JONATHAN TANNER

10 THINGS TO KNOW ABOUT MISINFORMATION AND DISINFORMATION

ODI
203 Blackfriars Road
London SE1 8NJ

+44 (0)20 7922 0300
info@odi.org

odi.org
odi.org/facebook
odi.org/twitter

Evidence.
Ideas.
Change.

Technology has transformed the way we create, access, share and digest information on a global scale. More than four billion people worldwide now use the internet, 97% of people live within range of a mobile phone network[1] and there are approximately 3.6 billion social media users on the planet.[2]

If you're accessing Facebook through a phone in Mozambique, sharing a joke on WhatsApp in India or uploading a video to TikTok in the US or Europe, you're part of a new digital information ecosystem sharing content via a range of digital devices and platforms.

For many people and organisations, these digital information ecosystems, underpinned by the internet and social media, present an important new means of expression, connection, commerce and creativity. Most major social media platforms are designed to encourage rapid sharing of information. One of the ways this is done is by promoting content that provokes strong emotions. Facebook's own internal research concludes that its algorithms 'exploit the human brain's attraction to divisiveness'.[3]

By accident or design, the internet and social media have created the ideal conditions for a huge increase in false information and conspiracy theories. This can cause real harm offline, especially because digital literacy and digital policy are both currently unable to keep up with the pace of change.

In recent years, major democracies have had to investigate foreign interference in their digital information ecosystems. Over a third of Europeans now encounter so-called 'fake news' every day.[4] In late June this year, the World Health Organization (WHO) held its first-ever conference looking at 'infodemiology' in response to misinformation related to Covid-19.[5] Now established fact-checking organisations are emerging across the world and major media organisations have misinformation and disinformation (MDI) reporters.[6]

Here are 10 things you need to know about MDI and how it can be tackled.

01 WHAT IS MDI?

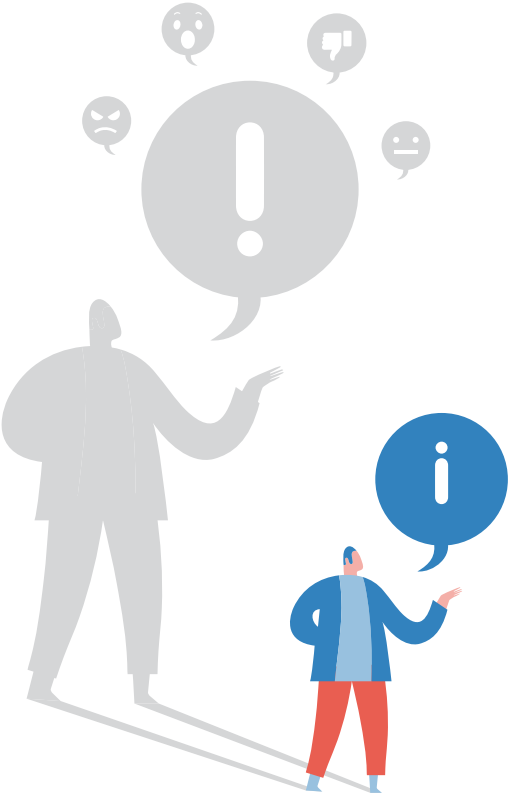
Let's get the definitions out of the way first.

Misinformation is false and often harmful information, which is not shared with malicious intent.

Disinformation is false and malicious information, which is shared deliberately to cause harm.[7]

We've grouped these problems together as 'MDI', but tackling misinformation and disinformation will require different strategies. The best strategies for dealing with MDI will always require an understanding of local information ecosystems, including offline networks of influence in communities with lower levels of digital penetration.

MDI comes in many forms. It can include stories on websites that impersonate established media brands, manipulated images or video, pictures, quotes and even facts taken out of context in memes and gifs, as well as content which is entirely fictitious.



02 WHO'S SPREADING IT?

Everybody!

We are all potential spreaders of MDI. Whenever we forward a viral message or retweet something, we run the risk of amplifying false or harmful information. Psychologists have found that we are more likely to share MDI with those we are closest to.[8] This is especially the case if it's making a point you agree with on Facebook or Twitter, or it comes directly in the form of memes and viral videos sent via WhatsApp or Instagram.

Despite this, most of us have never knowingly shared MDI. That tends to be done by states looking to influence events beyond their borders, politicians and their supporters looking to win power, extremist groups like Qanon, Boko Haram[9] or Al Qaeda trying to recruit or radicalise members and unethical PR companies or entrepreneurs looking to make money.

03 IS THIS A NEW PROBLEM?

Not exactly. MDI is an old problem in a new context.

We have always had to deal with gossip, rumour, hearsay and propaganda. The reason it's such a problem now is because of the pace at which digital information ecosystems have evolved and the way in which they are being manipulated. MDI can now travel at much greater speed and scale, including across borders. This happens especially through social media, which is actively designed to encourage us to share information and content quickly. As it stands, most governments either don't want to or can't create policies to protect citizens from MDI and the harms it brings.

04 HOW DOES IT SPREAD?

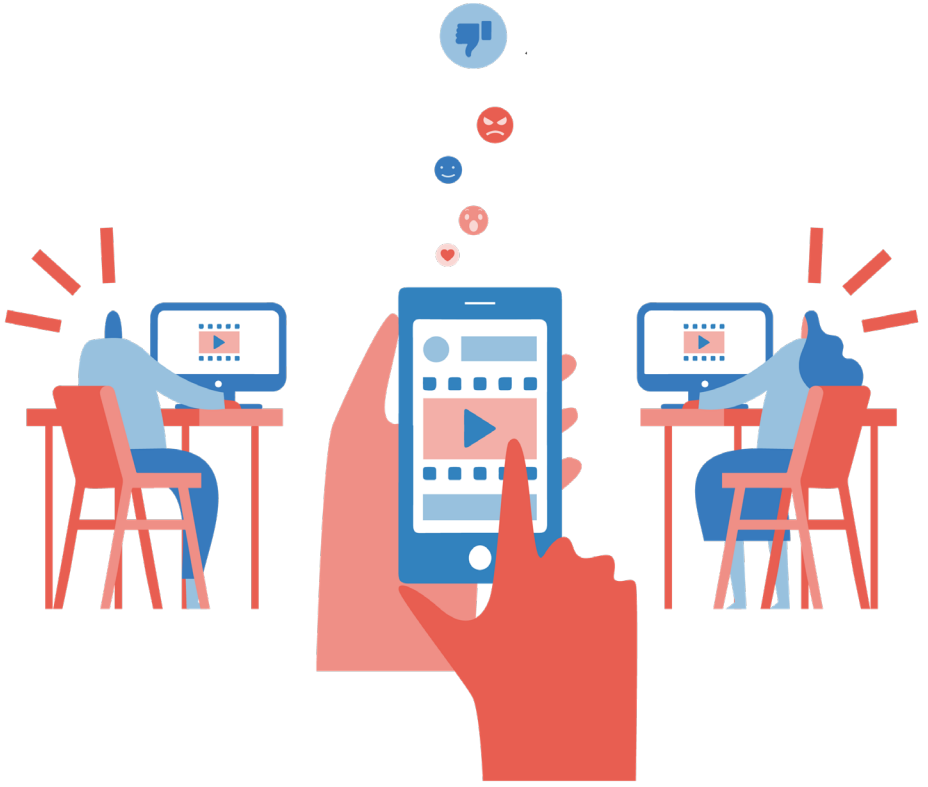
Easily.

A variety of techniques are used to spread MDI. Most take advantage of social media platforms designed to promote popular content that provokes strong emotions. MDI with 'viral' qualities is often based around memes and short videos that are widely shared on closed messaging apps like WhatsApp or Facebook Messenger.

Agents of MDI can build fake websites[10] or create fake social media accounts to host their messages, a tactic known as 'computational propaganda'.[11] These 'bots' are automated, but can be used to draw people towards human-led MDI accounts. Alternatively, people can embed themselves into existing Facebook or WhatsApp groups and use fake news stories to spread MDI among legitimate accounts, who then share the false content widely, sometimes to the extent that it is picked up by mainstream news outlets.

It is likely that those spreading MDI will increasingly draw on artificial intelligence (AI) to create more sophisticated ways to do so, including creating more realistic bot accounts[12] and hard-to-spot 'deepfake' videos, which some researchers are already calling the 'most serious AI crime threat'.[13]

All of this occurs in an environment where many traditional media organisations, who would often be the first to spot and tackle MDI, are struggling to maintain their income as advertising revenue shifts to the big tech companies.



05 IS THIS ALL ABOUT POWER?

Not quite. But it's a very large part of it.

The ability to control or shape narrative is one of the most important aspects of power. MDI can form part of a deliberate political strategy to exacerbate existing social tensions or sow doubt and confusion. It is present in debates around major political issues like climate change, migration and inequality, and also in localised or event-specific discourse.

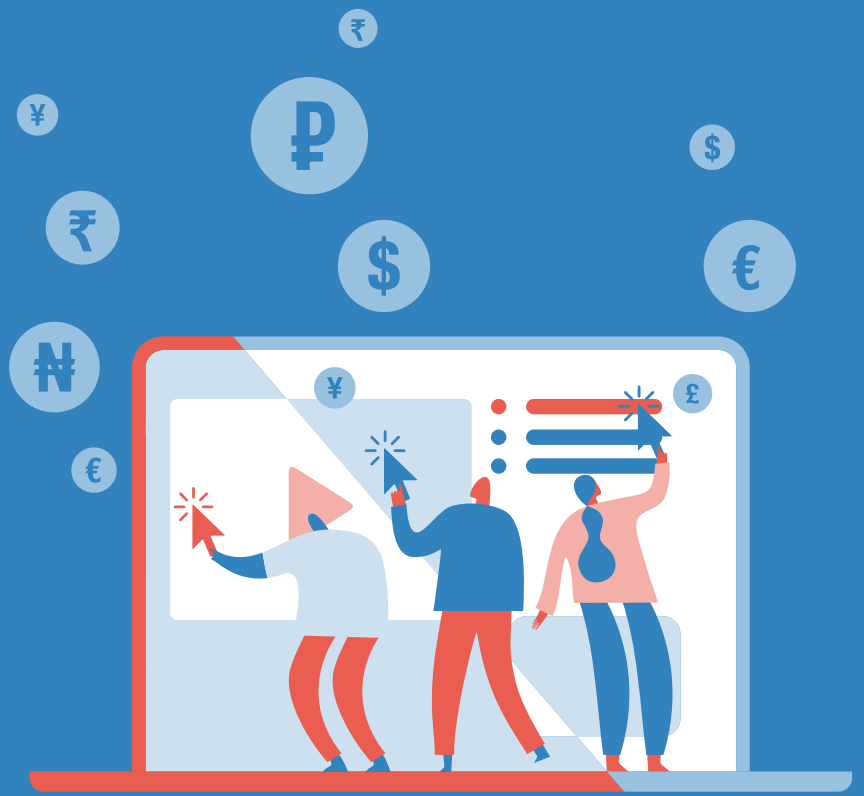
It's not just major powers that are involved. In 2020, a report from the Atlantic Council showed how a Tunisian company had tried to influence elections in Togo and Côte d'Ivoire.[14] In July 2020 Facebook removed inauthentic accounts in the Democratic Republic of Congo[15] and Brazil.[16]

06 WHAT ABOUT THE MONEY?

There is a lot of money to be made from MDI.

Digital advertising models are built around getting us to click links and visit pages where adverts are served, usually through major companies like Google and Facebook.

By creating popular profiles individuals can make thousands of dollars from their accounts, especially when using MDI and conspiracy theories to create clickbait.[17] Large platforms like YouTube and Twitter also profit from this; the Centre for Countering Digital Hate recently claimed that the anti-vaxxer movement alone is worth almost $1 billion a year to big tech.[18] During moments of particular social anxiety, hoaxes can be used to defraud people either through wrongfully masquerading as a charity or by actively seeking personal data and financial details.



07 WHO CAN I TRUST?

Good question.

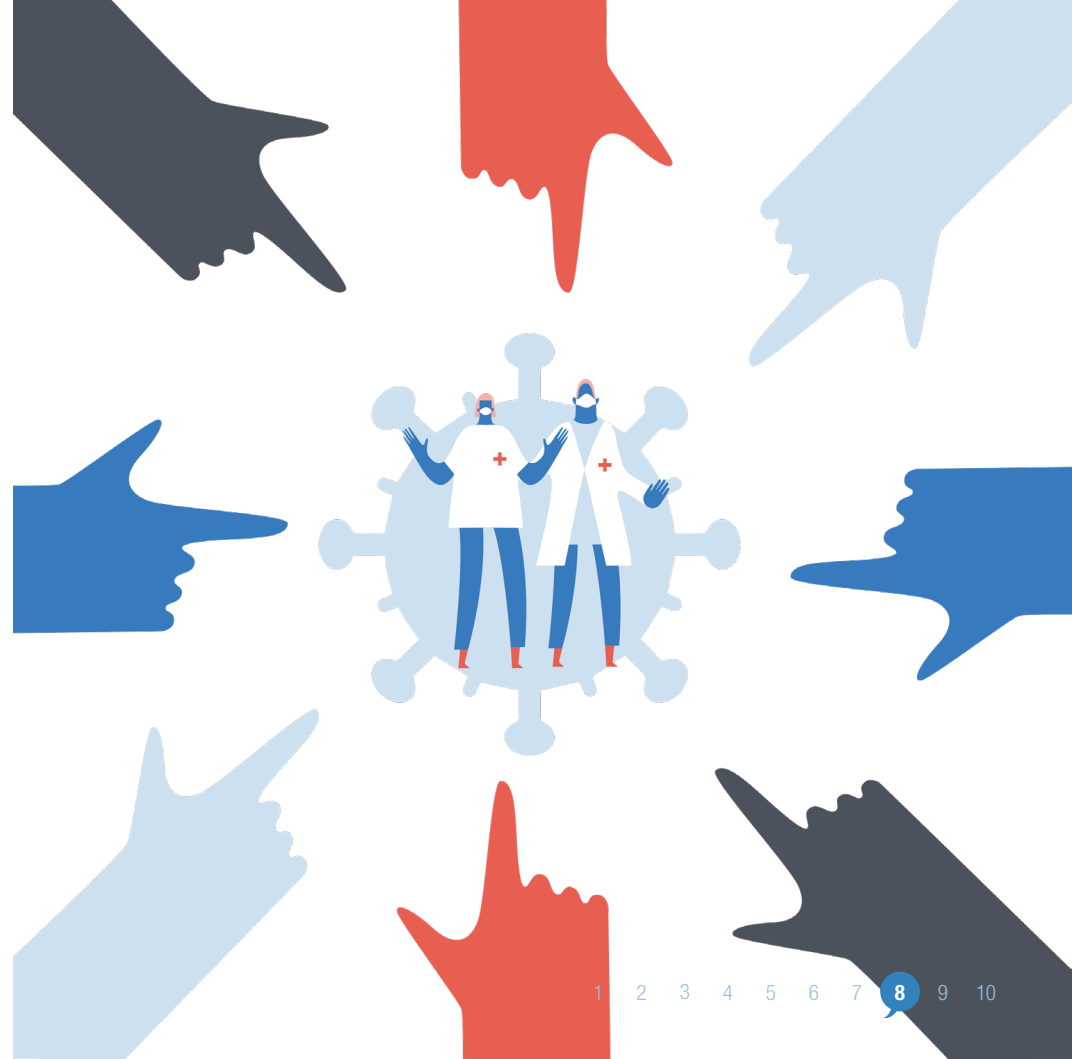
Trust plays a critical role in digital information ecosystems. Where trust in government and official sources of information is low, citizens judge public information differently compared to those countries where trust is high. How trust is created and given to different actors and institutions varies between contexts. In many countries there is an instinctive distrust of official information and citizens are more likely to trust religious or community leaders and friends and family. Understanding the role of trust in digital information ecosystems, and how individuals and institutions can gain or retain it, is critical to tackling the threat posed by MDI.

08 HOW MUCH DAMAGE DOES IT DO?

A lot.

MDI is often used to harden racist attitudes and drive discrimination and marginalisation. This can lead to violence and abuse and can undermine the role of official institutions in delivering public services like vaccination campaigns. In 2019 in Pakistan, polio vaccinations were suspended after MDI spread via WhatsApp triggered attacks on aid workers. During Covid-19, there have been attacks on healthcare workers in India, Mexico and elsewhere.[19] So far in 2020, a number of deaths have been attributed to Covid-19 MDI and thousands more have been injured.[20]

MDI spreads more quickly during periods of intense anxiety and uncertainty. In the US, the Federal Emergency Management Agency routinely establishes 'rumour control' to counteract MDI on social media in the aftermath of disasters. During the Syrian civil war, MDI has been used to undermine the humanitarian work of the White Helmets,[21] and the August 2020 explosion in Beirut and subsequent political unrest has seen MDI quickly circulate online to exploit tensions.[22] MDI also has consequences for the role of research and policy expertise in society when it creates doubt around established facts and evidence. This uncertainty can lead to poor public policy outcomes which then negatively affect people's lives.



09 WHAT CAN INSTITUTIONS DO ABOUT THIS?

It's a hard problem to solve.

It's unlikely to be possible to completely stop people misusing information to earn power or profits. To address MDI, organisations need to develop a better understanding of modern digital information ecosystems. This will help in developing the right mix of interventions, including support to independent journalists and fact-checkers, efforts to boost digital media literacy and new policy frameworks for preventing online harm. During moments of intensity that present a high risk of MDI it will be important for anti-MDI approaches to be coordinated and allow scope for innovative approaches which may challenge institutional norms.

10 OK, SO WHAT CAN I DO ABOUT IT?

Each of us has a responsibility to try to prevent the spread of MDI.

This is why the United Nations is investing in campaigns designed to get people to stop and think before sharing viral content.[23] Even if we don't share MDI, we can still be part of the problem if we don't try to address it when we see it. This doesn't mean trying to shame people who share MDI, but instead understanding why people may have shared false information and explaining the potential damage it can cause. We can also look for ways to engage with and support the growing number of civil society organisations[24] working to shape the future of digital societies.

REFERENCES AND RESOURCES

ODI's **Digital Societies** team combines expertise on policy, research, communication and evaluation, working alongside governments, citizens and states to build successful digital societies.

Thanks to Louise Shaxson, Aaron Bailey-Athias and Rose Beynon for their comments on an earlier draft, to Matthew Foley and Katie Forsythe for editorial support and Ottavia Pasta for design.

1 International Telecommunication Union (2019) 'Measuring digital development. Facts and figures 2019'. Geneva: ITU (www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf).

2 Clement, J. (2020) 'Number of social network users worldwide from 2017 to 2025'. Webpage. Statista (www.statista.com/statistics/278414/number-of-worldwide-social-network-users/#statisticContainer).

3 Horwitz, J. and Seetharaman, D. (2020) 'Facebook executives shut down efforts to make the site less divisive'. Wall Street Journal, 26 May (www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499).

4 European Commission (2018) *Fake news and disinformation online*. Flash Eurobarometer 464. Brussels: EU (www.ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183).

5 WHO (2020) 'How infodemics affect the world and how they can be managed'. Pre-conference booklet. 1st infodemiology conference, 29 June 2020, Geneva (www.who.int/docs/default-source/epi-win/infodemic-management/infodemiology-preconference-booklet.pdf).

6 BBC (n.d.) 'Fake news'. News topic webpage. BBC (www.bbc.co.uk/news/topics/cjxv13v27dyt/fake-news).

7 Wardle, C. and Derakhshan, H. (2017) *Information disorder. Toward an interdisciplinary framework for research and policy making*. Council of Europe report. DGI (2017)09. Strasbourg: Council of Europe (rm.coe.int/Report-D/09000016807bf5f6).

8 Shah, K. (2020) 'When your family spreads misinformation'. The Atlantic, 16 June (www.theatlantic.com/family/archive/2020/06/when-family-members-spread-coronavirus-misinformation/613129/).

9 Bukarti, A.B. (2020) 'How is Boko Haram responding to Covid-19?'. Policy briefing. London: Tony Blair Institute for Global Change (www.institute.global/policy/how-boko-haram-responding-covid-19).

10 FactCheck.org (2017) 'Misinformation directory'. FactCheck webpost. FackCheck.org (www.factcheck.org/2017/07/websites-post-fake-satirical-stories/).

11 Woolley, S.C. and Howard, P.N. (2017) *Computational propaganda worldwide: executive summary*. Working Paper No. 2017.11. Oxford: University of Oxford (blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf).

12 Schneier, B. (2020) 'Bots are destroying political discourse as we know it'. The Atlantic, 7 January (www.theatlantic.com/technology/archive/2020/01/future-politics-bots-drowning-out-humans/604489/).

13 University College London (2020) '"Deepfakes" ranked as most serious AI crime threat'. UCL News webpage. UCL (www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat).

14 Carvin, A. (2020) *Operation Carthage: how a Tunisian company conducted influence operations in African presidential elections*. Report for the Digital Forensic Research. Washington DC: Atlantic Council (www.atlanticcouncil.org/in-depth-research-reports/operation-carthage-how-a-tunisian-company-conducted-influence-operations-in-african-presidential-elections/).

15 Facebook (2020) *July 2020 coordinated inauthentic behavior report*. Menlo Park, CA: Facebook Inc. (www.about.fb.com/news/2020/08/july-2020-cib-report/).

16 Brito, R. and Paraguassu, L. (2020) 'Facebook, Twitter remove accounts of Bolsonaro supporters following court order'. Reuters Business News, 25 July (uk.reuters.com/article/uk-brazil-fakenews/facebook-twitter-remove-accounts-of-bolsonaro-supporters-following-court-order-idUKKCN24Q001).

17 Global Disinformation Index (2020) 'Why is ad tech giving millions to EU disinformation sites?'. Blog. GDI (www.disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/).

18 Center for Countering Digital Hate (2020) *The anti-vaxx industry. How big tech powers and profits from vaccine misinformation*. London: CCDH (www.counterhate.co.uk/anti-vaxx-industry).

19 ReliefWeb (2020) 'Attacks on health care during the COVID-19 pandemic'. News post. ReliefWeb (www.reliefweb.int/report/world/attacks-health-care-during-covid-19-pandemic).

20 Islam, S. et al. (2020) 'COVID-19-related infodemic and its impact on public health: a global social media analysis' *American Journal of Tropical Medicine and Hygiene* (www.doi.org/10.4269/ajtmh.20-0812).

21 Starbird, K. and Wilson, T. (2020) 'Cross-platform disinformation campaigns: lessons learned and next steps'. *Harvard Kennedy School (HKS) Misinformation Review* (www.doi.org/10.37016/mr-2020-002).

22 Waters, N. (2020) 'The Beirut explosion – is it a bird? Is it a plane? Is it a faked video of a missile?'. Blog. Bellingcat (www.bellingcat.com/news/mena/2020/08/07/the-beirut-explosion-is-it-a-bird-is-it-a-plane-is-it-a-faked-video-of-a-missile/).

23 UN Affairs (2020) 'Pause before sharing, to help stop viral spread of COVID-19 misinformation'. UN News webpage. UN (news.un.org/en/story/2020/06/1067422).

24 See First Draft (www.firstdraftnews.org), Digital Action (www.digitalaction.co) and the Web Foundation (www.webfoundation.org).