Information Disorder: The Essential Glossary

Claire Wardle

Research by: Grace Greason,
Joe Kerwin, Nic Dias

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy

July 2018

Definitions and terminology matter. For the policy-makers, technology companies, politicians, journalists, librarians, educators, academics, and civil society organisations all wrestling with the challenges posed by information disorder, agreeing to a shared vocabulary is essential.

This glossary features the most frequently used and commonly misunderstood words, acronyms, and phrases that relate to information disorder. It is designed to be a living document that will evolve as a reference point alongside research findings, shifts in technology, and the inevitable debates sparked by the definitions.

Algorithm

An **algorithm** is a fixed series of steps that a computer performs in order to solve a problem or complete a task. For instance, social media platforms use algorithms to compile the content that users see. These algorithms in particular are designed to show users material that they will be interested in, based on each user's history of engagement on that platform. For example, algorithms can often filter content so that users primarily see types of content with which they have previously engaged. Users tend to engage with content that provokes an emotional reactions like fear and anger. As such, it's argued that algorithms designed to take advantage of users' emotions create an environment wherein disinformation created to play into deep-seated fears and cultural identities will flourish.[1]

API

An **API**, or application programming interface, is a means by which data from one web tool or application can be exchanged with, or received by another. Many working to examine the source and spread of polluted information depend upon access to social platform APIs, but not all are created equal and the extent of publicly available data varies from platform to platform. Twitter's open and easy-to-use API has enabled thorough research and investigation of its network, plus the development of mitigation tools such as bot detection systems. However, restrictions on other platforms and a lack of API standardization means it is not yet possible to extend and replicate this work across the social web.

Artificial intelligence (AI)

Artificial intelligence (AI) describes computer programs that are 'trained' to solve problems that would normally be difficult for a computer to solve. These programs "learn" from data parsed through them, adapting methods and responses in a way that will maximize accuracy. As disinformation grows in its scope and sophistication, some look to AI as a way to effectively detect and moderate concerning content. AI also contributes to the problem, automating the processes that enable the creation of more persuasive manipulations of visual imagery, and enabling disinformation campaigns that can be targeted and personalized much more efficiently.[2]

Automation

Automation is the process of designing a 'machine' to complete a task with little or no human direction. It takes tasks that would be time-consuming for humans to complete and turns them into tasks that are completed quickly and almost effortlessly. For example, it is possible to automate the process of sending a tweet, so a human doesn't have to actively click 'publish'. Automation processes are the backbone of techniques used to effectively 'manufacture' the amplification of disinformation.

Black hat SEO

Black hat SEO (search engine optimization) describes aggressive and illicit strategies used to artificially increase a website's position within a search engine's results, for example changing the content of a website after it has been ranked. These practices generally violate the given search engine's terms of service as they drive traffic to a website at the expense of the user's experience.[3]

Bots

Bots are social media accounts that are operated entirely by computer programs and are designed to generate posts and/or engage with content on a particular platform. In disinformation campaigns, bots can be used to draw attention to misleading narratives, to hijack platforms' trending lists, and to create the illusion of public discussion and support.[4] Researchers and technologists take different approaches to identifying bots, using algorithms or simpler rules based on number of posts per day.[5]

Botnet

A **botnet** is a collection or network of bots that act in coordination and are typically operated by one person or group. Commercial botnets can include as many as tens of thousands of bots.[6]

Data Mining

Data mining is the process of monitoring large volumes of data by combining tools from statistics and artificial intelligence to recognize useful patterns. Through collecting information about an individual's activity, disinformation agents have a mechanism by which they can target users on the basis of their posts, likes, and browsing history. A common fear among researchers is that, as psychological profiles fed by data mining become more sophisticated, users could be targeted based on how susceptible they are to believing certain false narratives.[7]

Dark Ads

Dark ads are advertisements that are only visible to the publisher and their target audience. For example, Facebook allows advertisers to create posts that reach specific users based on their demographic profile, page 'likes', and their listed interests, but that are not publicly visible. These types of targeted posts cost money and are therefore considered a form of advertising. Because these posts are only seen by a segment of the audience, they are difficult to monitor or track.[8]

Deep Fakes

Deepfakes is the term currently being used to describe fabricated media produced using artificial intelligence. By synthesizing different elements of existing video or audio files, AI enables relatively easy methods for creating 'new' content, in which individuals appear to speak words and perform actions, which are not based on reality. Although 'deepfakes' are still in their infancy, it is likely we will see the term 'deepfakes' used more frequently in disinformation campaigns, as these techniques become more sophisticated.[9]

Dormant Account

A **dormant account** is a social media account that has not posted or engaged with other accounts for an extended period of time. In the context of disinformation, this description is used for accounts that may be human- or bot-operated, which remain inactive until they are 'programmed' or instructed to perform another task.[10]

Doxing

Doxing or **doxxing** is the act of publishing private or identifying information about an individual online, without his or her permission. This information can include full names, addresses, phone numbers, photos, and more.[11] Doxing is an example of malinformation, which is accurate information shared publicly to cause harm.

Disinformation

Disinformation is false information that is deliberately created or disseminated with the express purpose to cause harm. Producers of disinformation typically have political, financial, psychological, or social motivations.[12]

Encryption

Encryption is the process of encoding data so that it can be interpreted only by intended recipients. Many popular messaging services such as WhatsApp encrypt the texts, photos, and videos sent between users. This prevents governments from reading the content of intercepted WhatsApp messages, and journalists from attempting to monitor mis- or disinformation being shared on the platform.

Fact-Checking

Fact-checking (in the context of information disorder) is the process of determining the truthfulness and accuracy of official, published information such as politicians' statements and news reports.[13] Fact-checking emerged in the U.S. in the 1990s, as a way of authenticating claims made in political ads airing on television. There are now around 150 fact-checking organizations in the world,[14] and many now also debunk mis- and disinformation from unofficial sources circulating online.

Fake Followers

Fake followers are anonymous or imposter social media accounts created to portray false impressions of popularity about another account. Social media users can pay for fake followers as well as fake likes, views, and shares to give the appearance of a larger audience. For example, one English-based service offers YouTube users a million "high-quality" views and 50,000 likes for $3,150.[15]

Malinformation

Malinformation is genuine information that is shared to cause harm.[16] This includes private or revealing information that is spread to harm a person or reputation.

Manufactured Amplification

Manufactured Amplification occurs when the reach or spread of information is boosted through artificial means. This includes human and automated manipulation of search engine results and trending lists, and the promotion of certain links or hashtags on social media.[17] There are online price lists for different types of amplification, including prices for generating fake votes and signatures in online polls and petitions, and the cost of downranking specific content from search engine results.[18]

Meme

The formal definition of the term **meme**, coined by biologist Richard Dawkins in 1976, is an idea or behavior that spreads person to person throughout a culture by propagating rapidly, and changing over time.[19] The term is now used most frequently to describe captioned photos or GIFs that spread online, and the most effective are humorous or critical of society. They are increasingly being used as powerful vehicles of disinformation.

Misinformation

Misinformation is information that is false, but not intended to cause harm. For example, individuals who don't know a piece of information is false may spread it on social media in an attempt to be helpful.[20]

Propaganda

Propaganda is true or false information spread to persuade an audience, but often has a political connotation and is often connected to information produced by governments. It is worth noting that the lines between advertising, publicity, and propaganda are often unclear.[21]

Satire

Satire is writing that uses literary devices such as ridicule and irony to criticize elements of society. Satire can become misinformation if audiences misinterpret it as fact.[22] There is a known trend of disinformation agents labelling content as satire to prevent it from being flagged by fact-checkers.

Scraping

Scraping is the process of extracting data from a website without the use of an API. It is often used by researchers and computational journalists to monitor mis- and disinformation on different social platforms and forums. Typically, scraping violates a website's terms of service (i.e., the rules that users agree to in order to use a platform). However, researchers and journalists often justify scraping because of the lack of any other option when trying to investigate and study the impact of algorithms.

Sock Puppet

A **sock puppet** is an online account that uses a false identity designed specifically to deceive. Sock puppets are used on social platforms to inflate another account's follower numbers and to spread or amplify false information to a mass audience.[23] The term is considered by some to be synonymous with the term "bot".

Trolling

Trolling is the act of deliberately posting offensive or inflammatory content to an online community with the intent of provoking readers or disrupting conversation. Today, the term "troll" is most often used to refer to any person harassing or insulting others online. However, it has also been used to describe human-controlled accounts performing bot-like activities.

Troll Farm

A **troll farm** is a group of individuals engaging in trolling or bot-like promotion of narratives in a coordinated fashion. One prominent troll farm was the Russia-based Internet Research Agency that spread inflammatory content online in an attempt to interfere in the U.S. presidential election.[24]

Verification

Verification is the process of determining the authenticity of information posted by unofficial sources online, particularly visual media.[25] It emerged as a new skill set for journalists and human rights activists in the late 2000s, most notably in response to the need to verify visual imagery during the 'Arab Spring'.

VPN

A **VPN**, or virtual private network, is used to encrypt a user's data and conceal his or her identity and location. This makes it difficult for platforms to know where someone pushing disinformation or purchasing ads is located. It is also sensible to use a VPN when investigating online spaces where disinformation campaigns are being produced.

[1] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
[2] Ghosh, D. & B. Scott (January 2018) #DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet, New America
[3] Ghosh, D. & B. Scott (January 2018) #DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet, New America
[4] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
[5] Howard, P. N. & K. Bence (2016) Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendu, COMPROP Research note, 2016.1, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2016/06/COMPROP-2016-1.pdf
[6] Ignatova, T.V., V.A. Ivichev, V.A. & F.F. Khusnoiarov (December 2, 2015) Analysis of Blogs, Forums, and Social Networks, Problems of Economic Transition
[7] Ghosh, D. & B. Scott (January 2018) #DigitalDeceit: The Technologies Behind Precision Propaganda on the Internet, New America
[8] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
[9] Li, Y. Chang, M.C. Lyu, S. (June 11, 2018) In Ictu Oculi: Exposing AI Generated Fake Face

Videos by Detecting Eye Blinking, Computer Science Department, University at Albany, SUNY

[10] Ince, D. (2013) A Dictionary of the Internet (3 ed.), Oxford University Press

[11] MacAllister, J. (2017) The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information, Fordham Law Review, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5370&context=fl

[12] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[13] Mantzarlis, A. (2015) Will Verification Kill Fact-Checking?, The Poynter Institute, https://www.poynter.org/news/will-verification-kill-fact-checking

[14] Funke, D. (2018) Report: There are 149 fact-checking projects in 53 countries. That's a new high, The Poynter Institute, https://www.poynter.org/news/report-there-are-149-fact-checking-projects-53-countries-thats-new-high

[15] Gu, L., V. Kropotov & F. Yarochkin (2017) The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public. Oxford University, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-howpropagandists-abuse-the-internet.pdf

[16] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[17] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[18] Gu, L., V. Kropotov & F. Yarochkin (2017) The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public. Oxford University, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-howpropagandists-abuse-the-internet.pdf

[19] Dawkins, R. (1976) The Selfish Gene. Oxford University Press.

[20] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[21] Jack, C. (2017) Lexicon of Lies, Data & Society, https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf

[22] Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

[23] Hofileña, C. F. (Oct. 9, 2016) Fake accounts, manufactured reality on social media, Rappler, https://www.rappler.com/newsbreak/investigative/148347-fake-accounts-manufactured-reality-social-media

[24] Office of the Director of National Intelligence. (2017). Assessing Russian activities and intentions in recent US elections. Washington, D.C.: National Intelligence Council, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[25] Mantzarlis, A. (2015) Will Verification Kill Fact-Checking?, The Poynter Institute, https://www.poynter.org/news/will-verification-kill-fact-checking