Monetisation of Fake News in the Cyber Domain: A Roadmap for Building Domestic and International Cyber Resilience

Usama Nizamani[*]

Abstract

The online domain has witnessed the proliferation of fake news in the past few years all over the world. This overwhelming amount of (dis)information has created incentives for the proliferators of fake news to benefit from ongoing political developments across the world, due to the courtesy of the existing model of online revenue generation on the Internet. The unregulated, liberal and open nature of the Internet has created an unintended consequence of incentive maximisation for fake news. This paper takes an analytical look at the relationship between revenue generation model in the cyber-domain and how content producers of fake news benefit from it. This paper postulates that the existing online advertisement model remains lucrative for fake news publishers particularly in regions such as South Asia. Its interplay with social media platforms enables further monetisation and spreading of fake news to Internet users. It analyses the relationship between these factors and suggests cross-sector solutions for de-incentivising and countering fake news in the cyber domain.

Keywords: Fake News, Programmatic Advertising, Advertisement-Dollars, Internet Intermediaries, Media Literacy, Online Revenue Generation Model.

Introduction

Fake news is defined as "false stories that appear as news, spread on the Internet and usually created to influence political views or as a joke."[1] Fake

[*] *The author is Consultant at the Islamabad Policy Research Institute (IPRI).*

[1] "Fake News," meaning in the Cambridge English Dictionary, n.d., https://dictionary.cambridge.org/dictionary/english/fake-news

news is promoted by various actors and for different motives.[2] These motives range from publishing commercially-driven sensational content mainly for earning online advertisement revenue and launching government-sponsored misinformation campaigns,[3] generating swarms of *Twitter* and *Facebook* both accounts and producing satire or parody content.[4] The 2016 US elections changed the very perception of fake news. The reach of fake news made democracies, Internet tech firms such as *Facebook* and *Google* and even media outlets realise that it can disrupt the environments in which democracies have normally operated so far.

In accordance with the research findings, various driving factors have been identified for fake news production, which often ranges from making money, spreading disinformation to influence democratic electoral process and also for the accomplishment of the ulterior political or commercial objective.[5] While fake news is also published and disseminated for geopolitical purposes, the fake news publishers often engage in its publication for the end-objective of earning money or monetising their fake news stories.

Before the advent of the Internet, the production of fake news was so costly[6] that it alone worked as a deterrent. In the US, a group named *Yes Man* printed a parody of *Washington Post* with anti-Trump content, which cost US$30,000 to producers and publishers of fake news.[7] However, the Internet and Social Media have reduced the cost and reach while incentivising the production and sustainability of fake news itself. Users of social media and the Internet are also unable to tell the difference between the *Washington Post* or a dubious news publisher as *Denver Guardian.*[8]

[2] James Carson, "Fake News: What Exactly is it – and How Can you Spot it?," *Telegraph,* November 20, 2019, https://www.telegraph.co.uk/technology/0/fake-news-exactly-has-really-had-influence/

[3] Campaigns that are specifically designed by government to promote its propaganda against domestic or external actors.

[4] Carson, "Fake News."

[5] Abby Ohlheiser, "This is How Facebook's Fake News Writers Make Money," *Washington Post,* November 18, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/

[6] Zeynep Tufekci, "The Imperfect Truth about Finding Facts in a World of Fakes," *Wired,* February 18, 2019, https://www.wired.com/story/zeynep-tufekci-facts-fake-news-verification/.

[7] Ibid.

[8] Ibid.

Fake news was disseminated during the US election 2016[9] and in the post-referendum phase of Brexit, Russia based company Internet Research Agency employed fake accounts on *Twitter* to spread fake stories.[10] Some of these stories spread anti-Muslim content against the local British Muslim community in order to polarise the society.[11]

During the US elections in 2016, fake news resulted in more engagement on social media than the 20 mainstream news combined.[12] Some of the fake news came from a small European country, Macedonia, which, despite its small population, has a large tech-savvy youth that is seeking opportunities through freelancing and IT-related work. In an interview to *AJ+* (*Al Jazeera+*) Monika Bickert, Head of Global Policy at *Facebook* acknowledged that there are nearly 87 million fake accounts on the platform itself. Some of the Macedonian youths earned a fortune, as much as US$100,000 a month. *Buzzfeed* reported that other successful individuals made US$5,000 per month.[13] The proliferation of fake news occurred as a result of demand-supply cycle.[14]

This perception that fake news flourishes in a vacuum in the cyber domain does not hold ground. In the US and other countries, fake news circulated due to the high demand for sensational content. Given this demand, the suppliers of fake news proliferated to meet this ever-growing demand. Similarly, it is also believed that factors such as confirmation bias[15] are some of the reasons why people fall for false stories.[16] The

[9] Katie Rogers and Jonah Engel Bromwich, "The Hoaxes, Fake News and Misinformation We Saw on Election Day," *New York Times,* November 8, 2016, https://www.nytimes.com/2016/11/09/us/politics/debunk-fake-news-election-day.html

[10] Robert Booth, et.al., "Russia used Hundreds of Fake Accounts to Tweet about Brexit, Data Shows," *Guardian,* November 14, 2017, https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets

[11] Ibid.

[12] "Macedonia's Fake News Factories," *You Tube*, last modified, June 19, 2018, https://www.youtube.com/watch?v=qjnsV8MhVK8

[13] Ohlheiser, "This is How Facebook's Fake-News Writers Make Money."

[14] "Macedonia's Fake News Factories."

[15] Peter Cohan, "Does Facebook Generate Over Half of its Ad Revenue from Fake News?," *Forbes,* November 25, 2016, https://www.forbes.com/sites/petercohan/2016/11/25/does-facebook-generate-over-half-its-revenue-from-fake-news/

relationship between fake news and its driving different factors have been studied in various researches: fake news contents and their reach through social media and its effects on democracies and democratic institutions.[17] However, data is limited on the monetisation of fake news and its relationship with programmatic advertising, social media platforms and online advertisement tools which serve to monetise and sustain resources for proliferation and continuation of fake news over the Internet.

With this background, this paper will examine structural factors such as Internet Ecosystem that enables or allows presence and at times, enable unintended mushrooming of objectionable content such as fake news, hate speech and extremist violence. Despite various attempts to control the spread of fake news by Internet intermediaries such as *Facebook* and *Google*, it still continues to exist and pose a significant problem.[18] The paper then extends the discussion and explains the online revenue generation strategy employed by fake news publishers, followed by an overview of the role of groups such as *Facebook* and *Google* in the catalytic role between fake news and Internet platforms.

In addition, the role of privacy practices on these platforms is also considered and how this serves in monetising fake news. The discussion also highlights examples from Pakistan, India, Bangladesh and Sri Lanka. It explores a range of options for multiple stakeholders at different tiers as measures against increasing the reach and monetisation of fake news by government institutions, private corporations, civil society organisations, media, advertisement agencies, brands and exploring technological solutions for limiting monetisation of the fake news publication.

This paper is a qualitative study which relies on secondary data from academic studies, reports, documentaries, newspaper reports and articles on fake news. It particularly reviews the literature on the monetisation of fake news and existing online advertisement model. The existing ecosystem of

[16] "Macedonia's Fake News Factories."

[17] Edda Humprecht, "Where 'Fake News' Flourishes: a Comparison Across Four Western Democracies," *Information, Communication & Society* 22, no. 13 (2018): 13, doi:10.1080/1369118x.2018.1474241.

[18] Foo Yun Chee, "Google, Facebook, Twitter Must Do More Against Fake News: EU," *Reuters*, January 29, 2019, https://www.reuters.com/article/us-eu-tech-fakenews/google-facebook-twitter-must-do-more-against-fake-news-eu-idUSKCN1PN1QW

the Internet and online advertisement model allows fake news publishers to monetise their content. It enables them to profit from it and expand their reach through the use of social media platforms and online advertisement business-model.

This study, in particular, identifies the relationship between social media and Internet intermediaries that indirectly incentivises and expands the reach of fake news. Presence of fake news on the cyber domain in South Asia is also analysed. This study prescribes cross-sector cooperation between different bodies to de-incentivise and limits the reach of fake news over the Internet.

Internet Ecosystem and Fake News Publishers

An often-overlooked factor, while understanding the existence of fake news, hate-speech, terrorism and violent extremism is the structure of the Internet and the manner in which it affects the presence of certain content. Although, some content falls in zero-tolerance space such as child pornography, drug and arms sales, the demand for such products is still satiated on the dark web.[19] Interestingly, those seeking to monetise fake news do not operate on the dark web. However, what has largely led to the unhindered proliferation of fake news over the Internet, particularly popping up of the fake news websites is due to the ecosystem of the Internet itself. The Internet Ecosystem is critical to the emergence of fake news.[20] It happens due to the internationalised nature of the Internet, which was done by keeping the Internet as free and open so that it serves as a medium for benefitting the masses. As a result, the Internet did not develop into a uniform entity, which may serve to regulate the content that appears on it.

While some critics may raise alarm bells about the absence of a uniform entity which polices the Internet or regulates the content which appears on it by the hour, it is this very architecture of the Internet that has proven to be

[19] Eric Jadine, "The Dark Web Dilemma: Tor, Anonymity and Online Policing," *Global Commission on Internet Paper Series* 21, (2015): 7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711

[20] L Gordon Crovitz, "A New Business Takes on Fake News," *Wall Street Journal,* March 4, 2018, https://www.wsj.com/articles/a-new-business-takes-on-fake-news-1520189066

revolutionary. The existing ecology of the Internet is based on a multi-stakeholder approach,[21] which comprises of a range of actors such as:

a) The Internet Corporation for Assigned Names and Numbers (ICANN)
b) Internet Engineering Task Force (IETF)
c) World Wide Web Consortium (W3C)
d) Internet Assigned Numbers Authority (IANA)
e) Internet Operators
f) Engineers
g) Internet vendors such as Domain Name Service providers,
h) Network Operators
i) Internet Exchange Points[22]

These actors follow the common principle of the free flow of altruistic and commercial ideas and information. This has also led to the denial of an exercising monopoly over information by the privileged over the non-privileged segments of the world and society.[23] However, this very ecosystem allows fake news publishers to produce, publish, disseminate and monetise their content. Satire news often uses false information combined with exaggerated satire humour. Fake news also shares the common denominator of false information with satire news, thus, often blurring the lines between the two.

The creators and proliferators of fake news operate in the open while engaging with normal Internet users in order to monetise their content. The presence of giant Internet intermediaries and social media and advertisement firms such as *Facebook* and *Google*, played an enabling role for fake news publishers to expand their reach to a wider number of audiences. This factor has also raised the issue of far more assumption of responsibility by social media companies to take measures to control the reach of fake news. Reaching a large number of Internet users is the sole

[21] "Internet Governance ─ Why the Multi-stakeholder Approach Works," Internet Society, last modified April 26, 2016, https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/

[22] "Who Makes the Internet Work: The Internet Ecosystem," Internet Society, last modified February 3, 2014, https://www.internetsociety.org/internet/who-makes-it-work

[23] "Internet Governance."

motivator of fake news publishers in the cyber domain that intend to monetise and profit from their content.

There are many others that use publication and wider dissemination of fake news for political or larger geopolitical objectives such as governments or a company like Internet Research Agency (IRA), giant Internet advertisement and social media companies such as *Google* and *Facebook*, along with ad-tech firms remain critical to the monetisation of fake news. The extensive user-base and reach of social media companies enabled fake news producers to profit during the 2016 US elections and also during the Brexit referendum. Examination of the major interventions used by fake news publishers to produce, disseminate and monetise their content are critical to understanding the very strategies employed by fake news publishers to monetise and commercialise their content.

Online Revenue Generation Model and Fake News Publishers

The available literature on the monetisation of fake news in the cyber domain has analysed various steps that are undertaken from producing fake news content to monetising it and expanding its reach for reinforcing the incentives and the reach of fake news content and their websites.[24] The research compiled by the Centre for Information Technology and Society at the University of California, Santa Barbara, identified five steps that producers of fake news tend to follow.[25] In the cyber domain, the first step comprises setting up a website featuring fake news content. To do so, producers of fake news will buy a relatively cheap domain name that sounds familiar or nearly identical to authentic news websites. Some website providers will sell such domain names for a fee as low as US$1 per year. A webhost technically provides the space for storing the website. The domain name, on the other hand, serves as the address to reach and have access to a website. Some webhosting will offer services for storage of content as low as US$2.75 a month.[26] To illustrate how easy it could be to impersonate a

[24] "Where Does Fake News Come From?," Centre for Information Technology and Society (CITS), https://www.cits.ucsb.edu/fake-news/where

[25] Ibid.

[26] Laura Sydell, "We Tracked Down a Fake-News Creator in the Suburbs: Here's What We Learned," *NPR*, November 23, 2016, https://www.npr.org/sections/alltechconsidered/2016/11/23/503146770/npr-finds-the-head-of-a-covert-fake-news-operation-in-the-suburbs

news website, consider the example of *www.dawn.com,* which is a legitimate news website; whereas the hypothetical domain name www.dawnnews.com may sound real it could supposedly be exploited for creating a fake-news website. The utilisation of such techniques is done primarily to make the domain name and fake news site catchier to Internet users, to attract as many clicks as possible and to attract dollars.

The second step involves stealing content from other websites including from satire websites, tabloid or *click-bait* websites. Clickbait is the practice of creating a sensationalistic, exaggerated, outright false headline and posting doctored images to attract clicks from users.[27] Doing so allows fake news producers to reduce the amount of time and effort invested in creating their own content. The report cites the third step when producers move to monetise their fake news content. For this purpose, online advertisement is put to use by providing some space of the website to advertising companies for displaying advertisements to website visitors.[28] The advertisement revenue is generated by attracting visits on the webpage and relatively more revenue is created when visitors click on advertisements. The role of ad-tech firms in this entire exercise is that of the middlemen for providing access to fake news producers to advertisers. Ad-tech companies develop algorithms which rely on tracking data, which is done through cookies that keep sending back information regarding the browsing behaviours of the users. These cookies keep track of what websites the users visited and clicked on. Based on these pieces of data, ad-tech firms build profiles of visitors. Subsequently, from this data, ad-tech firms then target with adverts the relevant products based on customised preferences of visitors.

The fourth step consists of expanding the reach of such fake news content or visits on fake news through the use of social media platforms. This has also been observed in the 2016 US Presidential elections.[29] Fake news producers often make pages and fake social media accounts in order to expand their reach. The last step comprises repeating the entire process since fake news

[27] "Where Does Fake News Come From?"

[28] Jonathan Albright, "#Election 2016: Propaganda-lytics & Weaponised Shadow Tracking," *Medium,* November 22, 2016, https://medium.com/@d1gi/election2016-propaganda-lytics-weaponized-shadow-trackers-a6c9281f5ef9

[29] Andrew Guess, Brendan Nyhan, Jason Reifler, "Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 US Presidential Campaign," European Research Council, January 9, 2018, https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf

producers prefer to employ different strategies to maintain the flow of monetary incentives.[30] Therefore, they will create multiple websites publishing similar content; as a result of this, some fake news websites will receive more traffic in comparison to other websites. When fake news websites are reported they are taken down but often start again from scratch with a new website.

One of the most important dimensions of online advertisement revenue generation employed by ad-tech firms is "programmatic advertising," which is the automated process of buying and selling ads through software. Such software mostly relies on machine learning algorithms to target segmented audiences matching a specific set of user-profile.[31] In this process, once a website is uploaded and made online, an automated auction takes place as the advertisers begin placing bids on it. These bids are based on what advertisers know about users visiting these pages. For this purpose, the website publisher first allocates a certain space on their websites for advertisement, the advertisers or the ad agencies subsequently place their bids, during this course ad-tech firms act as intermediaries.[32] In many ways, the ad-tech firms revolutionised the art of digital advertisement. These firms rely on behavioural targeting[33] leading advertisers to shift their marketing strategies, which centred on cultivating long-term brand loyalty to time-bound and immediate term interactions. This has also resulted in a changing shift in the advertisers' priorities to offer long-term news subsidies to the news channels in favour of online and programmatic advertisements.[34] These concerns are particularly important for Pakistan as Internet access becomes economical and wider throughout the country and region.

[30] Ibid.

[31] "What is Programmatic Advertising," Acuity, last modified December 15, 2017, https://www.acuityads.com/blog/2017/12/15/what-is-programmatic-advertising/

[32] Julian Thomas, "Programming, Filtering, Ad-blocking, Advertising and Media Automation," *Media International Australia,* 166 (2017): 34-43, https://doi.org/10.1177/1329878X17738787

[33] In behavioural targeting the advertisers and ad-tech firms focus on reaching the users while browsing the internet at the time when they are most likely to engage in a purchase of a good or service.

[34] Andrew Mcstay, "Micro-Moments, Liquidity, Intimacy and Automation: Developments in Programmatic Ad-Tech," in *Commercial Communication in the Digital Age – Information or Disinformation?* ed., Gabriele Siegert, M Bjørn Von Rimscha and Stephanie Grubenmann (Bangor: Bangor University, 2017), 143-159, https://research.bangor.ac.uk/portal/files/19775213/Micro_Moments_Liquidity_Intimacy_and_Automation_Developments_in_Programmatic_Ad_tech.pdf

The researchers have, however, alluded to the problem of the lack of transparency in the process of programmatic advertising in the cyber domain. Ad-tech firms mostly do not disclose the process involved in the placement of ads, which puts news websites at a disadvantage as they are placed alongside hoax news websites.[35] Unfortunately, at present, news websites and fake news are present in a shared online ecosystem. The research compiled by Joshua Braun and Jessica L Eklund characterised hoax news as falling within the purview of online advertisement fraud.[36] This process initially involves setting up a website, after which vendors are engaged to send visitors to a website. The vendors then divert traffic of online visitors, which is purchased at a cut-off rate by fake news publishers. Mostly, these visitors consist of click-workers and online bots (rather than legitimate visitors) that are employed for generating genuinely seeming impressions on a website. These visitors are, in fact, not genuine visitors which are solely employed for the purpose of generating traffic on a website. This incoming traffic of visitors and impressions is monetised after publishers sell these fake impressions using programmatic advertising tools. In truth, the actual ad-dollars of advertisers incentivise attention of "counterfeit users."

However, it is also noted that while generating online traffic, legitimate visitors also visit the website in sufficient numbers to provide a cover for the fake traffic created on the website by bots and click workers. This makes the job difficult for identifying fraudulent traffic by ad-tech firms and advertisers, which becomes akin to finding a needle in the haystack. One of the major problems with seeing ads lays in how certain cookies are designed to track and target you even over objectionable and unethical websites. To illustrate the point, a user visiting a website may see a cricket bat on an e-commerce website *(Daraz)* and they end up seeing its ads on a fake news website also. Similarly italicise, in comparison to premium websites, the ad-space is cheaper on less common and popular websites. At times, advertisers buy ad-space on premium websites to begin tracking their desired set of users, then place ads on much cheaper websites.[37] Such techniques to generate ad-money by ad-tech firms and advertisers create a

[35] Joshua A Bruan and Jessica L Eklund, "Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes and the Business of Journalism," *Digital Journalism* 7 (2019): 1-20.

[36] Ibid.

[37] Ibid, 6-8.

trade-off between the ethical question of placement of ads on hoax news websites with the relatively lucrative option of placing ads on cheaper websites.

The monetisation of fake news could not be possible without the reach offered by some social media platforms. Although, it is not appropriate to suggest that social media played a collisional role in expanding the reach of fake news, however, its use by hoax news publishers has been noticed in various social and political events across the world. Given the vast connectivity, reach and revenue generation model of social media platforms, their role also merits analysis.

a) Role of Internet Intermediaries in the Cyber Domain

As discussed earlier, the role of Internet intermediaries has come to light for their expansive network. These networks expanded the reach of fake news in the 2016 US elections and are capable of disseminating hoax and fake news content to a wider audience. The role of *Facebook* and *Google* in incentivising was unprecedented during the US elections. A widely shared fake story posted by a fictional Denver news outlet prior to the US elections "FBI Agent Suspected Hillary Email Leaks Found Dead in Apparent Murder-Suicide" was shared more than 500,000 times on *Facebook*.[38] The US elections also proved that even renowned members of the election campaigns were either gullible or discreet in sharing fake news with users, since doing so validates the credibility of the hoax news but it eventually creates more financial incentive for publishers of such fake news. After much criticism, *Facebook* and *Google* decided to remove fake news content from their platforms.

Due to the reach of platforms like *Google* and *Facebook*, the publishers can use it to post their fake news websites and stories to a large number of users in order to increase traffic on their websites. This increase in fake news sites' traffic enables social media websites to play an indirect role in monetising the content of fake news websites. Similarly, action against fake news publishers will also result in the decline of revenues for *Google* and *Facebook*.[39] Whether undertaking a crackdown has resulted in significant

[38] Ohlheiser, "This is How Facebook's Fake-News Writers Make Money."

[39] Cohan, "Does Facebook Generate Over Half of its Ad Revenue from Fake News?"

revenue losses for *Facebook* and *Google* is yet to be known, the reach of fake news and disinformation can be cataclysmic due to their presence on social media platforms.

A study by Reuters Institute observed that fake news websites, in comparison to news websites, received around 10 million minutes and 7.5 million minutes per month in comparison to 178 million minutes per month by *Le Monde* and 443 million minutes by *La Repubblica* in France and Italy respectively.[40] However, the reach and interaction with fake news content (in the form of comments, shares and likes) nearly matched or outdid the reach of most popular news brands. In France, it was observed that a false news page belonging to *Santé+* magazine received an average of over 11 million interactions per month, which was five times greater than established news sites combined.[41] In France, the three fake news outlets known for frequently posting fake news outdid the reach of five news sites combined on *Facebook*. In most of the cases, the false news websites' reach was limited in comparison to news websites, however, the ability of a handful of fake news sites over *Facebook* to outdo the reach of news websites remains a cause of concern.

However, in Italy, the reach of the false news sites and pages remained limited in comparison to news site pages.[42] Still, in comparison to the state-owned Italian news broadcaster *Rainews*, eight of the 20 false news pages from the Italian sample on *Facebook* attracted more interaction. One limitation of this research was that it could not account for the reach of the false news content and website links that were forwarded via private messaging apps or news shared in form of pictures without any news links. Similarly, the empirical data that was generated did not automatically suggest that all false news outlets automatically perform well on *Facebook* or any other social media outlet.[43] Moreover, one limitation of such study is the lack of significance attached to important social and political events that

[40] Richard Fletcher, Alessio Cornia, Lucas Graves and Rasmus Klies Nielsen, "Measuring the Reach of 'Fake News' and Online Disinformation in Europe," Factsheet, February, 2018, Reuters Institute and University of Oxford, (2018), 1-10, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-02/Measuring%20the%20reach%20of%20fake%20news%20and%20online%20distribution%20in%20Europe%20CORRECT%20FLAG.pdf

[41] Ibid.

[42] Ibid.

[43] Ibid.

can be driving factors or enabling elements to further fake news and it is at such times that publishers of fake news are likely to expand the reach of false stories and seek lucrative opportunities to monetise their content.

Google is one of the leading Internet tech corporations and the largest internet intermediary as well, however, most of its business is sustained through revenues from advertisement. Google Ad Works is one of the prime advertisement services that are operated by *Google*. The company allows its business clients to display ads across four types of services. These include ads shown against search results, secondly, on websites, pages and Gmail, the third category enables clients to display ads on its video hosting platform *YouTube* and the last category consists of advertising apps over *Google*'s network.[44] In 2018, *Google's* parent company Alphabet made 22 per cent higher revenues compared to 2017 and earned a total revenue of US$39 billion, with a surplus revenue of US$8.9 billion.[45]

Lately, *Google* has come under criticism for its flexible exercise of censuring websites hosting objectionable content such as fake news and extremist content.[46] It has resorted to only take off ads from pages of websites, containing objectionable content in violation of its policies.[47] A policy practice as this limits revenue flowing in from ad revenues, it does little to stifle publishers of fake news to sustain their work by monetisation of non-objectionable content on their website. As a consequence, ads continue to be displayed from *Google Ads* on other pages of the same website. A brand safety initiative called "Storyzy" found in its research in 2017 that 90 per cent of fake news sites that were monetising their audience through programmatic advertising were using *Google AdSense*. The

[44] "Google Ads Choose How You Want to Reach Your Customers," Google, last modified April 10, 2019, https://ads.google.com/home/how-it-works/

[45] Dominic Rushe, "Alphabet Shares Sink Despite Making US$8.9bn profit in Last Quarter," *Guardian,* Monday 4, 2019, https://www.theguardian.com/technology/2019/feb/04/alphabet-google-shares-profits-earnings-quarterly-report

[46] Storyzy, "Google Ad Sense Allows Ads on Extremist Sites," *Medium,* September 6, 2017, https://medium.com/@Storyzy/google-adsense-allows-ads-on-extremist-sites-33958eb86aa7

[47] "Google Content Policies," Google, last modified April 10, 2019, https://support.google.com/adsense/answer/1348688?hl=en

audience of these fake news publishers represents a staggering 120 million monthly visitors.[48]

The practice of de-monetising pages alone does little to remove a rewarding mechanism for fake news publishers from publishing disinformation over their websites or content. While in the case of *Breitbart News*, nearly 2600 brands blacklisted the entire website and decided against featuring its advertisements on it. The brand safety initiative Storyzy believes that in order to discourage fake news publishers, it is rather better to take down all advertisements from the website than to restrict ads from being placed on objectionable pages of the same website.[49]

b) Relationship of Privacy with Online Revenue Generation and Fake News

In the cyber domain, Internet intermediaries including firms like *Facebook* are reluctant to replace their existing model of business, which relies on monetising user data for attracting advertisements on its platform. This existing business model relies on the advertisers having to pay *Facebook* to compromise users' privacy for advertisements. Some have also called on *Facebook* to replace the current model with a subscription-based model. However, this is likely to shrink the burgeoned revenues and user base of *Facebook*, since users will be unlikely to pay the amount of money to the intermediary that advertisers can pay *Facebook* for access to their profiled market segment.[50] *Facebook*, through its existing model, has generated a US$50 billion annual revenue run rate, which is growing at 50 per cent each year, with a 50 per cent operating income margin, generating a market cap of almost US$500 billion.[51]

Despite *Facebook*'s efforts to clamp down on the spread of misinformation and fake news over its platform, as it had in the first quarter of 2018 by deleting nearly 583 million fake accounts the existing *Facebook* tools are designed in a manner to maximise the number of shares and likes,

[48] Ibid.

[49] Ibid.

[50] Len Sherman, "Why Facebook will Never Change its Business Model," *Forbes,* April 16, 2018, https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model/

[51] Ibid.

which tend to reinforce vulnerable tendencies of users to promote the viral spread of misinformation.[52] A major concern still remains the spread of stories by valid users over the platform.[53] Fact-checking or flagging of fake stories is often done after they have gone viral among users.[54] This factor was also acknowledged by a member of fact-checking initiative in Pakistan that it is difficult to ensure the reach of fact-checked counter-stories than the original fake news stories, which normally become viral over the Internet.[55]

The questions regarding the utilisation of users' offline and logged-in consumption data and how it's used by *Google* and *YouTube* in targeting users for advertisements and exposing them to a series of recommended videos remains shrouded in mystery. It's often noted even when users do not actively seek content from fake-news publishers in particular; their timeline on *YouTube* displays videos from fake news publishers. The lack of transparency regarding the workings of giant Internet platforms such as *Facebook* and *Google*'s algorithms raises questions regarding the utilisation of consumer's data for targeting them with advertisements over their platforms. As a result, this still continues to be one of the factors that sustain the spread of fake news to benign and active consumers of fake news. Being business leaders in the Internet domain, these companies are likely to be seen as trendsetters for other smaller companies applying programmatic advertisement tools to target consumers for exposure to online advertisements.

Increasing Trend of Fake News in South Asia

In Pakistan, fake news continues to circulate over different online mediums, including *Youtube*, *Facebook*, and *WhatsApp*. A variety of players disseminate fake news, there are some publishers that are able to produce and attract more viewership on their content than others. In some cases, dissemination of fake news is done for political purposes, while in others it is done for monetisation. One such popular fake news publisher in Pakistan

[52] Len Sherman, "Zuckerberg's Broken Promises Show Facebook is not your Friend," *Forbes,* May 23, 2018, https://www.forbes.com/sites/lensherman/2018/05/23/zuckerbergs-broken-promises-show-facebook-is-not-your-friend/#1c481bda7b0a

[53] Ibid.

[54] Ibid.

[55] In an Interview with Talal Raza, Programme Manager, Media Matters for Democracy, Islamabad.

with nearly 1.7 million subscribers is *Haqeeqat TV* on *YouTube*. The channel publishes multiple videos every day on different news events, with some of these videos generating more than 100,000 views. A recent fake news video published on April 2, 2019, on this channel regarding terror attacks in Christchurch titled "New Development is Taking Direction after Having Forensic Report."[56] The narrator in the video termed the terror attacks in Christchurch as being fake and staged. The video, as of the writing of this paper, generated 244,072 views.[57] Most of the views on this channel and other such fake news *YouTube* channels are generated through clickbait techniques in which publishers use sensational headlines and photo-shopped images over the video to tempt people to click them in order to increase the number of views on them. Some of the videos on this channel have generated more than a million views. These channels are likely to employ click-workers and bots to generate a higher number of views, impressions and comments on its videos. Also, this channel is observed to churn out videos by the day for monetisation purposes other than any political objectives.

In India, the daunting challenge of fake news is no different as access to smartphones becomes wide-spread among a growing number of people in India. In India, content promoting "Hindu Glory" and nationalistic messages are shared often by users without any need to verify it.[58] These messages are often shared as people feel duty-bound to share them forward.[59] There is a lack of discipline regarding consumption of news online in India, a range of fake news videos did the rounds on *YouTube,* one such video claimed that when Prime Minister of Narendra Modi met the French President, Emanuel Macron, the latter as a gesture of respect in the Indian culture touched the feet of the Indian Prime Minister (however, this display of respect by the French President never took place).[60]

[56] "New Development is Taking Direction After Having Forensic Report," Youtube, last modified April 2, 2019, https://www.youtube.com/watch?v=YtPVmvuxp4s

[57] Ibid.

[58] John McCarthy, "How the *BBC* is Tackling the 'Growing' Problem of Fake News in Asia and Africa," *Drum,* January 28, 2019, https://www.thedrum.com/news/2019/01/28/how-the-bbc-tackling-the-growing-problem-fake-news-asia-and-africa

[59] Ibid.

[60] Manish Singh, "In India, 'Fake News' and Hoaxes Catch Fire as Millions see YouTube for the First Time," *CNBC,* March 12, 2018,

One of the major factors that make people vulnerable to consume and indirectly incentivise fake news publishers is due to the dismal rate of digital literacy within Internet users.[61] Fake news publishers are also reported to deplete revenues of established content producers on *YouTube* with increased traffic.[62] Ahead of the 2019 general elections in India, *Facebook* disclosed that its measures for verifying buyers of political advertisements still remain imperfect and suggested the additional government of ad-spending disclosures to bring increased transparency.[63] After partnering with fact-checking companies *Facebook* was able to limit the circulation and reach of viral posts and content by 80 per cent, however, modified versions of the same content could be re-circulated and avoid detection.[64] *Facebook* has also begun to add disclaimers alongside political ads stating, "published-by" and "paid by."[65] In India, fake news has had as many consequences in the offline domain (physical world) for people as it has in the cyber domain. A score of people have been killed in India by violent mobs after being termed as child kidnappers. *WhatsApp* was often used as a means of spreading misinformation.[66] Although, spreading misinformation like this is not monetised, it entails serious consequences for the safety and security of other people. Understanding the disruptive implications of forwarded messaging, *Facebook* after much criticism decided to restrict forwarding messages on *WhatsApp* to a maximum of five users.[67]

In South Asia, Bangladesh witnessed a massive proliferation of fake news ahead of the 2018 general elections. Nine *Facebook* pages, associated with the government, were removed by *Facebook* ahead of the elections in

https://www.cnbc.com/2018/03/12/in-india-many-see-fake-news-on-youtube-thanks-to-cheap-data-plans.html

[61] Ibid.

[62] Ibid.

[63] Joseph Menn, "Facebook has made Headway against Abuses Ahead of India Election," *Reuters*, April 8, 2019, https://www.reuters.com/article/us-facebook-india-election/facebook-says-has-made-headway-against-abuses-ahead-of-india-election-idUSKCN1RK0T4.

[64] Ibid.

[65] Ibid.

[66] "How WhatsApp Helped Turn an Indian Village into a Lynch Mob," *BBC News,* July 19, 2018, https://www.bbc.com/news/world-asia-india-44856910

[67] Jacob Kastrenakes, "WhatsApp Limits Message Forwarding in Fight Against Misinformation," *Verge,* January 21, 2019, https://www.theverge.com/2019/1/21/18191455/whatsapp-forwarding-limit-five-messages-misinformation-battle

December 2018. Some six accounts were also removed on the charger of involvement in engaging in coordinated inauthentic behaviour.[68] Fake news also has the potential of being used as a tool for silencing criticism against the government and Bangladesh appears to have not remained immune to this practice. The government also cracked down against *Facebook* pages impersonating the pages of popular news websites.[69] These pages were blamed by government agencies for promoting propaganda against the government.[70]

In Sri Lanka, after the spate of eight terrorist attacks at multiple hotels and churches which killed 207 people and injured more than 450 during Easter, on April 21, 2019, the Government of Sri Lanka turned to block access to *Facebook* and *Instagram* as fake news began proliferating. The government feared that the fake news could incite communal violence and create law and order situation, which could jeopardise social harmony between the diverse communities of the island nation.[71]

In the midst of the fake news doing rounds over social media in the aftermath of the terrorist attacks, Sri Lank Red Cross Society rubbished the news claiming their building being attacked by the terrorists.[72] This also validates the finding that fake news mostly spreads around social and political events of significant importance. Although, blocking access to social media is perhaps not a worthy approach for countering fake news, as it can provide governments with a precedent to silence dissent in the face of severe criticism. However, the desperation on government's part goes on to tell the reach social media provides to fake news which is either being used

[68] Zeba Siddiqui and Ruma Paul, "Facebook, Twitter Remove Fake News Sites in Bangladesh Ahead of Election," *Reuters,* December 21, 2018, https://www.reuters.com/article/us-bangladesh-election-facebook/facebook-and-twitter-remove-pages-and-accounts-in-bangladesh-ahead-of-election-idUSKCN1OJ2N3

[69] Ibid.

[70] Ibid.

[71] "Sri Lanka Attacks: Several Arrested after 2017 Killed at Hotels and Churches on Easter Sunday," *Guardian,* April 21, 2019, https://www.theguardian.com/world/live/2019/apr/21/sri-lanka-explosions-dozens-killed-and-hundreds-injured-in-church-and-hotel-blasts

[72] "Sri Lanka Red Cross," *Twitter,* https://twitter.com/SLRedCross/status/1119852468559646725

for monetisation, political or other nefarious purposes by a range of malicious actors.

Cited from across the region, these examples are a testament to the reach of fake news in the cyber domain through social media and that it can be used for monetisation of fake news as well. Similarly, events of social and political importance can serve as critical catalysts in proliferating and reinforcing the reach of fake news. This may well be used for political purposes by malicious actors producing fake news but such events can be capitalised to monetise such content.

Measures for Building Cyber Resilience

In the cyber domain, complete removal of fake news is near impossible.[73] Its continued presence offers incentives for intellectual, legal, novel online and physical world measures to discourage its scope, presence and operability. The existing literature on the de-monetisation of fake news has suggested limited measures that offer a variety of means to discourage the flow of fake news. However, there is a need for a different approach for promotion of interaction across horizontal and vertical tiers of public, private sectors and multilateral forums. An array of all such approaches need to be reported in order to limit and create a demonetisation cycle for fake news publishers to limit the scope of incentives as a means of discouraging the scale and frequency of fake news in the online domain.

a) Automated Blacklisting

Fake news publication in the cyber domain can be tackled through blacklisting. This practice involves maintaining lists of banned websites, web-portals, social media accounts and pages that are declared as untrustworthy and found involved in fraudulent practices and particularly involved in fake news production and publication. *Google AdSense* maintains a list of millions of fake news publishers; it is also known to update its list annually, however, new websites keep coming up over the Internet in thousands by the hour.[74] Some experts are also of the view that

[73] Joseph S Nye, "Is Fake News Here to Stay," *Boston Globe,* December 7, 2018, https://www.bostonglobe.com/opinion/2018/12/07/fake-news-here-stay/Xm7ia1gfcATpVN34J6nUhL/story.html.

[74] Braun and Eklund, "Add Tech Platforms," 9-10.

through the employment of techniques such as spoofing, which includes impersonating a reputable publisher by offering up fake metadata and the other technique may include cloaking which consists of providing acceptable versions of a webpage to algorithmic and human moderators while versions containing fake news and objectionable content are shown to ordinary users. Fake news publishers also copy the same content from the blacklisted website to post it to a newly created website.

However, others have suggested that automated blacklists can be used to help overcome the issue of circumventing methods employed by fake news publishers. The dynamic, automated and updated lists would help address this problem by detecting the pages that are resurfacing in the cyber domain after being blacklisted or being taken down.[75] There is another supportive argument regarding the automated blacklists which is that they are politically neutral, therefore, the concerns about targeting a certain type of fake news content over the other can be overcome in the cyber realm. One such automated list maintained by Storyzy fake news sites categorises fake news under nine items which include, conspiracy, extreme left, extreme right, false information, hate, pseudoscience, satire, clickbait and propaganda.[76] Maintaining automated lists can also make adaptation by fake news publishers more difficult or costlier, similarly devising methods to detect spoofing or cloaking can also enable corporations and advertisers to demonetise or limit the flow of revenues to fake news publishers.

b) Inter-Ministerial Institution and Advisory Board

Reach and circulation of fake news can be detrimental for democratic institutions and the trust between the public and the state. To retain this trust, it requires regulation from private stakeholders but also from public institutions and civil society. Improving coordination between bodies such as Pakistan Electronic Media Regulatory Authority (PEMRA) which may include attaches from Pakistan Telecommunication Authority (PTA), Information Ministry, Federal Investigation Agency (FIA) and two active members of civil society groups in order to increase coordination between relevant stakeholders on initiating action against publishers of fake news. This cross-institutional representation in combination with a representation of civil society organisations will serve as a means of

[75] Storyzy, "Google Adsense Allows Ads on Extremist Sites."

[76] Ibid.

balancing against over-reach on content which may be misconstrued as disinformation. In tandem with these measures, news media groups need to maintain a segmented digital presence in order to make it difficult for fake news publishers to maintain their presence. Maintaining a separate or simultaneous journalistic presence in the online domain particularly at the social media will attract and enable retention of viewers that prefer staying connected online than prefer watching television.

c) Building Multilateral Foundation for Cyber Resilience

Stakeholders in the cyber domain — states, corporations, civil society organisations and tech companies — can be encouraged to become a part of multilateral arrangements led by the UN or international forums like Internet Governance Forum (IGF) which can help address the presence and spread of fake news by providing guidelines, assistance in technical and legal capacity building and also offer standardised practices to prevent growth of fake news in the online domain. Similarly, multilateral groups can devise a body of indicators against which the countries may be ranked against regarding their performance to curb fake news in the online domain. These lists may also issue specific policy guidelines, lay grounds for an international treaty for member countries to legislate domestic laws in conformity of international standards to protect free speech, while at the same time put up credible measures demonstrating zero-tolerance for fake news in the online domain. Similarly, multilateral bodies at the regional level such as South Asian Association for Regional Corporation (SAARC), Shanghai Cooperation Organisation (SCO) and Association of South East Asian Nations (ASEAN) may build and share standards on countering proliferation and publication of fake news in the online and offline domains. These bodies may also exchange their respective best experiences in countering fake news publication in the online domain.

d) Legislation on Fake News in Cyber Domain

The near absence of fake news related laws is putting media and news business in competition against a ghost competitor and also aggravating the problem for various institutions in the country to take appropriate legal action against fake news publishers in the country. For legislation of such laws, consensus-based domestic laws become extremely crucial for ensuring free-speech, citizen journalism or criticism of the government and include oversight mechanisms to create checks and balances for executive power. Therefore, seeking proactive counsel from media organisations, PEMRA, civil society organisations, local ad-tech firms and Internet intermediaries such as *Google, Facebook, Twitter* and cellular companies can be crucial in the development of balanced legislation to limit the reach of fake news in the cyber domain. These laws may also include penal fines for publishers of fake news publishers in order to discourage future engagement from their end. Similarly, government regulators may also stipulate fines on internet intermediaries that demonstrate an unwillingness to remove content, accounts and pages engaging in the publication of fake news.

e) Promoting Media Literacy

According to cyber experts, poor media literacy of Internet users is a huge challenge.[77] Media literacy is an approach and a framework also for the media users to analyse, evaluate, educate, interact and participate with the content of media in various means. This includes media in different varies from print, electronic to media content available over the internet.[78] Public awareness of citizens, Internet users can be done at a large scale in order to familiarise people with the ability to critically analyse the media they engage with over the internet. In order to increase media literacy, a cross-generational approach need to be made. School and college curricular can include content dedicated to media literacy. To this end, government, media channels, regulatory bodies and civil society organisations may design and disseminate public awareness messages over the radio, social media, television and cellular networks. The campaigns based in local vernacular, featuring renowned media personalities and celebrities can enable the effective promotion of awareness campaigns in order to educate and to a relative extent inoculate public against the effects of fake news in the cyber domain. Awareness of skills such as critical thinking and mere emphasis on prevention of mental laziness by internet users can be imperative in limiting the adverse effects of fake news and its reach in the cyber domain.

[77] "Media Literacy: A Definition and More," Centre for Media Literacy (CML), https://www.medialit.org/media-literacy-definition-and-more

[78] Ibid.

f) Employing Self-Regulation of Web Industries

Advertisement agencies, ad-tech firms need to agree to industry-based guidelines to ensure removal of fake news content and all such publishers' content in Pakistan. The contents of such a code may also require compliance from *Google, Facebook* and ad firms as a requirement to give advertisements. Similarly, these measures can also provide more leverage to industry-based actors to discourage displaying of advertisements alongside the content of fake news publishers. With respect to news publishers, advertising agencies and trading groups can maintain white lists for sanctioning displaying of their ads on news websites or publishers that are considered legitimate by members of the industry.

g) Utilising Artificial Intelligence (AI)

Internet intermediaries such as *Google* and *Facebook* along with start-up organisations establishing their ideas around fact-checking of disinformation can create AI-based systems which will be able to recognise "deepfakes"[79] and fake news content which can be flagged through automated programmes before posts begin to go viral, this will enable fact-checking and tech firms to build pre-emptive measures from having content and posts go viral by users which are known to be false. While deepfakes will require identification of fake and morphed video and audios of individuals, it can be done effectively through deep-learning.[80] On the other hand, text-based news can effectively be countered through the use of Machine Learning and Natural Language Processing to identify proliferation of fake news stories over the internet. Maintaining large amounts of data and training large data sample can help train software which will enable fact-checking organisations, intermediaries and regulators to flag and remove fake news over the stories. It will also be a cost-effective

[79] Deepfakes are videos in which a human subject is impersonated and their voice is also doctored by producers of the content. The video is manipulated in order to give a synchronised impression between the visual display and audio of the video.

[80] Deep-learning is an AI based approach falling under unsupervised learning. The technique involves training software to learn and solve a particular problem on its own. This particular approach can be effective as an alternative solution for identifying deep-fake content.

resource since reliance on human regulators can be reduced through effective employment of AI-based approaches.

h) Creating Online Public Portals

Reducing the costs of reporting and flagging fake news contents is one of the uphill tasks. One measure to overcome human-resource-related issues or flagging of content from diversified sources is to encourage reporting of fake news content for fact-checking. This process can be facilitated by maintaining a plain portal for publishing links to video, posts, pages and portals that are containing or hosting fake news or disinformation on its pages. This will also help raise the number of fake news content being flagged. In order to overcome the problem of false-positive, the Internet users must be solicited to provide additional information regarding the content being flagged in order to save time and effort while fact-checking and further reporting the content.

Conclusion

The monetisation of fake news is a prime motivator of proliferation and publication of fake news. The current literature on this issue has found that, so far, the cost of producing and publishing fake news online is relatively low. This allows some publishers of fake news to create additional revenues in order to sustain their business cycle. Fake news and its monetisation leave news websites and their social media presence at a disadvantage, its perpetuation leaves democratic institutions vulnerable and they can also serve to be a catalyst of chaos. In the online domain, fake news allows the publishers of such content to spread their message among people connected to the Internet that lack media literacy and remain susceptible to producers of disinformation in the cyber domain. The growing connectivity of the Internet and arise in the numbers of Internet users is likely to increase the vulnerability of users not well versed with media literacy and the inability to distinguish fake news from the news in the developing region as South Asia.

Similarly, despite the efforts undertaken by Internet intermediaries and Internet tech firms such as *Facebook*, *Google* and *Twitter* they have not been completely successful in limiting the reach of fake-news curtailing and rising the cost of fake news publishers today will leave certain groups to be producers of far more disruptive, resilient and adaptable measures to sustain their spree of disinformation in the realm of cyber. Left unchecked, few prominent individuals producing fake news can become leaders of creating a ‘new-normal’ in the media business which will entail detrimental consequences for legitimate players in the online news media. In order to counter and prevent monetisation of fake news in the cyber domain, diverse stakeholders and entities comprising intermediaries like *Google*, *Facebook* and *Twitter*, web-hosting companies, media regulatory bodies, government institutions and civil society organisations can collaborate together against monetisation and proliferation of fake news in the online domain.