

# The dark side of the Internet: Fueling misinformation in the COVID-19 pandemic and the 2020 US Presidential Election

Communication and the Public  
1–22

© The Author(s) 2025

Article reuse guidelines:

[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)

DOI: 10.1177/20570473251323752

[journals.sagepub.com/home/ctp](https://journals.sagepub.com/home/ctp)



**Zhicong Chen**   
Nanjing University, China

**Wenting Yu**  
The Hong Kong Polytechnic University, Hong Kong SAR, China

**Yixiao Sun**   
**Cheng-Jun Wang**  
Nanjing University, China

**Xiao Fan Liu**  
City University of Hong Kong, Hong Kong SAR, China

## Abstract

Characterized by robust technical anonymity and a conspicuous absence of stringent regulations, the dark side of the Internet represent the less illuminated aspects of the digital world. This study analyzed a national survey conducted in the United States in November 2020 ( $N=702$ ) to understand the relationship between using the dark side of the Internet and misinformation beliefs in both public health and political context. With the help of propensity score matching and instrumental variables, the results reveal that the users of the dark side of the Internet are more inclined to believe the misinformation about the COVID-19 pandemic and the 2020 US Presidential Election. Overall, the findings significantly contribute to the existing body of knowledge concerning the social impacts of technologies that grant a high level of user anonymity while operating with minimal regulatory oversight.

## Keywords

2020 US Presidential Election, COVID-19, misinformation belief, the dark side of the Internet, Tor

### Corresponding authors:

Cheng-Jun Wang, School of Journalism and Communication, Nanjing University, 163 Xianlin Street, Nanjing, Jiangsu 210023, China.  
Email: [wangchengjun@nju.edu.cn](mailto:wangchengjun@nju.edu.cn)

Xiao Fan Liu, Department of Media and Communication, City University of Hong Kong, Run Run Shaw Creative Media Centre, 18 Tat Hong Avenue, Kowloon Tong, 999077, Hong Kong SAR, China.  
Email: [xf.liu@cityu.edu.hk](mailto:xf.liu@cityu.edu.hk)



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (<https://creativecommons.org/licenses/by-nc/4.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

Malicious contents on the Internet always need to find pathways to percolate and reach its potential audience. Built on emerging technology for anonymous communication, the dark platform (e.g. 8kun imageboard websites) and the Dark Web (e.g. the Onion Router (Tor) network) represent the less regulated or unregulated aspects of the Internet. In this study, the dark side of the Internet refers to both the dark platform (the dark side of the surface Web) and the Dark Web (the dark side of the subsurface Web). Owing to the robust technical infrastructure ensuring a high level of anonymity, the dark side of the Internet has played a pivotal role in enabling the widespread propagation of extremist contents on a global scale, a substantial portion of which falls under the category of misinformation (Caiani & Parenti, 2009; French & Epiphaniou, 2015).

The rise of dark platforms (e.g. the 8kun imageboard website) has brought much attention to the proliferation of deceptive information (Zeng & Schäfer, 2021). The dark platforms operate as a parallel information system alongside social media platforms. While there are false claims about COVID-19 on many social media platforms (Enders et al., 2021), the dark platforms often manifest a notably elevated prevalence of misinformation, especially in the form of conspiracy theories. This phenomenon could be attributed to the inherent platform characteristics, specifically the heightened degree of user anonymity and the cultural norms cultivated within the predominantly anonymous environment. Therefore, greater emphasis should be placed on conducting a thorough investigation into the consequences of such marginalized groups.

Compared to the dark platform, the Dark Web (e.g. Tor network) represents an even more extreme case. The Dark Web has become an ideal place for sheltering unlawful and restricted contents, under the technical protection of the onion routing strategies provided by the Tor anonymity network (Alfosail & Norris, 2021). The anonymity of the Tor network ensures that user browsing histories are technically untraceable by third-party actors and offers a valuable opportunity to safeguard user identities during online activities (Nugent, 2019). As a result, the Tor network has been well-known for both legal and illegal online activities (Avarikioti et al.,

2018; Owen & Savage, 2016). Built on the Tor anonymity network, the Dark Web ecosystem provides a good opportunity to study the hidden world that operates in a fully anonymous setting and therefore should not be ignored.

While empirical research on the dark side of the Internet has gradually increased over the years (Chen et al., 2023; Davis & Arrigo, 2021; ElBahrawy et al., 2020), there are still research gaps in prior research. First, both the Dark Web and the Surface Web should be considered together when capturing the entire map of online information ecology (Beshiri & Susuri, 2019; Jin et al., 2023; Martin et al., 2018). A substantial number of restricted contents tend to escape into the Dark Web to circumvent censorship and regulations from the authorities. A good example of such content is the Daily Stormer (a far-right website), which was shut down on the Surface Web due to its extreme ideology but then restarted on the Tor network (Vandiver, 2020). Second, there is still scant information in the existing literature about the potential social and political implications of the dark side of the Internet. Third, advanced data analytical methodologies, such as propensity score matching (PSM) and instrument variables (IV), have not been adequately incorporated into investigations of the dark side of the Internet and potential social impacts.

To fill these research gaps, this study formulates the following key question: what is the relationship between using the dark side of the Internet and misinformation belief? We claim that more use of the dark side of the Internet may be positively correlated with higher levels of misinformation beliefs during political elections and public health crises. To explore the social impacts of the dark side of the Internet, this study concentrates on the US landscape, a country characterized by one of the most substantial concentrations of users on the dark side of the Internet around the world, that is, the highest penetration rate (The Tor Project, 2022). In the following sections, this study will explore how the use of the dark side of the Internet influences COVID-19 misinformation beliefs, as well as political misinformation beliefs during the presidential election. The research questions are empirically examined using a national cross-sectional survey conducted in November 2020, soon after the presidential election

in the United States, using hierarchical regressions, PSM, and instrumental variables.

## Literature review

### *The dark side of the Internet and misinformation beliefs*

In this article, the dark side of the Internet encompasses both the dark platforms (Zeng & Schäfer, 2021) and the Dark Web (Gehl, 2018). As a whole concept, the dark side of the Internet represents a shadowy underbelly of the digital world, characterized by illicit activities, anonymity, and the exploitation of vulnerabilities (Barton, 2016; Chen et al., 2024). There is a range of elements that collectively contribute to its ominous reputation. The Dark Web, with its encrypted communication channels and hidden forums, serves as a hub for cybercriminals to exchange knowledge, tools, and stolen data, thus further facilitating their nefarious activities. Criminals have exploited the Internet's interconnected nature to launch attacks, steal personal information, commit financial fraud, and perpetrate various forms of online criminal activities. Hacking, phishing, ransomware attacks, and identity theft are also prevalent in this realm (French & Epihanou, 2015).

Moreover, the dark side of the Internet serves as a breeding ground for extremist ideologies, hate speech, and the spread of conspiracy theories (Johnson et al., 2019). Online platforms within the dark web create echo chambers where like-minded individuals reinforce and amplify their beliefs, leading to radicalization and the potential for real-world harm. These platforms enable the dissemination of propaganda, recruitment of new members, and coordination of malicious activities, posing huge challenges to societal harmony and public safety (Chen & Liu, 2021; Chen et al., 2021). More extremely, with its anonymity, weak supervision, and potential for exploitation, the dark side of the Internet is a multifaceted entity that harbors a range of illicit activities (Ranaldi et al., 2022; Sirola et al., 2022). Therefore, although the dark side of the Internet represents only a fraction of the Internet's vast landscape, we cannot overshadow its potential for connectivity and knowledge sharing.

Several studies have established a strong interconnection between online media usage and the formation of misinformation beliefs (Enders et al., 2023; Stępińska et al., 2023). The online forums and online communities on the dark side of the Internet have provided platforms for like-minded individuals to validate and spread conspiracy theories, intensifying their impact on vulnerable individuals (Gaudette et al., 2020). These networks may further reinforce false narratives, contributing to the radicalization of individuals and the perpetuation of misinformation-driven worldviews (Soldatos, 2017). One way this occurs is through disinformation campaigns orchestrated on the Dark Web. Malicious actors can leverage the anonymity and global reach of the dark web to disseminate false information, manipulate narratives, and exploit people's biases and vulnerabilities (Chen, 2008). In addition, the Dark Web hosts websites that mimic legitimate news sources but peddle entirely fabricated stories or heavily biased contents. These fake news websites thrive on the dissemination of misinformation, deceiving readers and distorting public discourse. By exploiting the lack of regulation and oversight in the Dark Web, these sites can propagate falsehoods without facing the consequences typically associated with spreading misinformation (Kavallieros et al., 2018).

Numerous studies have sought to unravel the mechanisms behind individuals' misinformation belief. Some scholars view misinformation belief as an inherent tendency influenced by factors like demographic characteristics (Anspach & Carlson, 2022), personality (Lai et al., 2020; Taurino et al., 2023) and in-group identity (Robertson et al., 2022; Van Bavel et al., 2024). However, these studies often overlook the potential impact of the external information environment on individuals' misinformation belief. Other research pays attention to the role of the media information environment in shaping misinformation belief (Ahmed & Rasul, 2022; De Coninck et al., 2021; Enders et al., 2023), but these studies do not adequately address the issue of bidirectional causality—specifically, whether users actively choose media platforms consistent with their inherent misinformation belief, or if their level of misinformation belief are passively influenced by the media contents.

To summarize, there are two major reasons behind misinformation beliefs. First, information on social media often prioritizes novelty over authenticity (Vosoughi et al., 2018), and social media platforms typically experience less censorship than traditional media (Lemaire, 2023). Second, the complexity of information on social media can lead to user fatigue (Ravindran et al., 2014), making individuals too overwhelmed to verify the authenticity of the information and thus more susceptible to misinformation (Jiang, 2022).

As the Dark Web operates with minimal regulatory oversight, the two factors contributing to stronger misinformation belief tend to be more pronounced in this environment. The lack of regulation provides fertile ground for malicious communicators to manipulate information more effectively, particularly during the COVID-19 pandemic (Sirola et al., 2022). The proliferation of untraceable content on the Dark Web not only hampers efforts to identify the sources of information and verify its authenticity, but also reinforces users' beliefs in misinformation.

However, the observed correlation between Dark Web use and stronger misinformation beliefs may be spurious. Individuals who are already inclined to believe misinformation may be more likely to use the Dark Web. This endogeneity issue complicates the causal interpretation of the relationship between Dark Web exposure and misinformation. Prior study has indicated that individuals with stronger perceptions of misinformation are more likely to consume news on social media and other alternative media outlets (Hameleers et al., 2022). The theoretical basis of this perspective is rooted in social identity theory, which posits that individuals believe in misinformation because they align with the beliefs of their in-groups (Cookson et al., 2021). As a digital space characterized by various subcultures where users gather due to shared beliefs, many users actively engage on the Dark Web and share information on these platforms because they feel a sense of belonging within these communities (Sirola et al., 2024). Consequently, an echo chamber effect may reinforce individuals' beliefs in misinformation (Wolfowicz et al., 2023). Furthermore, the Dark Web's propensity to challenge dominant narratives also allows it to shape internal discourse and establish itself as a safe

haven for niche groups to exchange information (Gehl, 2016), thereby strengthening the cohesion of these in-groups and further amplifying the volume of voices within the echo chamber.

Overall, the role of new media technology in social and political contexts has always been a significant and debatable topic in information and communication studies, particularly how people use and interact with media platforms and how media influences people's behavior in information-seeking and sharing (Beshiri & Susuri, 2019; Devine et al., 2015). In this study, we do not aim to compare the two aforementioned perspectives separately. While we acknowledge the role of user selection mechanisms, our primary focus is to explore whether using the Dark Web can increase individuals' belief in misinformation, which requires minimizing the problem of endogeneity and mitigating reversed relationship. To this end, we employed rigorous data analysis methods to investigate the relationship between users' exposure to the Dark Web and their levels of misinformation belief.

### *Misinformation during the COVID-19 pandemic*

The COVID-19 pandemic has evolved into a significant socio-political concern within US society, marked by a proliferation of misinformation and conspiracy theories (Stepińska et al., 2023). Despite calls for political consensus, there is growing evidence that the public response to the COVID-19 pandemic was widely politicized in the United States (Druckman et al., 2021). For example, according to a representative national sample, liberals exhibited a higher perceived risk compared to conservatives (Kerr et al., 2021). Meanwhile, liberals were more critical of government and placed less trust in the political actors who handled the pandemic, while simultaneously placing more trust in medical experts, such as the World Health Organization. Furthermore, coherent empirical evidence has revealed significant political polarization between different partisanshipes beyond attitudes. Moreover, liberals consistently exhibited significantly higher levels of probability of COVID-19 prevention behaviors (such as wearing face masks and washing

hands more often). Therefore, COVID-19 was perceived as both a public health crisis and a political communication crisis (Gollust et al., 2020).

As one of the most widely used services on the Tor network, cryptomarkets have been deeply influenced by the COVID-19 pandemic (Barratt & Aldridge, 2020). Although the Tor network ensures high levels of anonymity and network safety, online transactions still must be completed by offline deliveries, which are inevitably obstructed by multiple pandemic prevention measures. At the peak of market disruption, the rate of successful deliveries decreased to only 21% of all transactions due to failed issues on shipments (Bergeron et al., 2020). Simultaneously, cryptomarket users demonstrated significant reactions to the COVID-19 pandemic (Bracci et al., 2021). For example, cryptomarkets started offering products related to COVID-19 (such as masks and test kits) as soon as the pandemic started. At that time, there was a significant shortage of prevention products (e.g. masks) in the regular economy. Subsequently, when the approved vaccines were released, vendors on the Dark Web started to offer fabricated proofs of vaccination and COVID-19 passports. When the regular economy was able to satisfy the demand for public goods, the Dark Web started to decrease its offerings (Bracci et al., 2021). All the evidence has demonstrated that the Dark Web operates as an “underground world” that is complementary to the real world (Razaque et al., 2021).

Moreover, in response to COVID-19, contents that were not available on other platforms emerged. A study examined the sales of some COVID-19 related goods (such as masks and vaccines) on Dark Web marketplaces and found that activities in Dark Web marketplaces were highly responsive to the emerging crisis under COVID-19 (Bracci et al., 2021). This example demonstrates that the Dark Web is deeply influenced by real-world events outside the ecosystem. Another study demonstrated that more than 20% of commonly visited Tor network domains usually import resources from (or directly link to) the Surface Web. Specifically, those comprising 20% with imported contents from external sources on the Surface Web are

among the most prevalent websites on the Tor network (Sanchez-Rola et al., 2017).

Over the period of COVID-19 pandemic, imageboard websites have also become a hotbed for the dissemination of various pieces of misinformation (some are even political) related to the pandemic. For example, there was a shift in the types of meme templates and images posted in threads about the COVID-19 pandemic by users on the well-known 4chan platform (a sister website to 8kun). Initially, in January 2020, users from the /pol/ channel on 4chan often discussed COVID-19 with humorous hazmat suit memes. Subsequently, there were increasing references to charts and graphs related to scientific information about COVID-19 as the pandemic progressed (Jin et al., 2020). These findings suggest that there were more discussions around the COVID-19 case counts and projections emerging on the imageboard platforms. In addition, politically charged memes and image contents became more popular on the platform.

Overall, people generally have much more time to stay at home and use the Internet to access the outside world nowadays. When users access either cryptomarkets or imageboard websites, they are more prone to encountering content that remains exclusive to the dark side of the Internet and is not accessible elsewhere. Furthermore, due to its special technical features, the culture and ecosystem of websites hosted on the dark side of the Internet tend to be quite special, and users tend to adhere to certain political attitudes. For example, the users of cryptomarkets are typically in favor of libertarianism, while imageboard website users tend to support far-right populism (McSwiney et al., 2021). It is probable that a socialization effect occurs between these users during the information exchanges on the websites. Therefore, users of cryptomarkets are likely to show differences in their beliefs and behaviors related to the COVID-19 pandemic. Accordingly, we ask the following research questions:

*Hypothesis 1 (H1).* The use of the dark side of the Internet is positively associated with misinformation beliefs related to the COVID-19 pandemic.

## *Misinformation during the 2020 US Presidential Election*

The increasing trend of hate speech and misinformation on the Internet presents a myriad of challenges to the quality of society's information environment, particularly in the elections (Carlson, 2020). In particular, many recent studies have discussed the potential impacts of misinformation and fake news on electoral processes (Green et al., 2022; Gunther et al., 2019; Leyva & Beckett, 2020). People with more beliefs in misinformation about certain candidates may be less likely to vote for them, and such beliefs may further reinforce a vote for their preferred candidates (Cantarella et al., 2023). Therefore, distorted beliefs about political issues have the potential to influence people's vote on a ballot, controlling for political orientations and audience sophistication (Reedy et al., 2014; Wells et al., 2009). For example, exposure to misleading information regarding the European refugee situation significantly increased voting intentions for far-right candidates (Barrera et al., 2020). Taken together, voter partisanship and perceived news credibility tend to have strong associations with the belief in misinformation, which could further influence voting choices in elections.

As users from the dark side of the Internet tend to be more sensitive to personal privacy about their online behaviors, they are also likely to be less trusting in authorities. Cryptomarket users tend to hold strong political attitudes. Much of the commentary in social media (sometimes by the market users themselves) demonstrated that cryptomarkets represented an unfettered, perfect, and anarcho-capitalist (or libertarian) space for a competitive market (Obreja, 2024). Trust in mainstream media could serve to guide and navigate the public in complex political situations within society, and thus closely related to beliefs in political misinformation (Mansoor, 2021). Individuals who exhibit skepticism or a lack of trust in mainstream media are inclined to resort to social media or non-mainstream media platforms for their information consumption (Hameleers et al., 2022). Online media has become a perfect venue for mistrustful

members of the public in search of alternative facts, which can be highly persuasive. The less one trusts news media and politics, the more one believes in online disinformation (Zimmermann & Kohring, 2020).

Public authorities, commentators, and civil society groups have reported that the rise of far-right ideologies has been cultivated in anonymous online spaces in recent years (Baele et al., 2023; Europol, 2019; Törnberg & Törnberg, 2023). Imageboard websites are particularly known as a gathering place for far-right groups and their far-right centered and populist antagonistic speech (Hagen, 2022; Nagle, 2017; Tutters & Hagen, 2019). For example, 8kun (previously called 8chan) has become another home of the discredited far-right QAnon conspiracy theory (Weill, 2020). The Internet has rendered it easier for these people to promote extremist messages and hate speech without being investigated by the police. A well-known example is the QAnon conspiracy theory, which originated on 4chan.

Online platforms such as anonymous forums and imageboards have created opportunities for far-right actors to bypass the gatekeepers of institutional political discourse (such as parties and mainstream media) (Atton, 2006; Schroeder, 2019). Users on the dark side of the Internet are more likely to be exposed to special contents that are not shown elsewhere. Notably, as there are well-known far-right websites (such as the Daily Stormer and 8kun) hosted on the dark side of the Internet, users are much more likely to be exposed to a large amount of far-right information during the 2020 US Presidential Election. Furthermore, the dark side of the Internet has provided shelter for alternative media, allowing them to circumvent any state censorship and regulations from authorities. Therefore, it is highly likely that users initially hold relatively radical political attitudes when they intend to use the dark side of the Internet. Building upon the prior discussions, it is anticipated that distinctions in attitudes and behaviors, particularly in misinformation beliefs, may emerge between users and non-users of the dark side of the Internet during the 2020 US Presidential Election. This leads to the formulation of the following research question:

*Hypothesis 2 (H2).* The use of the dark side of the Internet is positively associated with misinformation beliefs related to presidential candidates?

## Data and methods

### Data

A national survey was conducted online from 13 to 15 November 2020, which was within 2 weeks after the 2020 US Presidential Election, and was aimed at people aged 18–65 years who were currently living in the United States.<sup>1</sup> The survey was delivered by a company called “LUCID,” based in New Orleans, Louisiana, following Yu et al. (2024).<sup>2</sup> A quota sample, based on gender and age using census data as a reference (US Census Bureau, 2019), was drawn from the online access panel maintained by the company. Furthermore, we employed post-stratification to adjust the weights of subpopulations, enhancing the representativeness of the sample. The post-stratification weight was constructed for age, gender, and income using the 2020 Current Population Survey (CPS) as a benchmark.

At the beginning of the survey, the age and residence of respondents were asked to ensure that any who were aged below 18 or above 65, and those not currently living in the United States were filtered out. There were also two attention-checking questions embedded in the survey, and any respondents who failed to pass this check were excluded from the data. Furthermore, anyone who finished the survey within an extremely short time (<5 min) was also excluded. The final sample size is 702. Table 1 presents an exposition of the demographic variables.

### Measurement

*Dark platform use* ( $Mean = 2.031$ ,  $SD = 1.764$ ,  $alpha = 0.966$ ). To gauge the extent of dark platform usage, participants were asked to indicate their frequency of engagement with two widely recognized imageboard websites: 4chan and 8kun (formerly known as 8chan). Featured with full anonymity and image-based communication, 4chan and 8kun have created a special online public space that is widely known for cultural and

political memes (Nissenbaum & Shifman, 2017). The measurement was based on a 7-point Likert-type scale, ranging from 1 (“Never”) to 7 (“All the time”). Participants were instructed to provide ratings reflecting their typical level of activity on these platforms. The measure was then averaged for the two questions.

*Dark web use* ( $Mean = 2.077$ ,  $SD = 1.808$ ,  $alpha = 0.945$ ). To assess participants’ involvement with the Dark Web, we examined their reported frequency of engagement with specific platforms. Following previous studies which provided a systematic overview of the Dark Web marketplaces (Zaunseeder & Bancroft, 2019), we selected Dread, a prominent discussion forum, and White House Market, a notorious online marketplace associated with illicit goods and services, as representative of this environment. Participants were asked to indicate how frequently they visited these Dark Web platforms, using a scale ranging from 1 (“Never”) to 7 (“All the time”). The measure was then averaged for two questions.

*Tor browser use* ( $Mean = 2.795$ ,  $SD = 2.283$ ). The frequency of Tor browser use was assessed through a single question asking respondents about their general web browsing habits using the Tor browser. Participants provided their responses on a 7-point Likert-type scale, ranging from 1 (“Never”) to 7 (“All the time”). The survey indicated a relatively high proportion of Tor users, which aligns with previous research suggesting the United States has a significant number of Tor network users, especially following the 2013 revelations by Snowden (Rosso et al., 2020). To further validate the prevalence of Tor network usage, the survey included additional questions about specific websites commonly accessed through Tor. Bivariate Pearson correlation analyses were conducted to explore the relationships between general Tor network usage and the utilization of these specific websites (see Table 2).

*COVID-19 misinformation belief* ( $M = 3.123$ ,  $SD = 1.642$ ,  $alpha = 0.851$ ). This item was measured by asking respondents about their level of belief in six items. The wording was as follows: what is the likelihood that it is true? The six items contained six messages

**Table 1.** Characteristics of demographic variables.

Demographic variable	Level	Number	Percentage
Age group	18–29	162	23.1%
	30–49	299	42.6%
	50–65	241	34.3%
Gender	Male	344	49.0%
	Female	358	51.0%
Education level	12th grade or below, no high school diploma	21	3.0%
	High school graduate/diploma or equivalent	143	20.4%
	Some college education but no degree	163	23.2%
	Bachelor's degree	214	30.5%
	Postgraduate degree	161	22.9%
Personal yearly income	Under US\$5000	53	7.5%
	US\$5000–US\$9999	27	3.8%
	US\$10,000–US\$14,999	37	5.3%
	US\$15,000–US\$19,999	31	4.4%
	US\$20,000–US\$24,999	38	5.4%
	US\$25,000–US\$29,999	42	6.0%
	US\$30,000–US\$34,999	34	4.8%
	US\$35,000–US\$39,999	21	3.0%
	US\$40,000–US\$44,999	26	3.7%
	US\$45,000–US\$49,999	18	2.6%
	US\$50,000–US\$54,999	29	4.1%
	US\$55,000–US\$59,999	24	3.4%
	US\$60,000–US\$64,999	18	2.6%
	US\$65,000–US\$69,999	15	2.1%
	US\$70,000–US\$74,999	19	2.7%
	US\$75,000–US\$79,999	20	2.8%
	US\$80,000–US\$84,999	16	2.3%
	US\$85,000–US\$89,999	9	1.3%
	US\$90,000–US\$94,999	5	0.7%
	US\$95,000–US\$99,999	16	2.3%
	US\$100,000–US\$124,999	59	8.4%
	US\$125,000–US\$149,999	43	6.1%
	US\$150,000–US\$174,999	35	5.0%
US\$175,000–US\$199,999	23	3.3%	
US\$200,000–US\$249,999	18	2.6%	
US\$250,000 or more	26	3.7%	
Marital status	Married	365	52.0%
	Not married but in a relationship	100	14.2%
	Single	237	33.8%
Living area	Urban	507	72.2%
	Rural	195	27.8%

related to COVID-19, which were manually validated as misinformation. The measure was then averaged for the six items.

*Political misinformation belief* ( $M = 3.659$ ,  $SD = 1.420$ ,  $\alpha = 0.788$ ). This item was measured by asking the respondents about their level of beliefs in eight

**Table 2.** Zero-order correlations with Tor browser use.

Websites on the Tor network	Pearson correlations
DuckDuckGo <sup>a</sup>	$r = 0.59, p < 0.001$
8kun <sup>b</sup>	$r = 0.64, p < 0.001$
Dread <sup>c</sup>	$r = 0.65, p < 0.001$
White House Market <sup>d</sup>	$r = 0.65, p < 0.001$

<sup>a</sup><https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>

<sup>b</sup><http://8kun.top.qulatl2tl34vwefcc2pbsxi7vennhbew57jbl2d3pbhvjhozkoizdoqd.onion/>

<sup>c</sup><http://dreadytofatroptsdj6io713xptbet6onoyno2yv7jicoxknyazubrad.onion>

<sup>d</sup>The White House Market has been shut down in 2021 (see the news: <https://www.wired.com/story/white-house-market-dark-web-drugs-goes-down/>). Despite never reaching the peak trading volumes of its antecedent cousins, the more well-known cryptomarkets Silk Road and AlphaBay, White House Market has already established itself as one of the most popular cryptomarket on the Dark Web. Established since August 2019, there have been 467, 371 users, including 2877 vendors, and 36,357 products listed on the White House Market.

items. The question wording was as follows: what is the likelihood that it is true? The eight items contained eight messages related to the presidential candidates in the 2020 US Presidential Election (two messages for every candidate: Donald Trump, Joe Biden, Amy Barrett, and Kamala Harris) that were manually validated as misinformation. The measure was then averaged on all eight items.

*Exposure to dark web scandals* ( $M = 1.912, SD = 1.153, \alpha = 0.903$ ). Exposure to Dark Web scandals was assessed using two questions. The first question asked participants to recall the amount of information they had encountered in the media (including television, radio, newspapers, magazines, and the Internet) over the past 12 months regarding Dark Web vendor arrests around the world. The second question focused on the participants' exposure to media coverage of Dark Web market crackdowns and "exit scams" during the same period. Exposure to Dark Web scandals was included as a control variable in the regression analyses to account for potential confounding factors and the influence of counter

information related to the Dark Web and the darker aspects of the Internet. This was done to address the possibility that exposure to such scandals might influence individuals' beliefs in the misinformation obtained from dark platforms and the Dark Web.

*Control variables.* To ensure a comprehensive analysis, the regression models included several control variables. First, traditional media use was incorporated as a control, measured by three questions that assessed the frequency of news consumption from different media platforms in the previous month, such as printed media (newspapers and magazines), radio, and television. Second, Internet use was considered as a control variable in the regression models. Given the proliferation of false or misleading information available online, the frequency of Internet use could be associated with both Tor usage and belief in misinformation. Furthermore, exposure to scandals related to Dark Web markets, as reported in the news, was integrated as a control variable. This control variable accounts for the potential impact of negative information dissemination about Tor and dark platforms in general through news coverage. Finally, individual demographic variables, including political identity, education, income, marital status, geographic area, age, and gender, were also included as control variables in the regressions.

### Analytical approach

This study aims to explore the relationship between the utilization of dark platforms and the Dark Web, and individuals' beliefs in health and political misinformation. In addition to conventional multivariate regression analysis, the research employs instrumental variable (IV) and propensity score matching (PSM) techniques to enhance the robustness of the findings. Instrumental variable analysis is a powerful statistical method used to address endogeneity and establish causal relationships between variables. It involves identifying an instrumental variable that is correlated with the variable of interest but only affects the outcome indirectly through its impact on the variable being studied. This instrumental variable acts as a "proxy" or source of exogenous variation, enabling researchers to isolate and estimate the

causal impact of the variable of interest. The instrumental variable approach relies on two critical conditions: relevance and exogeneity. Relevance ensures that the instrumental variable is correlated with the endogenous variable it is meant to instrument for, while exogeneity ensures that the instrumental variable is not directly associated with the outcome variable, except through its effect on the endogenous variable. By meeting these conditions, instrumental variables help address challenges related to endogeneity and produce more reliable estimates of causal effects.

Furthermore, the study employs PSM to estimate the effects of Tor network usage. The underlying principle of PSM is to pair respondents who have similar propensity scores, with one being exposed to the treatment (Tor network usage) and the other serving as a control. The goal is to identify matched pairs of individuals who have the same likelihood of receiving the treatment, akin to a between-subject experimental design. To calculate propensity scores, a logistic regression model is employed, where the treatment variable serves as the dependent variable ( $Y$ ). The independent variables in this regression model are the covariates that are expected to influence both the treatment and the outcome variable. These covariates should be potentially correlated with both the treatment variable and the outcome variable (Imbens & Rubin, 2015). Through this step, the probability  $P$  (i.e. the propensity score) of the individual unit receiving the treatment (in this case, the probability of using the dark side of the Internet) was calculated based on the following equation with a logit function

$$\text{logit}(Y = 1|X_{\text{covariates}}) = \log\left(\frac{P}{1-P}\right)$$

## Results

### *Hierarchical regression analysis*

To address the research questions, hierarchical regression analyses were conducted using conventional regression models for two outcome variables: COVID-19 misinformation belief (see Table 3) and

political misinformation belief (see Table 4). To ensure the robustness of our regression models, we conducted a Variance Inflation Factor (VIF) analysis to assess multicollinearity among the predictors. The VIF values for the variables are as follows: Political identity (1.03–1.07), Education (1.58–1.67), Income (1.80–1.87), Marriage (1.36–1.43), Area (1.17–1.22), Age (1.05–1.24), Gender (1.13–1.17), Traditional Media Use (1.71–1.76), Internet Use (1.06–1.09), Tor Browser Use (1.62–1.96), Exposure to Dark Web Scandals (1.75–1.91), Dark Platform Use (2.48), and Dark Web Use (2.73). Most of the VIF values are well below the threshold of 5.0, indicating that multicollinearity is not a significant issue in the hierarchical regression models.

After accounting for all covariates, the study found a statistically significant positive association between the use of dark platforms and beliefs in COVID-19 misinformation ( $\beta = 0.355$ ,  $SE = 0.043$ ,  $p < 0.001$ ), as well as political misinformation ( $\beta = 0.255$ ,  $SE = 0.041$ ,  $p < 0.001$ ). Similarly, the use of the Dark Web emerged as a significant predictor of both COVID-19 misinformation ( $\beta = 0.420$ ,  $SE = 0.043$ ,  $p < 0.001$ ) and political misinformation ( $\beta = 0.315$ ,  $SE = 0.041$ ,  $p < 0.001$ ). Taken together, the hierarchical regression analyses have demonstrated the significant relationships between both dark platform usage and Dark Web engagement and beliefs in health and political misinformation. Specifically, the use of the Dark Web appears to have a stronger association with misinformation beliefs (with larger regression coefficients) when compared to the use of dark platforms alone.

### *Propensity Score Matching*

To further validate the findings, the PSM method was employed. The use of the dark platforms and the Dark Web was dummy coded into 1 for the treatment group and 0 for the control group. Following the work of Kobayashi (2018), the level of media consumption and the individuals' demographic data (i.e. education, income, marriage, area, age, and gender) were selected to calculate the propensity scores. The covariate balancing propensity scores (CBPS) method was used to ensure covariate balance during the matching procedure (Imai & Ratkovic, 2014). We further employ

**Table 3.** Hierarchical regression analysis on COVID-19 misbelief.

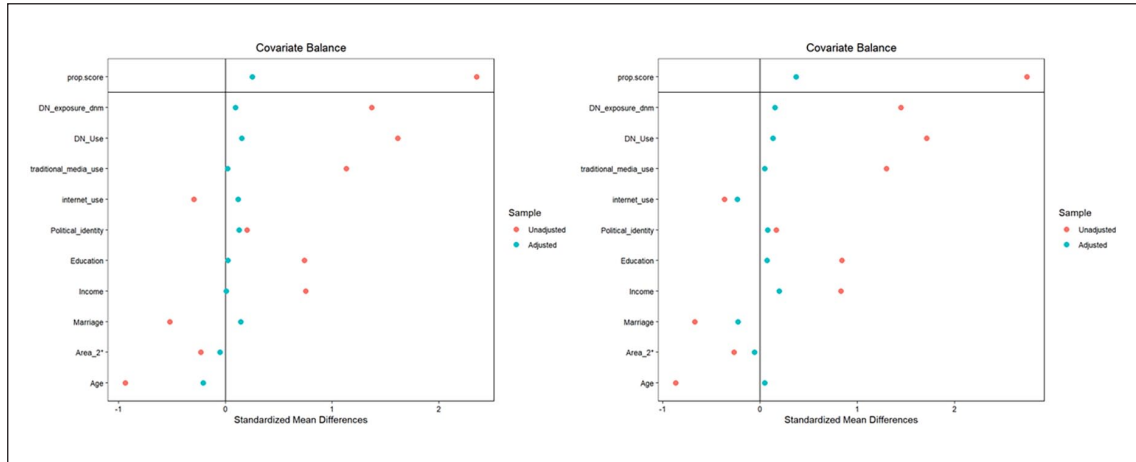
	COVID-19 misbelief		
Political Identity	0.146*** (0.019)	0.129*** (0.017)	0.111*** (0.016)
Education	0.001 (0.044)	-0.037 (0.040)	-0.081* (0.039)
Income	0.019* (0.009)	0.002 (0.008)	-0.003 (0.008)
Marriage	-0.220** (0.071)	-0.060 (0.066)	-0.033 (0.063)
Area	-0.205 (0.134)	0.020 (0.123)	0.074 (0.118)
Age	-0.034*** (0.004)	-0.018*** (0.004)	-0.013*** (0.004)
Gender	0.204 (0.118)	0.035 (0.108)	-0.002 (0.103)
Traditional Media Use		0.120** (0.044)	0.072 (0.042)
Internet Use		-0.092 (0.049)	-0.033 (0.047)
Tor Browser Use		0.195*** (0.028)	0.098*** (0.029)
Exposure to DNM Scandals		0.238*** (0.057)	0.098 (0.057)
Dark Platform Use			0.355*** (0.043)
Dark Web Use			0.420*** (0.043)
Constant	4.116*** (0.377)	2.484*** (0.494)	2.159*** (0.473)
Observations	702	702	702
R <sup>2</sup>	0.207	0.356	0.415
Adjusted R <sup>2</sup>	0.199	0.346	0.404
Residual Std. Error	1.470 (df=694)	1.328 (df=690)	1.267 (df=689)
F Statistic	25.863*** (df= 7; 694)	34.680*** (df= 11; 690)	40.657*** (df= 12; 689)

\*p &lt; 0.05; \*\*p &lt; 0.01; \*\*\*p &lt; 0.001.

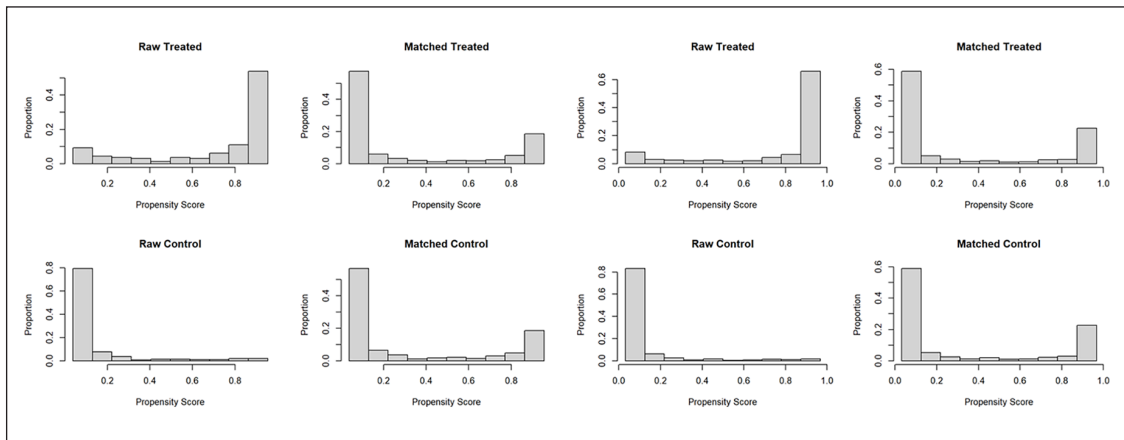
**Table 4.** Hierarchical regression analysis on political misbelief.

Political misbelief	
Political Identity	0.052*** (0.015)
Education	-0.071 (0.036)
Income	0.002 (0.008)
Marriage	0.025 (0.059)
Area	0.100 (0.111)
Age	-0.010** (0.004)
Gender	-0.055 (0.097)
Traditional Media Use	0.019 (0.040)
Internet Use	0.090* (0.044)
Tor Browser Use	0.084** (0.027)
Exposure to DNM Scandals	0.040 (0.053)
Dark Platform Use	0.255*** (0.041)
Dark Web Use	0.315*** (0.041)
Constant	2.273*** (0.443)
Observations	702
R <sup>2</sup>	0.313
Adjusted R <sup>2</sup>	0.301
Residual Std. Error	1.187 (df= 689)
F Statistic	26.199*** (df= 12; 689)
	0.071** (0.016)
	-0.025 (0.037)
	0.007 (0.008)
	-0.012 (0.061)
	0.022 (0.115)
	-0.015*** (0.004)
	-0.014 (0.101)
	0.071 (0.041)
	0.041 (0.045)
	0.172*** (0.026)
	0.155** (0.054)
	2.575*** (0.460)
	702
	0.254
	0.242
	1.236 (df= 690)
	21.398*** (df= 11; 690)
	4.492*** (0.340)
	702
	0.137
	0.128
	1.326 (df= 694)
	15.699*** (df= 7; 694)
	2.342*** (0.449)
	702
	0.295
	0.282
	1.203 (df= 689)
	23.984*** (df= 12; 689)

\*p &lt; .05; \*\*p &lt; .01; \*\*\*p &lt; .001.



**Figure 1.** Mean differences of propensity scores and covariates between matched pairs.



**Figure 2.** The histograms of propensity scores before and after matching.

optimal full matching method to group every pair of individuals into subclasses, and the effect size was then estimated using the multilevel modeling method (Hansen, 2004). This matching approach was optimal because the sum of the absolute distances between the treated and control units in each subclass was optimized to be as small as possible.

Figure 1 illustrates how much covariate imbalance was reduced using the CBPS method. The empirical analysis of covariate balances and propensity scores indicated that the matching was successful. The absolute standardized mean difference for

all the covariates substantially decreased ( $<0.5$ ) after the adjustment of the CBPS method, which is approximately the same level as the experimental data with random assignment. As a result, this subset of the sample forms a quasi-experimental dataset where respondents were assigned to the treatment or control condition in an “as-if random” manner. This approach mitigates concerns related to endogeneity and omitted variable bias, which are common issues in observational studies.

Figure 2 presents detailed histograms of the propensity scores for both the treatment and control

**Table 5.** The estimated Averaged Treatment Effects (ATE) on the matched sample.

	COVID-19 misbelief		Political misbelief	
(Intercept)	2.859*** (0.172)	2.690*** (0.070)	3.462*** (0.139)	3.357*** (0.087)
Dark Platform Use	0.741*** (0.186)		0.559* (0.232)	
Dark Web Use		1.391*** (0.291)		0.972*** (0.249)
Observations	702	702	702	702
R <sup>2</sup> /R <sup>2</sup> adjusted	0.054/0.053	0.182/0.181	0.040/0.038	0.114/0.113

\* $p < 0.05$ ; \*\*\* $p < 0.001$ .

groups, shown before and after the matching process. Initially, there was a noticeable difference in the distribution of propensity scores between the untreated and treated groups. However, following the application of the optimal full matching procedure, which involves assigning weights within each subclassification, the distribution of propensity scores became more balanced between the treated and control groups.

Once the matched subsample is generated, this study adopted the average treatment effect (ATE) as the major estimand, meaning the difference in the expected means between the actual outcome of those who were treated and the counterfactual outcome that would be observed if they were not treated. Regression analyses without covariates were estimated on the matched data with robust standard errors (see Table 5). The ATE of dark platform use on COVID-19 misinformation belief was 0.741 ( $SE=0.186$ ,  $p < 0.001$ ), and the ATE on political misinformation belief was 0.559 ( $SE=0.232$ ,  $p < 0.05$ ). The ATE of Dark Web use on COVID-19 misinformation belief was 1.391 ( $SE=0.291$ ,  $p < 0.001$ ), and the ATE on political misinformation belief was 0.972 ( $SE=0.249$ ,  $p < 0.05$ ).

### Instrumental variable

By utilizing instrumental variable analysis and PSM, this study aims to overcome common methodological challenges and provide more robust insights into the relationships between dark platform usage, Dark Web engagement, and beliefs in health and political misinformation. We utilize media exposure to Tor-related information as an instrumental variable to examine its impact on the use of Tor and the dark

websites hosted on it. While exposure to Tor-related information is highly likely to drive the use of Tor and access to dark platforms, it is unlikely that exposure to Tor will lead to belief in misinformation. Therefore, exposure to Tor can serve as a useful instrumental variable for exploring the relationship between Tor usage, dark platforms, and belief in misinformation (see Table 6).

When employing instrumental variables to estimate the relationships between using dark platforms and COVID-19 misinformation beliefs, both the weak instrument test (statistic=15.128,  $p < 0.001$ ) and Wu–Hausman test (statistic=5.803,  $p < 0.05$ ) yield significant and substantially large statistics. Consequently, the instrumental variable test is considered valid. According to the two-step least squares (2SLS) regression model, the use of dark platforms emerges as a significant predictor of COVID-19 misinformation belief ( $\beta = 1.048$ ,  $SE=0.343$ ,  $p < 0.01$ ). In addition, the inclusion of dark platforms as an explanatory variable in the model passes both the weak instrument test (statistic=15.128,  $p < 0.001$ ) and Wu–Hausman test (statistic=5.803,  $p < 0.05$ ), indicating statistical significance. The effect of dark platform usage on political misinformation belief is also significant ( $\beta = 0.857$ ,  $SE=0.318$ ,  $p < 0.01$ ).

Similar patterns are observed when examining the effect of using the Dark Web with the same instrumental variable. The weak instrument test (statistic=21.593,  $p < 0.001$ ) and the Wu–Hausman test (statistic=3.936,  $p < 0.05$ ) both yield significant and substantially large statistics. The use of the Dark Web is positively associated with belief in COVID-19 misinformation ( $\beta = 0.901$ ,  $SE=0.268$ ,  $p < 0.001$ ). Moreover, when incorporating the use of dark

**Table 6.** 2SLS regressions with instrumental variables.

	COVID-19 misbelief		Political misbelief	
Political Identity	0.075** (0.026)	0.075** (0.024)	0.026 (0.024)	0.026 (0.022)
Education	-0.167** (0.062)	-0.168** (0.057)	-0.132* (0.058)	-0.132* (0.053)
Income	-0.013 (0.011)	-0.011 (0.009)	-0.005 (0.010)	-0.003 (0.009)
Marriage	0.020 (0.078)	0.047 (0.074)	0.053 (0.073)	0.076 (0.070)
Area	0.180 (0.148)	0.243 (0.142)	0.152 (0.137)	0.205 (0.134)
Age	-0.004 (0.006)	-0.004 (0.006)	-0.003 (0.006)	-0.003 (0.006)
Gender	-0.072 (0.126)	-0.084 (0.116)	-0.101 (0.117)	-0.111 (0.109)
Traditional Media Use	-0.022 (0.068)	-0.029 (0.063)	-0.045 (0.063)	-0.051 (0.059)
Internet Use	0.082 (0.079)	0.048 (0.065)	0.183* (0.073)	0.156* (0.061)
Tor Network Use	-0.092 (0.099)	-0.057 (0.080)	-0.062 (0.092)	-0.034 (0.076)
Exposure to Dark Web Scandals	-0.177 (0.151)	-0.089 (0.114)	-0.185 (0.140)	-0.113 (0.107)
Dark Platform Use	1.048** (0.343)		0.857** (0.318)	
Dark Web Use		0.901*** (0.268)		0.738** (0.253)
Intercept	1.525* (0.637)	1.619** (0.565)	1.791** (0.591)	1.868*** (0.533)
Observations	702	702	702	702
R <sup>2</sup> /R <sup>2</sup> adjusted	0.192/0.177	0.332/0.320	0.069/0.053	0.207/0.194

\* $p < 0.05$ ; \*\* $p < 0.01$ ; \*\*\* $p < 0.001$ .

platforms as an explanatory variable, both the weak instrument test (statistic = 21.593,  $p < 0.001$ ) and the Wu–Hausman test (statistic = 3.341,  $p < 0.1$ ) produce significant and substantial results. Thus, the instrumental variable test is passed, and the use of dark platforms is positively linked to belief in political misinformation ( $\beta = 0.738$ ,  $SE = 0.253$ ,  $p < 0.01$ ).

In summary, the outcomes derived from traditional multiple regression analysis, PSM, and instrumental variables analysis exhibit remarkable consistency in both the direction and significance of effects, which underscores the robustness of the research findings. The analytical results uniformly signify that engagement with the dark side of the Internet, encompassing both dark platforms and the Dark Web, is positively correlated to heightened misinformation beliefs concerning both the COVID-19 pandemic and the 2020 US Presidential Election.

## Discussion

With an exceptionally high level of anonymity, the dark side of the Internet has become a crucial part of the online information ecosystem. However, the social and political implications of this new media technology remain largely unknown. The findings of this

study indicate that using the dark side of the Internet has a significant association with the beliefs in misinformation. The estimated coefficients obtained from hierarchical regressions slightly differ from those derived from PSM and 2SLS regressions utilizing instrumental variables. However, the differences primarily lie in the magnitude of the effects while maintaining the same direction. The relationships between the variables remain consistent across different analyses. While the effect sizes may differ, the direction of the relationships remains consistent. This suggests that the relationships observed between the variables are unlikely to be artifacts of a particular methodology or data treatment. Overall, this study's results paint a comprehensive picture suggesting that utilizing dark platforms and the Dark Web has a potent influence on user attitudes, particularly in terms of believing misinformation in public health crises and political contexts during an election.

### Theoretical implications

This study offers significant theoretical implications by establishing a novel link between the “dark side of the Internet” and the dissemination of misinformation. By examining the COVID-19 pandemic and

the US presidential election—two high-profile events with far-reaching consequences—the research pioneers the exploration of how anonymous online platforms influence societal discourse during critical periods (Green et al., 2022; Kerr et al., 2021). This dual focus not only advances our understanding of the dark side of the Internet but also enriches our knowledge of how such platforms intersect with significant socio-political events. After accounting for reverse causality, our findings still indicate a significant positive effect of dark web usage on individuals' misinformation belief. This suggests that even if users do not have a predisposition for using dark platforms, mere exposure—whether accidental or not—might guide them to be influenced by prevalent misinformation and develop stronger misinformation belief. These results confirm the media effect pathway and further highlight the negative impacts of dark platforms on society (Sirola et al., 2022).

In addition, this study provides solid evidence supporting the negative impacts of information manipulation within conservative media environments. Prior research has demonstrated that malicious communicators within conservative media ecosystems, such as the dark web, can more easily manipulate information through the aggregation of information into evidence collages and platform filtering (Krafft & Donovan, 2020). Whereas, these studies have not fully explored whether a conservative media environment can actually intensify misinformation beliefs among its users. This study introduces a robust outcome variable for this relationship and may serve as a crucial mediating variable for future research on how conservative media environments influence specific human behaviors.

### *Practical implications*

Practically, this research provides valuable insights that can serve as a compass for policymakers, law enforcement agencies, and online platforms in formulating precisely targeted interventions aiming at mitigating the adverse consequences linked to the dark side of the Internet (Davis & Arrigo, 2021). Our findings underscore the urgent need for continued, comprehensive research into the dynamic

landscape of the Dark Web and its far-reaching societal implications. Such knowledge is essential for developing effective countermeasures against illicit activities, safeguarding vulnerable populations, and promoting digital well-being. By illuminating the complexities of the Dark Web, policymakers can work toward a safer, more informed, and ethical online ecosystem.

For policymakers and law enforcement agencies, this study highlights the crucial role digital platforms play in shaping individual and collective perceptions. While prior research predominantly concentrated on online behaviors and interactions within such platforms (Alharbi et al., 2021; Bracci et al., 2021), this study broadens its scope to understand how these interactions extend into the offline world. The findings reveal a notable positive effect of the dark side of the Internet on misinformation beliefs. By placing particular emphasis on the relationships between the dark side of the Internet and misinformation beliefs, the research enriches existing theoretical frameworks (Barton, 2016; Devine et al., 2015), which emphasizes the transformative power of digital environments, particularly the “dark” alternative media platforms, on individuals' real-world beliefs and actions.

For online platforms, the research findings, in a broader context, shed light on the complex dynamics of online communication within anonymous platforms. With the increase in deplatforming measures, many contents (e.g. extreme ideologies and hate speech) are censored and restricted by online media platforms (Rogers, 2020). However, the moderated online contents do not necessarily disappear when they are cracked down by major Internet platforms, as they may shift to alternative media outlets. A significant portion of these restricted contents, such as extreme ideologies and hate speech, tend to escape into the dark side of the Internet. Over time, as malicious contents always find an audience, they tend to percolate back to mainstream websites on the Internet (Johnson et al., 2019). Therefore, understanding and managing online information environments necessitate careful consideration of the entire system. The dark side of the Internet should be particularly recognized as a vital

component of the overall landscape of online information ecology (Jardine, 2019).

### *Limitations and future directions*



There are several limitations to consider in interpreting this study's findings. First of all, the sampling approach employed was based on age and gender quotas. The study's sample may not accurately represent the diverse characteristics of the general users of the dark side of the Internet, thus could potentially introduce biases into the findings. Methodologically, caution is needed in interpreting the results related to PSM. Accurate estimation of propensity scores requires controlling for all potential confounders, which may not always be feasible in practice, leading to potential bias from omitted variables. In addition, this study focuses on the binary distinction between users and non-users of the dark side of the Internet, which simplifies the treatment variable for conceptual and operational convenience. Exploring more nuanced differences among users with varying levels of technology usage frequency through continuous coding could yield additional valuable insights. Finally, the cross-sectional nature of the data collection poses limitations in establishing the causal relationships between Tor usage and misinformation beliefs. Incorporating longitudinal data in future research could provide a more robust understanding of the temporal dynamics and causal effects involved.

The generalizability of this study's findings is mainly constrained by its focus on specific online platforms identified within the participant survey. While the literature has referenced a broad spectrum of platforms constituting the dark side of the Internet, such as Reddit, the study's results are exclusively applicable to 4chan, 8kun, and several other Dark Web websites. This narrowed scope limits the extrapolation of findings to the broader digital landscape. To mitigate this limitation, future research should expand its scope to encompass a wider array of online platforms and facilitate a more nuanced exploration of Dark Web usage, including variations in user behaviors, motivations, and involvement in different illicit activities or online communities. Future studies may generate further insights to

inform policy development, shape intervention strategies, and empower individuals to navigate the rapidly evolving digital landscape.

Despite all the limitations, this study offers a valuable foundation for further research in understanding the social implications of the dark side of the Internet. The findings shed light on the intricate and often hidden aspects of online behaviors and the consequences that arise from engaging with the darker corners of the digital realm. Future researchers can explore alternative sampling strategies to enhance the representativeness of the sample, allowing for a more accurate reflection of the diverse population engaging with the dark side of the Internet. Longitudinal data collection can also be employed to establish temporal and causal relationships. By addressing these methodological shortcomings, future studies may provide more insights into the evolving ecology of online behaviors and their offline consequences.

### **ORCID iDs**

Zhicong Chen  <https://orcid.org/0000-0003-0334-9454>  
Yixiao Sun  <https://orcid.org/0009-0005-2272-9067>

### **Notes**

1. The data are available on the OSF: <https://osf.io/9m78f/>
2. We chose to utilize LUCID for data collection due to its ability to efficiently recruit a nationally representative sample. While self-administered surveys offer greater control over data collection, LUCID's established infrastructure and respondent pool allowed us to gather a larger and more diverse sample within a shorter timeframe. This approach was particularly beneficial for capturing a broad range of demographic groups, enhancing the generalizability of our findings. Notably, LUCID has been used in other studies, which underscores its credibility and utility in academic research (such as Yu et al., 2024).

### **References**

- Ahmed, S., & Rasul, M. E. (2022). Social media news user and COVID-19 misinformation engagement: Survey study. *Journal of Medical Internet Research*, 24(9), Article e38944. <https://doi.org/10.2196/38944>

- Alfosail, M., & Norris, P. (2021). Tor forensics: Proposed workflow for client memory artefacts. *Computers & Security, 106*, Article 102311.
- Alharbi, A., Faizan, M., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Exploring the Topological Properties of the Tor Dark Web. *IEEE Access, 9*, 21746–21758. <https://doi.org/10.1109/access.2021.3055532>
- Anspach, N. M., & Carlson, T. N. (2022). Not who you think? Exposure and vulnerability to misinformation. *New Media & Society, 26*, 4847–4866. <https://doi.org/10.1177/14614448221130422>
- Atton, C. (2006). Far-right media on the internet: Culture, discourse and power. *New Media & Society, 8*(4), 573–587. <https://doi.org/10.1177/1461444806065653>
- Avarikioti, G., Brunner, R., Kiayias, A., Wattenhofer, R., & Zindros, D. (2018). *Structure and content of the visible darknet*. arXiv: 1811.01348 [cs]. <http://arxiv.org/abs/1811.01348>
- Baele, S. J., Brace, L., & Coan, T. G. (2023). Uncovering the far-right online ecosystem: An analytical framework and research agenda. *Studies in Conflict & Terrorism, 46*(9), 1599–1623.
- Barratt, M. J., & Aldridge, J. (2020). No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions. *International Journal of Drug Policy, 83*, Article 102894. <https://doi.org/10.1016/j.drugpo.2020.102894>
- Barrera, O., Guriev, S., Henry, E., & Zhuravskaya, E. (2020). Facts, alternative facts, and fact checking in times of post-truth politics. *Journal of Public Economics, 182*, 104–123. <https://doi.org/https://doi.org/10.1016/j.jpubeco.2019.104123>
- Barton, H. (2016). The dark side of the Internet. In I. Connolly, M. Palmer, H. Barton, & G. Kirwan (Eds.), *An introduction to cyberpsychology* (pp. 58–70). Routledge.
- Bergeron, A., Decary-Hetu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy, 83*, Article 102870. <https://doi.org/10.1016/j.drugpo.2020.102870>
- Beshiri, A. S., & Susuri, A. (2019). Dark web and its impact in online anonymity and privacy: A critical analysis and review. *Journal of Computer and Communications, 7*(3), 30–43. <https://doi.org/10.4236/jcc.2019.73004>
- Bracci, A., Nadini, M., Aliapoulos, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2021). Dark Web Marketplaces and COVID-19: Before the vaccine. *EPJ Data Science, 10*(1), Article 6. <https://doi.org/10.1140/epjds/s13688-021-00259-w>
- Caiani, M., & Parenti, L. (2009). The dark side of the web: Italian right-wing extremist groups and the Internet. *South European Society and Politics, 14*(3), 273–294.
- Cantarella, M., Fraccaroli, N., & Volpe, R. (2023). Does fake news affect voting behaviour? *Research Policy, 52*(1), Article 104628.
- Carlson, M. (2020). Fake news as an informational moral panic: The symbolic deviancy of social media during the 2016 US presidential election. *Information, Communication & Society, 23*(3), 374–388.
- Chen, H. C. (2008). Sentiment and affect analysis of dark web forums: Measuring radicalization on the internet [Conference session]. In *ISI 2008: 2008 IEEE international conference on intelligence and security informatics*, Taipei, Taiwan, 17–20 June, pp. 104–109. IEEE.
- Chen, Z., Jardine, E., Fan Liu, X., & Zhu, J. J. H. (2024). Seeking anonymity on the Internet: The knowledge accumulation process and global usage of the Tor network. *New Media & Society, 26*(2), 1074–1095. <https://doi.org/10.1177/14614448211072201>
- Chen, Z., & Liu, X. (2021). *Why do users leave anonymous online communities? An exploratory study of the silk road forum on the dark web*. In 71st Annual International Communication Association Conference (ICA21), Denver, CO, 27–31 May.
- Chen, Z., Meng, X., & Wang, C.-J. (2023). The dark web privacy dilemma: Linguistic diversity, talkativeness, and user engagement on the cryptomarket forums. *Humanities and Social Sciences Communications, 10*(1), Article 903. <https://doi.org/10.1057/s41599-023-02424-0>
- Chen, Z., Meng, X., & Yu, W. (2021). *Depolarization in the rise of far-right platforms? A moderated mediation model on political identity, misinformation belief and voting behavior in the 2020 US Presidential Election*. 2021 International Association for Media and Communication Research Conference (IAMCR 2021): Rethinking Borders and Boundaries.
- Cookson, D., Jolley, D., Dempsey, R. C., & Povey, R. (2021). “If they believe, then so shall I”: Perceived beliefs of the in-group predict conspiracy theory belief. *Group Processes & Intergroup Relations, 24*(5), 759–782. <https://doi.org/10.1177/1368430221993907>
- Davis, S., & Arrigo, B. (2021). The Dark Web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change, 76*(4), 367–386.

- De Coninck, D., Frissen, T., Matthijs, K., d'Haenens, L., Lits, G., Champagne-Poirier, O., Carignan, M.-E., David, M. D., Pignard-Cheynel, N., & Salerno, S. (2021). Beliefs in conspiracy theories and misinformation about COVID-19: Comparative perspectives on the role of anxiety, depression and exposure to and trust in information sources. *Frontiers in Psychology, 12*, Article 646394.
- Devine, J., Egger-Sider, F., & Rojas, A. (2015). The evolving impact of the invisible web: Exploring economic and political ramifications. *Journal of Web Librarianship, 9*(4), 145–161. <https://doi.org/10.1080/019322909.2015.1077183>
- Druckman, J. N., Klar, S., Krupnikov, Y., Levendusky, M., & Ryan, J. B. (2021). How affective polarization shapes Americans' political beliefs: A study of response to the COVID-19 pandemic. *Journal of Experimental Political Science, 8*(3), 223–234.
- ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Sci Rep, 10*(1), Article 18827. <https://doi.org/10.1038/s41598-020-74416-y>
- Enders, A. M., Uscinski, J. E., Seelig, M. I., Klofstad, C. A., Wuchty, S., Funchion, J. R., Murthi, M. N., Premaratne, K., & Stoler, J. (2023). The Relationship Between Social Media Use and Beliefs in Conspiracy Theories and Misinformation. *Political Behavior, 45*(2), 781–804. <https://doi.org/10.1007/s11109-021-09734-6>
- Europol. (2019). *Advisory network on terrorism and propaganda workshop: "Defining the global right-wing extremist movement."* <https://www.europol.europa.eu/newsroom/news/advisory-network-terrorism-and-propaganda-workshop-%E2%80%9Cdefining-global-right-wing-extremist-movement%E2%80%9D>
- French, T., & Epiphaniou, G. (2015). The world "wild" web: Cyber-security intelligence gathering opportunities from the "dark" side. *Liss, 2013*, 1265–1270. [https://doi.org/10.1007/978-3-642-40660-7\\_190](https://doi.org/10.1007/978-3-642-40660-7_190)
- Gaudette, T., Scrivens, R., Davies, G., & Frank, R. (2020). Upvoting extremism: Collective identity formation and the extreme right on Reddit. *New Media & Society, 23*, 3491–3508. <https://doi.org/10.1177/1461444820958123>
- Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 18*(7), 1219–1235. <https://doi.org/10.1177/1461444814554900>
- Gehl, R. W. (2018). *Weaving the Dark Web Legitimacy on Freenet, Tor, and I2P*. MIT Press. <https://doi.org/10.7551/mitpress/11266.001.0001>
- Gollust, S. E., Nagler, R. H., & Fowler, E. F. (2020). The Emergence of COVID-19 in the US: A Public Health and Political Communication Crisis. *Journal of Health Politics, Policy and Law, 45*(6), 967–981. <https://doi.org/10.1215/03616878-8641506>
- Green, J., Hobbs, W., McCabe, S., & Lazer, D. (2022). Online engagement with 2020 election misinformation and turnout in the 2021 Georgia runoff election. *Proceedings of the National Academy of Sciences, 119*(34), Article e2115900119.
- Gunther, R., Beck, P. A., & Nisbet, E. C. (2019). "Fake news" and the defection of 2012 Obama voters in the 2016 presidential election. *Electoral Studies, 61*, Article 102030.
- Hagen, S. (2022). "Who is/ourguuy??" Tracing panoramic memes to study the collectivity of 4chan/pol. *New Media & Society, 26*, 1735–1755.
- Hameleers, M., Brosius, A., & de Vreese, C. H. (2022). Whom to trust? Media exposure patterns of citizens with perceptions of misinformation and disinformation related to the news media. *European Journal of Communication, 37*(3), 237–268.
- Hansen, B. B. (2004). Full matching in an observational study of coaching for the SAT. *Journal of the American Statistical Association, 99*(467), 609–618. <https://doi.org/10.1198/016214504000000647>
- Imai, K., & Ratkovic, M. (2014). Covariate balancing propensity score. *Journal of the Royal Statistical Society Series B-statistical Methodology, 76*(1), 243–263. <https://doi.org/10.1111/rssb.12027>
- Imbens, G. W., & Rubin, D. B. (2015). *Causal inference in statistics, social, and biomedical sciences*. Cambridge University Press.
- Jardine, E. (2019). Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the darknet. *First Monday, 24*(12), Article 10266. <https://doi.org/10.5210/fm.v24i12.10266>
- Jiang, S. (2022). The roles of worry, social media information overload, and social media fatigue in hindering health fact-checking. *Social Media + Society, 8*(3), Article 20563051221113070. <https://doi.org/10.1177/20563051221113070>
- Jin, J., Williams, E., Lam, S., Savas, O., Hohman, E., Bosch-Ruiz, M., & Rodrigues, P. (2020). *Analysis of evolution of meme trends on 4chan.Org's/pol/board via image clustering*. <https://www.cmu.edu/ideas-social>

- cybersecurity/events/conference-archive/2020papers/afs\_4chan\_meme\_clustering.pdf
- Jin, P., Kim, N., Lee, S., & Jeong, D. (2023). Forensic investigation of the dark web on the Tor network: Pathway toward the surface web. *International Journal of Information Security*, 23, 331–346.
- Johnson, N. F., Leahy, R., Restrepo, N. J., Velasquez, N., Zheng, M., Manrique, P., Devkota, P., & Wuchty, S. (2019). Hidden resilience and adaptive dynamics of the global online hate ecology. *Nature*. <https://doi.org/10.1038/s41586-019-1494-7>
- Kavallieros, D., Chalanouli, C., Kokkinis, G., Papathanasiou, A., Lissaris, E., Leventakis, G., Giataganas, G., & Germanos, G. (2018). *Searching for crime on the web: Legal and Ethical perspectives*. 2018 international conference on cyber security and protection of digital services (Cyber Security).
- Kerr, J., Panagopoulos, C., & Van der Linden, S. (2021). Political polarization on COVID-19 pandemic response in the United States. *Personality and Individual Differences*, 179, Article 110892. <https://doi.org/https://doi.org/10.1016/j.paid.2021.110892>
- Kobayashi, T. (2018). Is the power of online campaigning in Japanese electoral politics a myth? A causal inference analysis of the 2013 Upper House Election. In S. Kiyohara, K. Maeshima, & D. Owen (Eds.), *Internet Election Campaigns in the United States, Japan, South Korea, and Taiwan* (pp. 115–136). Springer. [https://doi.org/10.1007/978-3-319-63682-5\\_5](https://doi.org/10.1007/978-3-319-63682-5_5)
- Krafft, P. M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication*, 37(2), 194–214. <https://doi.org/10.1080/10584609.2019.1686094>
- Lai, K., Xiong, X., Jiang, X., Sun, M., & He, L. (2020). Who falls for rumor? Influence of personality traits on false rumor belief. *Personality and Individual Differences*, 152, Article 109520. <https://doi.org/10.1016/j.paid.2019.109520>
- Lemaire, P. (2023). Online censorship and young people's use of social media to get news. *International Political Science Review*. <https://doi.org/10.1177/01925121231183105>
- Leyva, R., & Beckett, C. (2020). Testing and unpacking the effects of digital fake news: On presidential candidate evaluations and voter support. *Ai & Society*, 35, 969–980.
- Mansoor, M. (2021). Citizens' trust in government as a function of good governance and government agency's provision of quality information on social media during COVID-19. *Government Information Quarterly*, 38(4), Article 101597.
- Martin, J., Cunliffe, J., Decary-Hetu, D., & Aldridge, J. (2018). Effect of restricting the legal supply of prescription opioids on buying through online illicit marketplaces: Interrupted time series analysis. *BMJ*, 361, Article k2270. <https://doi.org/10.1136/bmj.k2270>
- McSwiney, J., Vaughan, M., Heft, A., & Hoffmann, M. (2021). Sharing the hate? Memes and transnationality in the far right's digital visual culture. *Information, Communication & Society*, 24(16), 2502–2521.
- Nagle, A. (2017). *Kill all normies: Online culture wars from 4chan and Tumblr to Trump and the alt-right*. John Hunt Publishing.
- Nissenbaum, A., & Shifman, L. (2017). Internet memes as contested cultural capital: The case of 4chan's /b/board. *New Media & Society*, 19(4), 483–501. <https://doi.org/10.1177/1461444815609313>
- Nugent, T. J. (2019). Prosecuting dark net drug marketplace operators under the federal crack house statute. *Fordham Law Review*, 88(1), 345–379. <https://ir.lawnet.fordham.edu/flr/vol88/iss1/9>
- Obreja, D. M. (2024). The social side of cryptocurrency: Exploring the investors' ideological realities from Romanian Facebook groups. *New Media & Society*, 26, 2748–2765.
- Owen, G., & Savage, N. (2016). Empirical analysis of tor hidden services. *Iet Information Security*, 10(3), 113–118. <https://doi.org/10.1049/iet-ifs.2015.0121>
- Ranaldi, L., Ranaldi, F., Fallucchi, F., & Zanzotto, F. M. (2022). Shedding light on the dark web: Authorship attribution in radical forums. *Information*, 13(9), 435.
- Ravindran, T., Yeow Kuan, A. C., & Hoe Lian, D. G. (2014). Antecedents and effects of social network fatigue. *Journal of the Association for Information Science and Technology*, 65(11), 2306–2320. <https://doi.org/10.1002/asi.23122>
- Razaque, A., Valiyev, B., Alotaibi, B., Alotaibi, M., Amanzholova, S., & Alotaibi, A. (2021). Influence of COVID-19 epidemic on dark web contents. *Electronics*, 10(22), Article 2744.
- Reedy, J., Wells, C., & Gastil, J. (2014). How Voters Become Misinformed: An Investigation of the Emergence and Consequences of False Factual Beliefs. *Social Science Quarterly*, 95(5), 1399–1418. <https://doi.org/https://doi.org/10.1111/ssqu.12102>
- Robertson, C. E., Pretus, C., Rathje, S., Harris, E. A., & Van Bavel, J. J. (2022). How social identity shapes conspiratorial belief. *Current Opinion in Psychology*, 47, Article 101423. <https://doi.org/10.1016/j.copsyc.2022.101423>

- Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication*, 35(3), 213–229.
- Rosso, M., Nasir, A., & Farhadloo, M. (2020). Chilling effects and the stock market response to the Snowden revelations. *New Media & Society*, 22(11), 1976–1995. <https://doi.org/10.1177/1461444820924619>
- Sanchez-Rola, I., Balzarotti, D., & Santos, I. (2017). The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services. *Proceedings of the 26Th International Conference on World Wide Web Www'17*, 1251–1260. <https://doi.org/10.1145/3038912.305265>
- Schroeder, R. (2019). Digital Media and the Entrenchment of Right-Wing Populist Agendas. *Social Media + Society*, 5(4), Article 2056305119885328. <https://doi.org/10.1177/2056305119885328>
- Sirola, A., Nuckols, J., Nyrhinen, J., & Wilska, T.-A. (2022). The use of the Dark Web as a COVID-19 information source: A three-country study. *Technology in Society*, 70, Article 102012.
- Sirola, A., Savolainen, I., & Oksanen, A. (2024). Who uses the dark web? Cross-national and longitudinal evidence on psychosocial, behavioral, and individual predictors. *Personality and Individual Differences*, 227, Article 112709. <https://doi.org/10.1016/j.paid.2024.112709>
- Soldatos, J. (2017). Designing Systems for Terroristic Indicators Analysis Based on Visible, Social and Dark Web Data Sources. *Risk of Skilled Scientist Radicalization and Emerging Biological Warfare Threats*, 138, 82–93. <https://doi.org/10.3233/978-1-61499-802-0-82>
- Stepińska, A. M., Theocharis, Y., Cardenal, A., Jin, S., Aalberg, T., Hopmann, D. N., Strömbäck, J., Castro, L., Esser, F., & Van Aelst, P. (2023). Does the platform matter? Social media and COVID-19 conspiracy theory beliefs in 17 countries. *New Media & Society*, 25, 3412–3437.
- Taurino, A., Colucci, M. H., Bottalico, M., Franco, T. P., Volpe, G., Violante, M., Grattagliano, I., & Laera, D. (2023). To believe or not to believe: Personality, cognitive, and emotional factors involving fake news perceived accuracy. *Applied Cognitive Psychology*, 37(6), 1444–1454. <https://doi.org/10.1002/acp.4136>
- The Tor Project. (2022). *Tor metrics: Users*. <https://metrics.torproject.org/userstats-relay-country.html>
- Törnberg, A., & Törnberg, P. (2023). White supremacists anonymous: How digital media emotionally energize far-right movements. *Journal of Information Technology & Politics*, 2023, 1–18.
- Tuters, M., & Hagen, S. (2019). (((They))) rule: Memetic antagonism and nebulous othering on 4chan. *New Media & Society*. <https://doi.org/10.1177/1461444819888746>
- US Census Bureau. (2019). *Age and sex composition in the United States: 2019*. <https://www.census.gov/data/tables/2019/demo/age-and-sex/2019-age-sex-composition.html>
- Van Bavel, J. J., Rathje, S., Vlasceanu, M., & Pretus, C. (2024). Updating the identity-based model of belief: From false belief to the spread of misinformation. *Current Opinion in Psychology*, 56, Article 101787. <https://doi.org/10.1016/j.copsyc.2023.101787>
- Vandiver, J. (2020). Alt-virilities: Masculinism, rhizomatics, and the contradictions of the American Alt-Right. *Politics, Religion & Ideology*, 21(2), 153–176.
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Weill, K. (2020). *Trump lost, one of the administrators quit, and it's far from clear who's in charge*. <https://www.thedailybeast.com/qanons-home-8kun-is-implodingand-q-has-gone-silent>
- Wells, C., Reedy, J., Gastil, J., & Lee, C. (2009). Information distortion and voting choices: The origins and effects of factual beliefs in initiative elections. *Political Psychology*, 30(6), 953–969. <https://doi.org/10.1111/j.1467-9221.2009.00735.x>
- Wolfowicz, M., Weisburd, D., & Hasisi, B. (2023). Examining the interactive effects of the filter bubble and the echo chamber on radicalization. *Journal of Experimental Criminology*, 19(1), 119–141. <https://doi.org/10.1007/s11292-021-09471-0>
- Yu, W., Chen, Z., Meng, X., & Yan, Q. (2024). Propagating COVID-19 Conspiracy Theories: The Influence of Right-Wing Sources. *Sage Open*, 14(2), 21582440241258026. <https://doi.org/10.1177/21582440241258026>
- Zaunseeder, A., & Bancroft, A. (2019). The fuzzy ideological and social space of the cryptomarkets: Libertarian ideology, agorism and exchange performances. In M. Tzanetakis & H. Stöver (Eds.), *Drogen, Darknet und Organisierte Kriminalität: Herausforderungen für Politik, Justiz und Drogenhilfe* (1st ed.) (pp. 137–160). Nomos Verlagsgesellschaft mbH & Co. KG. <https://doi.org/10.5771/9783845282831-137>
- Zeng, J., & Schäfer, M. S. (2021). Conceptualizing “dark platforms.” Covid-19-related conspiracy theories on 8kun and Gab. *Digital Journalism*, 9(9), 1321–1343. <https://doi.org/10.1080/21670811.2021.1938165>

Zimmermann, F., & Kohring, M. (2020). Mistrust, disinforming news, and vote choice: A panel survey on the origins and consequences of believing disinformation in the 2017 German Parliamentary Election. *Political Communication*, 3(2), 7215–7237. <https://doi.org/10.1080/10584609.2019.1686095>

### Author biographies

Zhicong Chen is a Research Assistant Professor at the School of Journalism and Communication, Nanjing University. His research focuses on computational social science and digital humanities.

Wenting Yu is an Assistant Professor at the Department of Chinese and Bilingual Studies, the Hong Kong Polytechnic University. She is interested in public opinion, health communication and the social impacts of new communication technology.

Yixiao Sun is a master's student at the School of Journalism and Communication, Nanjing University.

Her research focuses on computational psycholinguistics, examining how communicative materials influence both societal institutions and individual mental states and behaviours.

Cheng-Jun Wang is a Full Professor at the School of Journalism and Communication, Nanjing University. His research interest focuses on employing big data, computational methods and social theories to study human communication behaviours, including but not limited to information diffusion, attention flow and computational narrative. His research on computational communication appears in both SSCI- and SCI-indexed journals.

Xiao Fan Liu is an Assistant Professor at the Department of Media and Communication, City University of Hong Kong. Dr. Liu's research focuses on human behaviours in the cryptocurrency industry, on the Internet and in the dark web. His research has been published in top-tier journals such as *The Lancet Digital Health* and *New Media & Society*. He is an associate editor of *IEEE Transactions on Computational Social Systems*.