.* Retrieved from https://www.wired.com/story/beyond-meat-hits-back-against-the-haters-ethan-brown/

[19] A "dog whistle" refers to language that seems to have one meaning to the general public but holds a different meaning for some audiences.

[20] Reuters. (2024, April 3). *McDonald's did not congratulate Israeli military over Gaza killings.* Retrieved from https://www.reuters.com/fact-check/mcdonalds-did-not-congratulate-israeli-military-over-gaza-killings-2024-04-03

[21] Ray, S. (2024, May 29). *Delhi hits record 126 F degrees as extreme heat wave envelops North India.* Forbes. Retrieved from https://www.forbes.com/sites/siladityaray/2024/05/29/delhi-hits-record-126-f-degrees-as-extreme-heat-wave-envelops-north-india

Acknowledgements

This book is about a sensitive, complex, fast-moving topic that touches on many disciplines from the philosophical aspects of truth and trust in society, the strategies and stratagems of bad actors, the increasing reach of social media, artificial intelligence and other technologies, to governance and risk management practices.

The authors wish to acknowledge the fantastic input from, review by, and dialog with all of our colleagues at Gartner. Amongst them, **Leigh McMullen** was paramount in shaping this book project and some of its core ideas in the early stages.

Tom Turcan who has championed this project since its inception.

Chris Howard, Anthony Bradley and Julie Hopkins have been our trusted management sponsors at Gartner, providing research leadership and executive support.

Ben Voyles provided artful and thorough editing and writing support.

Marta La Torre provided project management and kept us on track.

Walter Baumann, Divya Malkani, Nicole Daniels, and Caroline Holloway provided amazing visualizations and great graphics support.

Expert reviewers and advisors: Many other colleagues that provided great thought leadership, collaboration and review, including: Patryck Allen, Dan Ayoub, Rachel Bernstein, Carsten Casper, Geoffrey Campen, Dorian Cundick, Emily Earl, David Furlonger, Nicole Green, Jonathan Grieb, Apeksha Kaushik, Akif Khan, Avivah Litan, Carl Manion, Owen Pengelly, Brian Prentice, Alfredo Ramirez IV, Errol Rasit, Mark Raskino, Don Scheibenreif, David Senf, Svetlana Sicular, Jake Sorofman, Darin Stewart, Daniel Sun and Bart Willemsen.

Primary research: The team that conducted the World Without Truth survey referenced within were lightning fast, delivered high quality outputs and were super responsive to our requests, led by Angela Krieter,

Nandita Stuxrud, and Gunveen Kaur Kohli. Support for the use of other Gartner surveys was provided by our Primary Research & Insights Team.

The authors would also like to thank our interviewees who gave generously of their time and insight:

- **Emily Bell**, Director Tow Center for Digital Journalism, Columbia Journalism School, non-executive director of the Scott Trust, the ownership body of the Guardian and the Chair of the Global Advisory Council on Social Media for the World Economic Forum.
- **Christopher Graves**, Founder of The Resonance Code, LLC, former President and Founder of the Ogilvy Center for Behavioral Science and former Global CEO & Chairman of Ogilvy Public Relations.
- **Dr. Mark Lee Hunter**, Adjunct Professor and Senior Research Fellow at INSEAD and founding member of the Global Investigative Journalism Network.
- **Viktor Mayer-Schönberger**, Professor of Internet Governance and Regulation at the Oxford Internet Institute.

Finally, the authors would like to acknowledge the continuous and tireless support of our families, without which we could not have written the book.

TRANSPARENCY NOTE: AI was used in the writing of this book. It was used only to suggest chapter summaries and enhance readability.

About the Authors

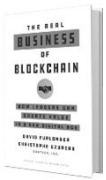
Dave Aron is a Distinguished Vice President Analyst and Gartner Fellow in Gartner's Emerging Technologies and Trends Group. He is a thought leader on digital business strategy, helping boards and CXOs understand and engage with advanced business and technology topics such as generative artificial intelligence, the world without truth, antifragility, and simplification. He has taught at London Business School and Oxford University's Said Business School, and has written two books, *The Essence of Strategy* (self-published, 2016) and *Understanding IT- a Manager's Guide* (with Jeffrey L. Sampler, FT Prentice Hall, 2003). Dave studied Computer Science at Queen Mary College, London, and earned an MBA at London Business School. Outside of work, Dave continues a lifelong passion for the countries and cultures of East and Southeast Asia, including the game of Go.

Andrew Frank is a Distinguished Vice President Analyst and Gartner Fellow in Gartner's Business Services Group. He focuses on applications of emerging marketing technology and trends, including adoption of generative AI and AI agents for content creation, advertising and customer experience. He has spent more than 30 years focusing on technology-driven innovation for major media companies, ad agencies, consumer brands and startups. He has authored articles in numerous trade publications, including the Harvard Business Review and Forbes. Andrew attended Wesleyan University and studied Artificial Intelligence as a postgraduate student at Columbia University. Outside of work, Andrew enjoys composing and performing music and designing computer games, which he did professionally early in his career.

Richard Hunter recently retired from Gartner where he was a Distinguished Vice President Analyst and Gartner Fellow in Gartner's CEO Research Group. His work has focused on issues that include digital business risk and the value of IT. Richard is the author of the acclaimed books *World Without Secrets* (Wiley, New York, 2002), IT Risk (with George Westerman, Harvard Business Press, Boston, 2007) and "The Real Business of IT" (with George Westerman, Harvard Business Press, October 2009). Before Gartner, Richard worked for more than a decade in data and information roles in the financial services industry. He is also a world-renowned harmonica player whose credits include authorship of the world's best-selling method for jazz and rock harmonica players. He studied music at Harvard University.

Other Gartner Books

When Machines Become Customers
AI-enabled Non-human Customers Are Coming To Your Business
Don Scheibenreif and Mark Raskino
Gartner, Inc., 3rd Edition August 2025



The Real Business of Blockchain
How Leaders Can Create Value in a New Digital Age
David Furlonger and Christophe Uzureau
Harvard Business Review Press, October 2019

The Connector Manager:
Why Some Leaders Build Exceptional Talent - and Others Don't
Jaime Roca and Sari Wild
Portfolio, September 2019

Infonomics
How to Monetize, Manage, & Measure Information as an Asset for Competitive Advantage
Doug Laney
Routledge, September 2017

Digital to the Core
Remastering Leadership for Your Industry, Your Enterprise and Yourself
Mark Raskino and Graham Waller
Routledge, October 2015

World Without Secrets
Business, Crime, and Privacy in the Age of Ubiquitous Computing.
Richard S. Hunter
Wiley 2002