INTELLIGENCE · ANALYSIS AND TRADECRAFT

"Deception and Disinformation: Counter-Narratives in Knowledge Generation"

Deception and disinformation are deliberate attempts to make others believe what is false. This article explains how deception works, why analysts and the public are vulnerable to it, how false information spreads online and what research shows about detecting and countering it.

ModQu research article · 2,827 words · 25 references (APA 7th edition)

Most errors in intelligence are honest: the evidence is incomplete, or the analyst misreads it. Deception is different. It is a deliberate effort by someone else to make the analyst believe something false. Disinformation extends the same effort to whole populations, using media and social networks to spread false or misleading stories. Both are as old as conflict and commerce, but digital communication has made disinformation cheaper, faster and harder to trace.

For any organisation that generates knowledge, whether an intelligence agency, a newsroom, a research firm or a company's insights team, deception poses a particular threat. It attacks the evidence on which judgements are built. This article explains how deception works, why people are vulnerable to it, how disinformation spreads, and what research shows about detecting and countering it, including the use of counter-narratives.

Defining the terms

Wardle and Derakhshan (2017), in a report for the Council of Europe, proposed a widely used framework for what they called **information disorder**. They distinguish three types:

- **Misinformation**: false information shared without intent to harm, for example a mistaken rumour passed on in good faith.
- **Disinformation**: false information knowingly created or shared to cause harm or gain advantage.
- **Malinformation**: genuine information shared to cause harm, such as leaked private documents released to damage someone.

The distinction matters because the response differs. Misinformation can often be corrected by better information. Disinformation involves an adversary who will adapt to corrections. Malinformation cannot be corrected at all, because it is true; the issue is how and why it is being used.

Deception, in the intelligence sense, is broader than disinformation. It includes any effort to mislead an opponent's perception, whether by spreading false stories, hiding real activities or staging false ones. Godson and Wirtz (2002) use the combined term **denial and deception**: denial prevents an opponent from learning the truth, while deception induces it to believe something false.

How deception works

Barton Whaley, who devoted a career to the study of deception, argued that every deception has two parts: hiding the real and showing the false (Whaley, 1982). Whaley identified three ways of hiding and three ways of showing.

Whaley's six methods of deception

Every deception hides something real and shows something false

Hiding the real	Example	Showing the false	Example
Masking	Concealing a product in development	Mimicking	Copying a rival's packaging
Repackaging	Calling a price rise a "new format"	Inventing	Fake reviews or a fabricated report
Dazzling	Burying a key change in a long filing	Decoying	Announcing a project to draw attention away

Based on Whaley (1982); table by ModQu with illustrative business examples

ModQu.com

Figure 1. Whaley's six methods of deception. Most real deceptions combine methods from both columns. Based on Whaley (1982); table by ModQu with illustrative business examples.

Masking makes something invisible; **repackaging** disguises it as something else; **dazzling** confuses the observer so that the real is lost among distractions. **Mimicking** makes something false look like something real; **inventing** creates a false reality from nothing; **decoying** draws attention towards a false target. Bell and Whaley (1991) showed that these methods apply equally in war, in business, in confidence tricks and in stage magic.

Whaley (2007), in a study of more than a hundred military operations, found that deception was common and usually effective: commanders who used it achieved surprise far more often than those who did not, and the deceptions were rarely detected even when the victim had good intelligence. Howard (1995) described how the British in the Second World War built a sophisticated deception organisation that, among other operations, persuaded German commanders that the main Allied landing in 1944 would come at the Pas de Calais rather than in Normandy. Macintyre (2010) recounts Operation Mincemeat, in which a corpse carrying false documents was allowed to wash ashore in Spain in 1943, leading German commanders to expect an Allied invasion of Greece and Sardinia rather than Sicily.

Why deception succeeds

Heuer (1981) explained deception through the psychology of perception. People interpret new information through their existing expectations, and they are much more easily persuaded that their expectations are correct than that they are wrong. The most effective deceptions therefore reinforce what the target already believes. Operation Mincemeat worked partly because German commanders already considered Greece a plausible Allied target. Heuer concluded that analysts cannot rely on spotting deception by its own features, because a good deception looks exactly like the truth. Instead they must consider the possibility of deception explicitly, especially when the stakes are high and an adversary has both the motive and the means to deceive.

Individual lie detection is also weak. Vrij (2008) reviewed research on how well people detect lies in face-to-face settings and found that accuracy is typically only slightly better than chance, even among professionals such as police officers. Common beliefs about the signs of lying, such as avoiding eye contact, have little support. Better results come from focusing on the content of what people say, its consistency and its verifiability, rather than on nervous behaviour.

Disinformation in the digital age

Digital platforms have transformed the scale and speed of disinformation. Vosoughi et al. (2018) analysed about 126,000 stories spread on Twitter between 2006 and 2017 and found that false news spread farther, faster and more widely than true news, in every category of information. The difference was driven by people rather than automated accounts: false stories were more novel and provoked stronger emotional responses, which made people more likely to share them.

Rid (2020) traces the history of organised disinformation, from Soviet "active measures" during the Cold War to the operations of the internet era. Rid shows that many techniques are old, such as forged documents, front organisations and the mixing of true and false material, but that digital platforms have made them faster and harder to attribute. Starbird et al. (2019) studied online information operations and found that they are often **collaborative**: a small number of organised actors seed content, which is then spread and adapted by many genuine users who come to believe it. This makes such operations hard to distinguish from authentic public debate.

Benkler et al. (2018) studied the American media system and argued that the effects of disinformation depend heavily on the structure of the media ecosystem. Where audiences rely on a closed set of partisan sources that reinforce one another, false stories can circulate with little correction. Chesney and Citron (2019) warned that **deepfakes**, convincing synthetic audio and video, add a further threat. They identified what they called the **liar's dividend**: once people know that fakes exist, genuine evidence can be dismissed as fake.

Why people believe false information

Research on the psychology of misinformation has grown rapidly. Two broad explanations compete. One holds that people believe false claims that fit their political or social identity: they reason towards the conclusions they want. The other holds that people often simply do not think carefully. Pennycook and Rand (2019) found that people who scored higher on a test of analytic thinking were better at distinguishing true from false headlines, regardless of whether the

headlines favoured their own political side. They concluded that susceptibility to fake news is better explained by lazy thinking than by partisan bias. In a later review, Pennycook and Rand (2021) noted that both factors play a role, but that inattention to accuracy is an important and correctable one.

Metzger et al. (2010) studied how people judge the credibility of online information and found that they rely heavily on shortcuts: the reputation of the source, endorsements by others, consistency with other sources and whether the content matches their expectations. These shortcuts are efficient but easy to exploit. A false story that appears on a professional-looking website and is shared by many people passes most of them.

Lewandowsky et al. (2017) argued that misinformation should be understood not only as a problem of individual error but as a feature of a changed information environment, in which trust in institutions has declined and alternative accounts of reality circulate freely. Ecker et al. (2022) reviewed the psychological drivers of misinformation belief and highlighted the **continued influence effect**: even after people accept a correction, the original false information often continues to influence their reasoning.

Correcting false beliefs

A natural response to false information is to correct it. Research on corrections has produced some surprising and some reassuring findings.

Nyhan and Reifler (2010) reported that, in some experiments, correcting a political misperception strengthened the false belief among those most committed to it, an outcome they called the **backfire effect**. The finding received wide attention. However, Wood and Porter (2019), testing corrections on 52 issues with more than 10,000 participants, found that backfire was rare: corrections generally moved people towards the truth, even when the correction ran against their politics. Walter et al. (2020), in a meta-analysis of fact-checking studies, confirmed that corrections have a meaningful positive effect on beliefs, though the effect is weaker for politically charged topics and when people have strong prior views.

The practical lesson is that correcting false information is worthwhile, but that corrections should be designed well. Ecker et al. (2022) recommend stating the truth clearly, explaining why the false claim is wrong, and, where possible, giving an alternative explanation that fills the gap the false claim leaves. A correction that simply says "this is false" leaves people with a gap in their understanding, which they may fill with the original falsehood.

Responding to false information: what the evidence supports

Approaches tested in research, and when each fits

Response	What it involves	Evidence	Best used
Debunking	Correct the claim; explain why it is false	Moderate effect; weaker on political topics	After a claim spreads
Prebunking	Warn and expose the technique in advance	Reduces later influence	Before an expected campaign
Accuracy prompts	Ask people to consider whether content is true	Improves sharing choices	On platforms and in teams
Verification	Check source, origin, time, place, motive	Standard practice in newsrooms	Before relying on content

Compiled from Walter et al. (2020), Ecker et al. (2022), Cook et al. (2017) and Pennycook and Rand (2021); table by ModQu

ModQu.com

Figure 2. Responding to false information. The approaches complement one another: verification protects an organisation's own judgements, while prebunking and debunking protect its audiences. Compiled from Walter et al. (2020), Ecker et al. (2022), Cook et al. (2017) and Pennycook and Rand (2021); table by ModQu.

Prebunking and inoculation

Correcting falsehoods after they spread is difficult. A growing body of research suggests that it is often more effective to prepare people in advance. The idea goes back to McGuire and Papageorgis (1961), who proposed **inoculation theory**: just as a vaccine exposes the body to a weakened virus, exposing people to a weakened form of a persuasive argument, together with its refutation, helps them resist the full argument later.

Cook et al. (2017) applied inoculation to misinformation about climate science. They found that explaining the technique used by a misleading argument, such as presenting fake experts to suggest that scientists disagree, reduced the argument's influence when participants later encountered it. Importantly, the inoculation worked even without addressing the specific false claim, because it taught people to recognise the technique. This approach, now often called **prebunking**, is attractive because one lesson about a technique can protect against many different false stories that use it.

Pennycook and Rand (2021) describe a simpler intervention: **accuracy prompts**. Asking people to consider whether a headline is accurate before they share content improved the quality of what they shared, apparently because it shifted their attention towards truth.

Counter-narratives

A **counter-narrative** is an alternative account that competes with a false or harmful story. Simply denying a narrative is often ineffective, because stories are remembered better than facts, and a denial repeats the very claim it disputes. A counter-narrative instead offers a coherent explanation of events that accounts for the evidence, fills the gap left by the false story and is at least as memorable.

The research on corrections supports this approach. Ecker et al. (2022) found that corrections providing an alternative causal explanation are more effective than bare retractions, because they replace the false element in people's mental model of what happened. Lewandowsky et al. (2017) argued that effective responses must address the wider context in which misinformation thrives, including declining trust, rather than individual claims alone.

For organisations, the principle is that the best defence against a false story is a true one, told clearly, early and through trusted messengers. When a company faces a false rumour about its product, a statement that the rumour is untrue is less effective than a clear account of what actually happened, supported by evidence and repeated by credible voices such as independent experts or customers.

Deception in business

Deception is not confined to war and politics. Companies conceal products in development, announce projects they do not intend to pursue, leak misleading information about prices or capacity and occasionally plant false stories about rivals. Bell and Whaley (1991) show that the same principles operate in commercial cheating as in military deception: the deceiver studies what the target expects and supplies evidence that fits.

Competitive intelligence teams therefore face the same problem as government analysts. A rival's public statements, its job postings, its regulatory filings and the gossip of its suppliers may all be partly managed. Godson and Wirtz (2002) argue that denial and deception are most likely where the stakes are high, where the deceiver has control over the channels the target relies on and where the target has a known set of expectations to exploit. Each of these conditions can be checked. An analyst who relies heavily on information the competitor itself publishes, about a decision that matters greatly to the competitor, should give serious weight to the possibility of deception.

Markets add a further form of disinformation: false reviews, inflated ratings and coordinated campaigns to damage a rival's reputation. These contaminate the data that marketing and insights teams use to understand customers. Screening such data, and comparing it with sources that are harder to manipulate, such as properly sampled surveys and sales records, protects both the analysis and the decisions based on it.

Deception and knowledge generation

For organisations that produce knowledge, deception and disinformation threaten the integrity of their evidence. Survey responses can be manipulated by bots or coordinated campaigns. Online reviews and social media data can be flooded with fake content. Documents can be forged and images altered. A research or intelligence process that does not account for these threats may produce confident conclusions from contaminated data.

Several practices reduce the risk:

1. **Verify before relying.** Silverman (2014), in a handbook for journalists, sets out a verification routine: identify the original source, establish when and where content was created, check whether it has appeared before and consider who benefits from its spread. The same routine applies to any evidence an analyst uses.
2. **Consider deception explicitly.** When an adversary has a motive and the means to deceive, include a deception hypothesis among the alternatives and ask what evidence would distinguish it (Heuer, 1981).
3. **Look for consistency across independent sources.** A deception is hard to sustain across many sources that the deceiver does not control. Evidence that appears only in one channel, or in channels the adversary could influence, deserves extra scrutiny.
4. **Check data quality in surveys and digital data.** Screening questions, attention checks, patterns of responses and the detection of duplicate or automated entries help protect research data.
5. **Watch for content that fits expectations too neatly.** The most dangerous deceptions confirm what the organisation already believes (Heuer, 1981). Evidence that is unusually convenient warrants a second look.

Common mistakes

- **Assuming deception will look suspicious.** Good deception looks normal; that is the point.
- **Relying on gut feeling to spot liars.** Research shows this is barely better than chance (Vrij, 2008).
- **Repeating the false claim prominently in a correction.** Lead with the truth, then address the falsehood.
- **Treating every error as deception.** Most false information is shared innocently. Accusing honest sources of deception damages trust and wastes effort.
- **Ignoring the liar's dividend.** Dismissing inconvenient evidence as fake is itself a vulnerability (Chesney & Citron, 2019).
- **Waiting too long.** False stories travel quickly (Vosoughi et al., 2018). A clear, early account is more effective than a perfect one issued a week later.

An illustration

A Canadian food producer notices a sudden surge of social media posts claiming that one of its products has made children ill. The posts include photographs and appear to come from many different parents. The company's insights team begins by verifying the content, following the steps Silverman (2014) describes. Reverse image searches show that several photographs were published years earlier in another country. Many of the accounts were created within the same week and post in similar language. Hospital and public health records show no increase in related illnesses.

The team concludes that the campaign is probably coordinated and that the central claim is false, while noting that a few posts appear to come from genuine, worried parents who have seen the story. The company does not simply deny the claim. It publishes a clear account: what the product contains, how it is tested, what the health authorities have confirmed and how the false images were traced. It invites an independent food safety expert to explain the findings and responds individually and respectfully to worried parents. Within two weeks, the volume of posts declines and surveys show that trust in the brand has recovered among most customers.

Conclusion

Deception and disinformation are deliberate attacks on knowledge. Classic studies of military deception show that they succeed most often by reinforcing what the target already believes, and that they are rarely detected by their own features. Research on digital disinformation shows that false stories spread faster than true ones and that people believe them more through inattention than through bias alone. Corrections work better than once feared, especially when they offer an alternative explanation, and prebunking can protect people in advance. For any organisation that generates knowledge, the best defences are systematic verification, explicit consideration of deception and clear, credible counter-narratives grounded in evidence.

References

Bell, J. B., & Whaley, B. (1991). *Cheating and deception*. Transaction.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

Cook, J., Lewandowsky, S., & Ecker, U. K. H. (2017). Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence. *PLOS ONE, 12*(5), Article e0175799. https://doi.org/10.1371/journal.pone.0175799

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K., & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology, 1*(1), 13–29. https://doi.org/10.1038/s44159-021-00006-y

Godson, R., & Wirtz, J. J. (Eds.). (2002). *Strategic denial and deception: The twenty-first century challenge*. Transaction.

Heuer, R. J., Jr. (1981). Strategic deception and counterdeception: A cognitive process approach. *International Studies Quarterly, 25*(2), 294–327.

Howard, M. (1995). *Strategic deception in the Second World War*. Norton.

Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the "post-truth" era. *Journal of Applied Research in Memory and Cognition, 6*(4), 353–369. https://doi.org/10.1016/j.jarmac.2017.07.008

Macintyre, B. (2010). *Operation Mincemeat: How a dead man and a bizarre plan fooled the Nazis and assured an Allied victory*. Harmony Books.

McGuire, W. J., & Papageorgis, D. (1961). The relative efficacy of various types of prior belief-defense in producing immunity against persuasion. *Journal of Abnormal and Social Psychology, 62*(2), 327–337. https://doi.org/10.1037/h0042026

Metzger, M. J., Flanagin, A. J., & Medders, R. B. (2010). Social and heuristic approaches to credibility evaluation online. *Journal of Communication, 60*(3), 413–439. https://doi.org/10.1111/j.1460-2466.2010.01488.x

Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior, 32*(2), 303–330. https://doi.org/10.1007/s11109-010-9112-2

Pennycook, G., & Rand, D. G. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition, 188*, 39–50. https://doi.org/10.1016/j.cognition.2018.06.011

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences, 25*(5), 388–402. https://doi.org/10.1016/j.tics.2021.02.007

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Silverman, C. (Ed.). (2014). *Verification handbook: A definitive guide to verifying digital content for emergency coverage*. European Journalism Centre.

Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), Article 127. https://doi.org/10.1145/3359229

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

Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and opportunities* (2nd ed.). Wiley.

Walter, N., Cohen, J., Holbert, R. L., & Morag, Y. (2020). Fact-checking: A meta-analysis of what works and for whom. *Political Communication, 37*(3), 350–375. https://doi.org/10.1080/10584609.2019.1668894

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe report DGI(2017)09). Council of Europe.

Whaley, B. (1982). Toward a general theory of deception. *Journal of Strategic Studies, 5*(1), 178–192. https://doi.org/10.1080/01402398208437106

Whaley, B. (2007). *Stratagem: Deception and surprise in war*. Artech House.

Wood, T., & Porter, E. (2019). The elusive backfire effect: Mass attitudes' steadfast factual adherence. *Political Behavior, 41*(1), 135–163. https://doi.org/10.1007/s11109-018-9443-y