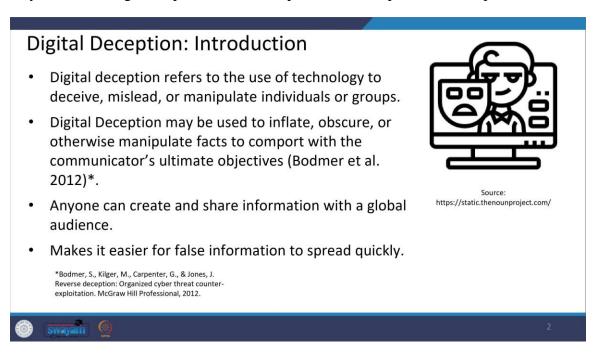
Online Communication in the Digital Age Prof. Rashmi Gaur Department of Humanities and Social Sciences Indian Institute of Technology Lecture – 44

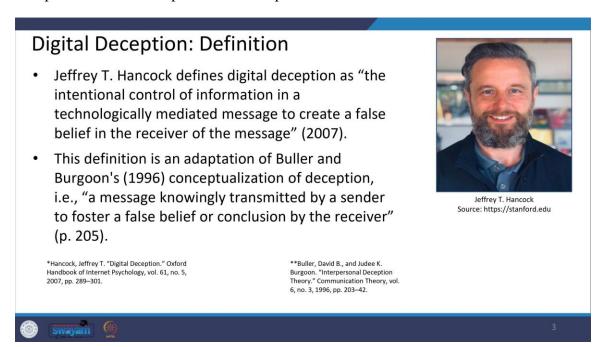
Digital Deception: Introduction

Good morning dear friends and welcome to today's module. In today's module, we will be exploring the concept of digital deception. In recent years, digital deception has become a growing concern as technological advancements have made it easier for individuals to spread false information and manipulate others online using the tools of digital communication. This module will explore the concept of digital deception, the reasons why it is becoming more prevalent and the potential consequences of this phenomenon.



Digital deception refers to the use of technology to deceive, mislead or manipulate either individuals or groups or certain sections of society. It may be used to inflate, obscure or otherwise manipulate facts to comport with the communicators ultimate objectives. Anyone can create and share information with a global audience immediately and makes it easier for false information to spread in a quick fashion.

In a previous module, we have discussed the concepts of cognitive dissonance, filter bubbles and echo chambers. We find that these concepts are highly relevant to today's discussion also. In an era characterized by the pervasive influence of digital communication, the notion of deception has taken new dimensions and complexities which is explained with the help of these concepts.



I would prefer to quote Jeffrey Hancock who has defined digital deception as the intentional control of information in a technologically mediated message to create a false belief in the receiver of the message. This definition is an adaptation of Buller and Burjoun's conceptualization of deception which they had proposed in 1996. They had suggested that a message which is knowingly transmitted by a sender to foster a false belief or conclusion by the receive is digital deception.

This module further delves into Hancock's adapted definition, shedding light on the deliberate maneuvering of information in digital messages to perpetuate deceit. It is also crucial in this context to understand the different forms of digital deception, the reasons for its rise and the potential consequences of this phenomenon. One of the reasons why digital deception is becoming more prevalent nowadays is the ease with which false information can be created and spread online. Anyone with an internet connection can now create a website or a social media account and share information with the global audience without any time gap. It can also put on different masks. Also there are fewer gatekeepers to verify the accuracy of the information making it easier for false information to spread quickly. Let us look at some factors that facilitate such deceptive behaviors in online digital communication.

Rise of Digital Deception

Anonymity: Digital communication platforms, such as social media, can amplify the feasibility of individuals partaking in deceitful conduct, enjoying a reduced likelihood of detection or culpability.

Ease of access:

- Case and Given (2016)* have noted that with the internet, information availability is no longer a problem.
- However, tools like social media bots or deep fakes can spread false information quickly and efficiently, making it difficult for people to distinguish between truth and falsehood.



Source: https://lepide.com

*Case, D.O. & Given, L.M. Looking for information: a survey of research on information seeking, needs, and behaviour (4th). Emerald Group Publishing, 2016.





One of the primary factors which has given rise to digital deception is the anonymity of it. Digital communication platforms such as social media etc. can amplify the feasibility of individuals partaking in deceitful conduct and enjoying a reduced likelihood of detection or culpability. The second aspect related to it is the ease of access. Case and given have noted that with the internet information availability is no longer a problem. However, tools like social media bots or deep fakes can spread false information quickly and efficiently making it difficult for people to distinguish between the truth and the falsehood.

Furthermore, financial incentives as well as ideological and political motivations play a huge part in the rise of digital deception.

 Financial incentives: Some individuals or organizations may engage in digital deception to generate profit.

Example: Clickbait articles or fake news stories can generate advertising revenue for websites, even if the content is false.

 Ideological or political motivations: Some individuals or organizations may engage in digital deception to create conspiracy theory networks that promote a particular ideology or political agenda (Ghosh and Scott, 2018)*.

Example: Spreading false information or propaganda through social media, online forums, or websites.

*Ghosh, Dipayan, and Ben Scott. "Digital deceit: the technologies behind precision propaganda on the internet." New America, 2018.



Source: https://cdn.aarp.net

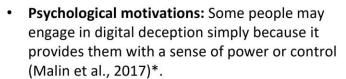


1

Sometimes we find that certain individuals or even organizations or certain groups of people may engage in digital deception to generate profit. For example, clickbait articles or fake news stories can generate advertising revenue for websites even if the content is fake. Another aspect is related with the ideological or political motivations. Some individuals or organizations may engage in digital deception in order to create conspiracy theory networks that promote a particular ideology or a particular political agenda. We can understand it better by looking at the websites, online forums and social media accounts through which false information or propaganda is spread and generated further.

And finally, it is the lack of regulation and psychological motivations which are important factors that have contributed to the spread of digital deception.







Source: https://shutterstock.com

*Maungwa, T. & Fourie, I. Exploring and understanding the causes of competitive intelligence failures: an information behaviour lens. Information Research, 23(4), 2018.

**Malin, Cameron H., et al. Deception in the digital age: exploiting and defending human targets through computer-mediated communications. Elsevier, 2017.



(

The digital realm exhibits a notable lack of comprehensive regulations and therefore it creates a conducive environment for individuals and entities to partake in deceptive maneuvers without any immediate apprehension of legal consequences. Similarly, some people may engage in digital deception simply because it provides them a false sense of power or control over others.

Digital deception can have serious consequences for individuals, organizations and society. Let us look at some of the potential consequences of digital deception.

Consequences of Digital Deception

- Reputation Damage: Individuals and organizations suffer harm to their reputation, leading to enduring detriments in terms of opportunities and prospects.
- Loss of Trust: Deterioration of trust between entities impedes the capacity for well-informed choices and substantive initiatives.
- Financial Loss: Individuals and organizations encounter fiscal losses attributable to fraudulent activities or deceptive stratagems.
- Sociopolitical Effects: Manipulated information gives rise to political instability, societal fractures, and heightened cybersecurity vulnerabilities.



Source: https://www.istockphoto.com



7

It immediately results in a damage to the reputation, a loss of trust, financial loss as well as certain socio-political effects in a negative manner. Individuals and organizations who are involved with any aspect of digital deception suffer from a harm to their reputation leading to enduring detriments in terms of further opportunities and future prospects. It also results in a deterioration of trust between entities and impedes the capacity for well-informed choices and substantive initiatives. Though immediately it may seem that digital deception leads to certain financial gains, but ultimately we find that individuals and organizations encounter fiscal losses attributable to fraudulent activities or deceptive stratagems immediately they are caught by the law enforcement agencies. Similarly, manipulated information gives rise to political instability, societal fractures and heightened cyber security vulnerabilities and all the nations consider them as criminal activities.

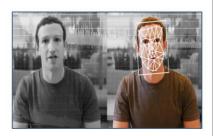
Further, the digital deception landscape has continued to evolve in the current era presenting new challenges. With the rapid progress in artificial intelligence technology, the creation and dissemination of AI generated deep fake videos have become increasingly prevalent. The rise of deep fakes has raised concerns about the potential for widespread misinformation and the erosion of trust in visual evidence.

Deep fakes are synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another. They are the manipulation of facial appearance through deep generative methods. Though similar type of digital deception has been practiced since 1990s, we find that AI has introduced a better ease as well as more challenges with different available tools.

Latest Developments

Al-generated deepfakes:

- Advancements in artificial intelligence have made it easier to create highly realistic deepfake videos, which can be used to manipulate and deceive viewers (Fraga-Lamas and Fernandez-Caramés, 2020)*.
- These manipulated videos use machine learning algorithms to superimpose someone's face onto another person or alter their appearance and actions, resulting in highly convincing but fabricated content.



Source: https://i.insider.com

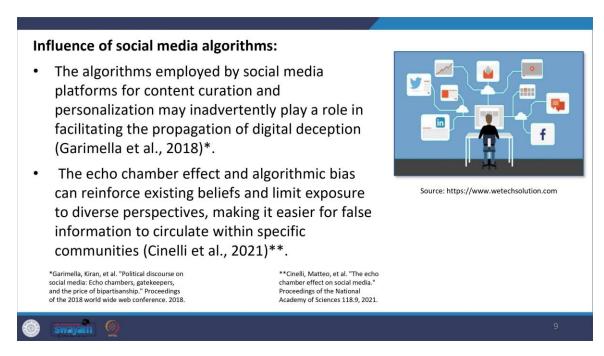
*Fraga-Lamas, Paula, and Tiago M. Fernandez-Caramés.
"Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality." IT professional 22.2 (2020): 53-59.



g

AI related advancements have made it easier to create highly realistic deep fake videos which can be used to manipulate and deceive viewers. These manipulative videos use machine learning algorithms to superimpose someone's face onto another person or alter their appearances and actions resulting in highly convincing but absolutely fabricated content.

Some popular AI tools which are being commonly used nowadays to create deep fakes are DeepSwap, FaceMagic, SwapStream, DeepFakesWeb or FaceHub etc. They are so easy to use that they require only a few clicks and almost all of them do not even require a download. And therefore some of these tools can be used to create deep fakes even during a live streaming. Moreover, social media platforms like Facebook employ complex algorithms that determine the content users see on their feeds often based on their preferences and engagement patterns.



The algorithms which are employed by social media platforms for content curation and personalization may inadvertently play a role in facilitating the propagation of digital deception. The echo chamber effect and algorithmic bias can reinforce existing beliefs and limit our exposure to diverse perspective making it easier for false information to circulate within specific communities.

Let us take a look at a video that explains how these algorithms function.



Something interesting, we have to find out the right time frame. In an era of digital deception scientists at Indiana University are using Twitter to investigate the nature of truth, lies and politics. The research program deals with how social media shape political communication and the more basic question is how ideas and information spread between people when they interact using technology.

They are working on ways to detect and diffuse Twitter misinformation campaigns. They call it the truthy project. Every day their computers at Indiana's center for complex networks and system research scan millions of Twitter messages looking for the line between free speech and fraud. So far they have found dozens of cases in which activists orchestrated networks of dummy Twitter accounts to sway voters or influence pending legislation. We have the impression that we have just scratched the surface, the tip of the iceberg because as soon as we started looking even before we knew that there was much of this going on we found lots of examples.

Sometimes prolific political tweeters are really automated computer programs designed to mimic human behavior and these Twitter tactics are cheap since user accounts are free and could potentially reach many more people than traditional attack ads. It's known as astroturfing, a fake grassroots political campaign. There is a lot of money around politics and a lot of influence that we've seen spent through TV campaigns for example and compared to that an astroturf campaign is very, very, very cheap. All you need is just an operative or a volunteer with or without the consent of the people that they are trying to promote who just sits down, creates a bunch of fake accounts and with a little bit of very simple scripts they can be up and running in minutes or in a few hours and in some cases they might get lucky and create quite an amount of attention. A single tweet topic can explode as others retweet it to friends who relay it in turn to friends of theirs.

In one case, the Truthy Project uncovered a pair of accounts that mimicking the chatter of two politically active women sent out more than 20,000 messages promoting congressional candidates, echoing each other's messages to create the illusion of a conversation and a groundswell of grassroots support. The system noticed that there was this pattern in which two accounts were constantly retweeting each other and one account was producing lots of content, mostly supporting and promoting one particular candidate or a small group of candidates. The other account just retweeted everything that this one account posted. And then they retweeted each other. And so we had these two nodes with a huge connection between them representing thousands and thousands of messages exchanged between these two accounts.

And when we looked, all these messages were the same or were the same kind of message. So that these messages contributed to give the appearance that there was a huge amount of chatter around this candidate. In fact, it was all fake, automatically generated by scripts. And when we posted about it, Twitter almost immediately shut down those accounts. Unchecked, these torrents of texts can drive a Twitter topic higher in web search engine rankings, where it can attract broader media attention.

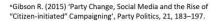
By studying Twitter, the researchers are hoping to learn more about how ideas spread and how people use the messaging service to influence each other. When people communicate online, they create trace data. And we can look at this to understand how they're communicating with each other about politics and what that means for democracy. The Indiana scientists are worried, though, that these digital deceptions that they've discovered undercut the trust that holds our society together. A well-functioning democracy requires accountability and trust.

And if we are in a situation where, as a result of technology, we have eroded our trust in the validity or verifiability of the information we're receiving, that's a very dangerous situation because democracy requires trust. By its terms of service, Twitter company rules forbid spam and efforts to mislead, confuse or deceive people. And routinely, the company takes down accounts its logarithms have determined are fake. But this sort of organized deception may be evolving faster than the company's security measures can control them. For The Wall Street Journal. science writer I'm Robert Lee Hotz.

Consequently, social media's advertising capabilities have been scrutinized for their potential to influence political campaigns and target specific groups with tailored messages.

Influence on Political Campaigns and Elections

- Since the 1990s, political parties have become heavily dependent on digital technology (Gibson, 2015)*.
- Social media's extensive reach and targeting capabilities have made it a prominent platform for political campaigns and election advertising.
- The ability to micro-target specific demographics has raised concerns about the impact of personalized political messaging and potential manipulation (Aldrich et al., 2016)
- Instances of foreign interference in elections, such as the Cambridge Analytica scandal, have highlighted the need for transparency and safeguards.



**Aldrich J., Gibson R., Cantijoch M, Konitzer T. (2016) Getting Out the Vote in the Social Media Era: Are Digital Tools Changing the Extent, Nature And Impact of Party Contacting in Elections?', Party Politics, 22, 165–178.



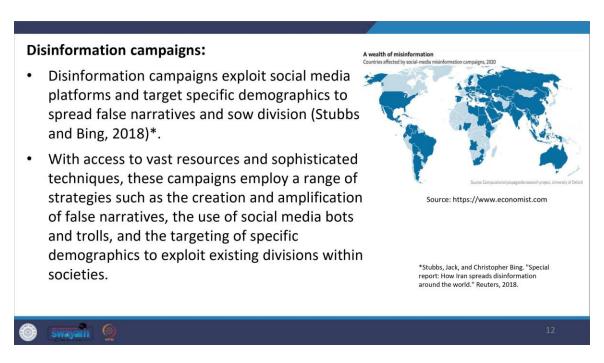
Source: https://albatrossmedia.ir



1

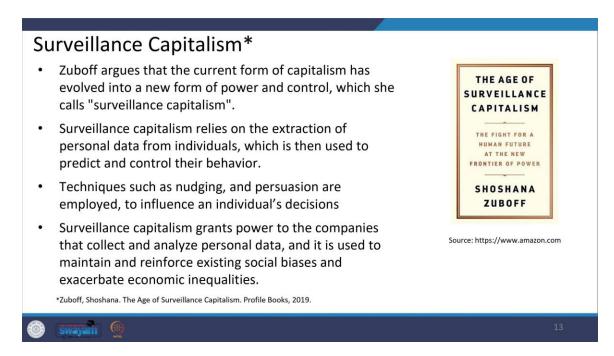
Since the 1990s, political parties are becoming more and more dependent on digital technology. Social media's extensive reach and the capabilities to target multiple audience simultaneously have made it a prominent platform for political campaigns and election advertising. The ability to micro-target specific demographics has raised concerns about the impact of personalized political messaging and potential manipulation. Instances of foreign interference in elections, such as the Cambridge Analytica scandal, have highlighted the need for transparency and stricter safeguards.

Similarly, deliberately planned disinformation campaigns have also become unfortunately a powerful tool in shaping public opinion and manipulating social and political landscapes.



Disinformation campaigns exploit social media platforms and target specific demographics to spread false narratives and thereby to sow division. With access to vast resources and sophisticated techniques, these campaigns employ a range of strategies such as the creation and amplification of false narratives, the use of social media bots and trolls and the targeting of specific demographics to exploit existing divisions within different social groups.

The goal is to sway public opinion, undermine trust in democratic institutions and disrupt the democratic processes ultimately. Additionally, algorithmic bias can lead to the amplification of sensational or misleading content, further exacerbating the spread of misinformation. Thus, these alternate realities portrayed on social media platforms have led to the rise of what Shoshana Zuboff has called as surveillance capitalism.



Zuboff argues that the current form of capitalism has evolved into a new form of power and control which she has called surveillance capitalism. In her opinion, surveillance capitalism relies on the extraction of personal data from individuals which is then used to predict and control the behaviour. Techniques such as nudging and persuasion are employed to influence an individual's decisions. Surveillance capitalism grants power to the companies that collect and analyse personal data and it is used to maintain and reinforce existing social biases and exacerbate economic inequalities.

Zuboff argues that the rise of surveillance capitalism has created a need for a new social contract that recognises these challenges and aims to prevent the misuse of personal data. However, the dynamic nature of digital deception poses significant challenges for policy makers and law enforcement agencies tasked with regulating and combating deceptive practices.

Challenges in regulation and enforcement:

- The decentralized and global nature of the internet makes it difficult to enforce consistent regulations across jurisdictions. (Bayer et al. 2019)
- The speed at which misinformation can spread across borders, coupled with the anonymity afforded by online platforms, presents challenges in holding perpetrators accountable.

*J. Bayer, N. Bitiukova, P. Bârd, J. Szakâcs, A. Alemanno and E. Uszkiewicz, Disinformation and Propaganda—Impact on the Functioning of the Rule of Law in the EU and its Member State., 2019.



Source: https://builtin.com



14

We should also be alert to the fact that the global and decentralised nature of the internet makes it difficult to enforce consistent regulation across jurisdictions. The speed at which misinformation can spread across borders coupled with the anonymity afforded by online platforms presents challenges in holding perpetrators accountable and to hold them responsible under the criminal justice programmes.

Policy makers face the delicate task of balancing freedom of speech with the need to protect individuals and societies from the harmful effects of digital deception. Overall, the consequences of digital deception are far-reaching and can have serious implications for individuals, organisations and society as a whole. It is therefore important to be aware of the potential risks and to take steps to counter digital deception. Successful initiatives and campaigns have now emerged to counter the impact of digital deception and promote a more informed and discerning public. Fact-checking organisations have now become vital in debunking false information and providing accurate alternatives.

Fact-Checking Organizations*

- Organizations such as Snopes, PolitiFact, and FactCheck.org have played a crucial role in countering digital deception.
- They employ a team of fact-checkers who investigate and debunk false information, providing the public with accurate and reliable information to counteract the spread of misinformation.
- Many evaluation criteria or visual metrics are used to determine the truthful level of the news in current factchecking resources.

*X. Zhang and A. A. Ghorbani, "An overview of online fake news: Characterization detection and discussion", Inf. Process. Manage., vol. 57, no. 2, 2020.



Source: https://www.who.int







We can refer to organisations such as Snopes, PolitiFact and FactCheck.org which have played a crucial role in countering digital deception. They employ a team of fact-checkers who investigate and ultimately debunk false information providing the public with accurate and reliable information to counteract the spread of misinformation. Many evaluation criteria or visual metrics are used to determine the truthful level of the news in current fact-checking resources.

At the same time, media literacy programmes equip individuals with the tools to navigate the digital landscape effectively, empowering them to critically assess information.

Media Literacy Programs*

- Various initiatives and educational programs have been implemented to promote media literacy and critical thinking skills.
- These programs aim to empower individuals to assess the credibility of information, identify bias, and navigate the digital landscape more effectively.
- Examples include **NewsGuard's** media literacy program and the **MediaWise** initiative by the Poynter Institute.



Source: https://ssir.org

*Bulger, Monica, and Patrick Davison. "The promises, challenges, and futures of media literacy." (2018).







In order to promote media literacy and critical thinking skills, we find that various initiatives and educational programmes have been implemented. These programmes aim to empower individuals to assess the credibility of information, identify bias and navigate the digital landscape more effectively. Examples include NewsGuard's media literacy programme and the MediaWise initiatives by the Poynter Institute.

Collaboration between social media platforms and fact-checkers have resulted in the flagging and removal of false content.

Collaborative Efforts by Social Media Platforms

- Social media platforms have recognized the need to address digital deception and have implemented measures to combat the spread of false information.
- For instance, platforms like Facebook and Twitter have partnered with fact-checking organizations to flag and reduce the visibility of false content.
- They have also introduced policies and algorithms to detect and remove malicious accounts and bot networks.



Source: https://about.fb.com





Social media platforms have also recognised the need to address digital deception and have implemented measures to combat the spread of false information. For instance, platforms like Facebook and Twitter have partnered with fact-checking organisations to flag and reduce the visibility of false content. They have also introduced policies and algorithms to detect and remove malicious accounts and bot networks. The picture on the right-hand side also illustrates an example to it.

Finally, public awareness campaigns have sought to educate individuals about the damages of digital deception.

Public Awareness Campaigns

- Governments, nonprofit organizations, and media outlets have launched public awareness campaigns to educate individuals about the dangers of digital deception.
- These campaigns aim to raise awareness, encourage critical thinking, and promote responsible digital behavior.
- Examples include the European Union's #EUvsDisinfo campaign and the BBC's "Beyond Fake News" initiative.



Source: https://ichef.bbci.co.uk



Several governments, non-profit organisations and media outlets have launched public awareness campaigns to educate individuals about the dangers of digital deception. These campaigns aim to raise awareness, encourage critical thinking and promote responsible digital behaviour. Examples include the European Union's EU versus Disinfo campaign and the BBC's Beyond Fake News initiatives.

These proactive measures collectively contribute to mitigating the spread and impact of misinformation, fostering a more informed and resilient society. Further, let us look at some real-world case studies to help contextualise the information we have looked at up till this point. Our first case study examines the development and curation of a GIF of Donald Trump tackling a CNN logo and what Trump's tweeting of the GIF means as a form of online harassment as well as digital aggression.

Case Study-Trump vs CNN

- This GIF originated on a subreddit known for sharing misogynistic, sexist, racist, ableist, and other problematic content, which Trump then recirculated on Twitter to make a claim about CNN being "fake news."
- The location where the GIF originated is problematic, as is the content of the GIF itself as it promotes violence and aggression toward the news media specifically.



Source: https://www.makeagif.com



19

This GIF originated on a subreddit known for sharing misogynistic sexist, racist, ableist and other problematic content which Trump then recirculated on Twitter to make a claim about CNN being fake news. The location where the GIF originated is problematic as is the content of the GIF itself as it promotes violence and aggression towards the news media specifically.

Trump often used Twitter to attack CNN using derogatory language and accusing the network of spreading fake news. CNN in turn sought to hold Trump accountable for his statements and actions often using provocative headlines and commentary to draw attention to his perceived missteps. CNN reported that Trump and his son had received an email containing stolen Democratic National Committee documents before they were released publicly.



President Trump had issued a charge against CNN in January 2017 when he chastised the broadcast channel for its coverage of the Steele dossier. The CNN had proceeded with this report claiming to possess facts of the FBI's briefing for the President-elect about the dossier. The Steele dossier as part of it had been circulating within Washington for months and was about to be published though without permission by the online news site BuzzFeed.

The CNN report was later retracted when it was discovered that the email had actually been sent after the documents were publicly available. In retaliation, Trump frequently used Twitter to attack CNN and its reporters calling them fake news and accusing them of having a certain bias against him. Let us look at a brief video which illustrates it further.



During the whole process, CNN kept on using provocative headlines and commentary to draw attention to Trump's perceived missteps such as the controversy surrounding his comments about the Charlotte's village protest in 2017. Thus, this case study provides an example of the role of media in what Marwick and Levis have called agenda setting.

Marwick and Lewis (2017)* noted:

- For manipulators, it doesn't matter if the media is reporting on a story in order to debunk or dismiss it; the important thing is getting it covered in the first place.
- The amount of media coverage devoted to specific issues influences the presumed importance of these issues to the public.
- This phenomenon, called agenda setting, means that the media is remarkably influential in determining what people think about. (p. 39)



Source: https://www.mediamanipulation.org

*Marwick, Alice E., and Rebecca Lewis. Media Manipulation and Disinformation Online. 2017.







It would be pertinent to quote Marwick and Levis in somewhat detail and I quote, for manipulators it does not matter if the media is reporting on a story in order to debunk or dismiss it. The important thing is getting it covered in the first place. So this part of the quote relates with the haste media has to be the first to report on a particular aspect. The quote continues, the amount of media coverage devoted to specific issues influences the presumed importance of these issues to the public. This part of the quote refers to the reach and the immediacy of the online media. Further, Marwick and Levis comment that this phenomenon called agenda setting means that the media is remarkably influential in determining what people think about. So, Marwick and Levis have clearly pointed out that this type of media spread and breach can be manipulated to propagate false information and thereby to set an agenda which may not be necessarily in the interest of the people.

The conflict between Trump and CNN also involved online harassment with supporters of both sides engaging in abusive behaviours towards each other on social media. Overall, this feud between Trump and CNN serves as an important example of digital deception in politics, highlighting the need for increased awareness, better transparency and accountability in the online sphere. It also underscores the importance of promoting responsible digital citizenship and ethical online behaviour in order to build a better informed and a more engaged public.

In conclusion, we can say that digital deception poses a significant and complex challenge in our interconnected world.



As we have seen, it is becoming increasingly sophisticated and challenging to detect digital deception now. It has also become easier for individuals and organisations to spread false information through social media and manipulate media to suit their own agenda. This also

has led to a proliferation of fake news stories and misinformation campaigns which can be difficult to distinguish from legitimate news sources. Misinformation and false narratives can be used to sow division and discord, undermine trust in institutions and influence political outcome.

As we move forward, it is imperative for individuals, organisations and policy makers to work together to enhance cyber security measures, improve media literacy and promote responsible digital behaviour. By doing so, we can protect ourselves from the harmful impacts of digital deception, safeguard the integrity of information and uphold the principles of truth and trust in the digital age. In the next module, we will be looking at some other aspects related to it.

Thank you.