

Factsheet 4: Types of Misinformation and Disinformation

Misinformation is false or inaccurate information. Examples include rumors, insults and pranks.

Disinformation is deliberate and includes malicious content such as hoaxes, spear phishing and propaganda. It spreads fear and suspicion among the population.

Types of Misinformation and Disinformation:

1. **Fabricated Content:** Completely false content;
2. **Manipulated Content:** Genuine information or imagery that has been distorted, e.g. a sensational headline or populist 'click bait';
3. **Imposter Content:** Impersonation of genuine sources, e.g. using the branding of an established agency;
4. **Misleading Content:** Misleading information, e.g. comment presented as fact;
5. **False Context:** Factually accurate content combined with false contextual information, e.g. when the headline of an article does not reflect the content;
6. **Satire and Parody:** Humorous but false stories passed off as true. There is no intention to harm but readers may be fooled;
7. **False Connections:** When headlines, visuals or captions do not support the content;
8. **Sponsored Content:** Advertising or PR disguised as editorial content;
9. **Propaganda:** Content used to manage attitudes, values and knowledge;
10. **Error:** A mistake made by established news agencies in their reporting.

The rise of Artificial Intelligence (AI) has also given birth to new forms of misinformation and disinformation. We call this Synthetic Media to indicate the artificial production, manipulation and modification of data and multimedia by automated means, especially AI algorithms, to mislead or change original meaning. There are fears that synthetic media could supercharge fake news, spread misinformation and distrust of reality and automate creative jobs.

“Deep Fakes” are one type of synthetic media where a person in an existing image or video is replaced with someone else's likeness. While the act of faking content is not new, deep fakes use powerful techniques from machine learning and AI to manipulate or generate visual and audio content with a high potential to deceive. Deep Fakes have garnered widespread attention for their use in revenge porn, fake news, hoaxes and financial fraud. Industry and governments are concerned to detect and limit their use. Some countries already have a national response or national institutions are working on it.

“Speech Synthesis” is another branch of synthetic media that can artificially produce human speech. A computer used for this purpose is called a “speech computer” or “speech synthesizer”. Synthesized speech concatenates pieces of recorded speech or it incorporates a model of the vocal tract and other human voice characteristics to create a completely “synthetic” voice.

In addition to new and more sophisticated ways of manipulating content, there are also a growing number of ways in which Social Media can be used to manipulate conversations:

- A **Sockpuppet** is an online identity used to deceive. The term now extends to misleading uses of online identities to praise, defend or support a person or organization; to manipulate public opinion; or to circumvent restrictions, suspension or an outright ban from a website. The difference between a pseudonym and a sockpuppet is that the sockpuppet poses as an independent third party, unaffiliated with the main account holder. Sockpuppets are unwelcome in many online communities and forums;
- **Sealioning** is a type of trolling or harassment where people are pursued with persistent requests for evidence or repeated questions. A pretense of civility and sincerity is maintained with these incessant, bad-faith invitations to debate;
- **Astroturfing** masks the sponsors of a message (e.g. political, religious, advertising or PR organizations) to make it appear as though it comes from grassroots participants. The practice aims to give organizations credibility by withholding information about their motives or financial connections;
- **Catfishing** is a form of fraud where a person creates a sockpuppet or fake identity to target a particular victim on Social Media. It is common for romance scams on dating websites. It may be done for financial gain, to compromise a victim or as a form of trolling or wish fulfillment.

