Lin, Trisha T. C.

Conference Paper

Investigating the relationship of disguised socialbots and disinformation threat in Taiwan

31st European Conference of the International Telecommunications Society (ITS): "Reining in Digital Platforms? Challenging monopolies, promoting competition and developing regulatory regimes", Gothenburg, Sweden, 20th - 21st June 2022

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Lin, Trisha T. C. (2022) : Investigating the relationship of disguised socialbots and disinformation threat in Taiwan, 31st European Conference of the International Telecommunications Society (ITS): "Reining in Digital Platforms? Challenging monopolies, promoting competition and developing regulatory regimes", Gothenburg, Sweden, 20th - 21st June 2022, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/265654

Investigating the relationship of disguised socialbots and disinformation threat in Taiwan

Trisha T. C. Lin, Ph.D.

Professor, Department of Radio and Television, National Chengchi University, Taiwan

Research fellow, Taiwan Institute for Governance and Communication Research

Address: No. 64, Sec. 2, ZhiNan Rd., Wenshan District, Taipei City 11605, Taiwan

Email: trishlin@nccu.edu.tw

Abstract

Taiwan has faced bot-driven disinformation campaigns during elections and COVID-19 outbreaks. Although past studies suggest ill-agenda socialbots accelerate and deteriorate disinformation influences, their relationship has not been examined quantitatively yet. To fill the research gap, this study aims to investigate the complex associations between socialbot attitude and disinformation interaction and related factors affecting disinformation threat. Disguised socialbots in this study refer to fake accounts to engage in malicious online activities via anthropomorphic social media interactions. A modified Theory of Planned Behavior (TPB) model is adapted to examine how socialbot attitudes and disinformation interaction are associated with perceived bot control and privacy concern, which influences disinformation threat. This web survey examines 750 Taiwanese socialbot users' perceptions and attitudes towards disguised socialbots in August 2021. Structural equation modeling (SEM) results show that socialbot attitude is positively associated with perceived bot control and disinformation interaction, but is not related to privacy concern. Disinformation interaction is positively associated with perceived bot control and privacy concern. That is, negative attitudes towards malicious socialbots result in users' increasing perceived bot control and competence with disinformation interaction. Additionally, the more interaction with disinformation, the higher degree of perceived bot control and privacy concern about socialbots. Moreover, perceived bot control and privacy concern predicts disinformation threat. Implications are discussed.

Keywords: Socialbot, disinformation, Theory of Planned Behavior, perceived bot control, privacy concern

1. Introduction

When Socialbot campaigns are purposefully designed for harm, they result in rumors, spam and disinformation (Al-Rawi, Groshek, & Zhang, 2018). Socialbots controlled by automated algorithms refer to fraudulent accounts on social media that mimicking human behaviors to mislead users (Lin, 2021). Socialbots were detected as influential voices in disseminating conspiracies and propaganda during elections and epidemic emergencies (Rabello, et al., 2020). When global coronavirus outbreaks occurred, rampant socialbot activities that spread pandemic and vaccination misinformation worsen infodemic and pose threats to global public health (Ferrara, 2020). Socialbots likely reduce social media trust and increases risks of misinformation, which amplifies human negative affect and causes sentiment polarization (Shi, et al., 2020). Although past literature suggests the relationship between socialbots and disinformation, there has been no prior quantitative research yet. To fill the research gap, this web study aims to investigate the complex associations between socialbot attitude and disinformation interaction and related factors affecting disinformation threat.

Media reports and studies show that Taiwan has faced bot-driven disinformation campaigns during elections and COVID-19 outbreaks (Lin, 2021). It is crucial to examine the relationship between malicious Socialbots and disinformation in this research site. Disguised Socialbots are defined as fake accounts to engaging in malicious online activities through anthropomorphic social media interactions. Regarded malicious socialbot campaigns as risk, the present study's theoretic foundation is based on widely-used Theory of Planned Behavior (TPB) that links core beliefs (attitude, subjective norm, and perceived control) with individual behavioral intentions (Lin & Bautista, 2017). In the context of Socialbots, privacy concerns are regarded as the major subjective norm, as users tend to worry about their personal data misuse or leaking. Specifically, perceived bot control includes perceived controllability and perceived self-efficacy in bot detection. Additionally, Socialbots and disinformation likely result in risks to democracy and public health (Ferrara, 2020; Shi, et al., 2020), so this study proposes disinformation threat (Schmuck & von Sikorski, 2020) as the dependent variable to replace generic behavioral intention. Thus, a modified TPB model is adapted to examine how Socialbot attitudes and disinformation interaction are associated with perceived bot control and privacy concern, which influences disinformation threat.

The web survey was conducted in August 2021 to examine 750 Taiwanese

socialbot users' perceptions and attitudes towards the emerging technology. The cyberpanel sample above 20 years old fits 2021 Taiwanese social media user profile in demographic quotas (i.e., gender, age and education). Structural equation modeling (SEM) was used for statistical testing. The study that examines the relationship between malicious socialbots and disinformation threat contributes in theory and in practice. Theoretically, it extends a modified TPB to the context of socialbot and disinformation in order to understand users' media psychology during risks. It also finds that attitude can be treated as the precedent to behavioral control and social norm. Importantly, SEM results confirm the statistically significant relationship between socialbots and disinformation. Practically, it shed lights to the importance of promoting digital literacy about disguised socialbots (e.g., risks to democracy and public health) and disinformation interaction (e.g., differentiation and detection) because it can increase social media users' bot control and privacy concern, and thus improve perceived threat resulted from disinformation.

2. Literature Review

2.1 Theoretical Foundation

Theory of planned behavior (TPB) is an influential theory for predicting human behaviors and the processes that govern it (Barlet, 2019). According to Ajzen (2002, p.665), human actions are guided by "behavioral beliefs" about predicted results or other attributes of the behavior, "normative beliefs" about normative expectations of others, and "control beliefs" about preventing inhibitors from hindering behavioral performance. TPB has been widely employed from health-related research (Prabawanti et al., 2015) to various new media studies (Gretter & Yadav, 2018; Zhang et al., 2020) and risk communication research (Anser et al., 2020; Kim & Kim, 2020). Recently, scholars have extended the TPB in understanding various psychological and contextual factors (e.g., attitude, subjective norms, and perceived behavioral control) that predict social media users' adoption intention of emerging technologies (Anser et al., 2020) and perceived risk moderates the relationship between behavioral intentions and actual behaviors. Zhao et al (2016) employed the TPB to examine debunking disinformation on social media and found subjective norms and perceived behavioral control positively predicted intentions to combat rumors in times of social crises. Pundir et al. (2021) also used TPB as a basis for investigate social media users' intentions to verify news and debunk disinformation before sharing on social media. Thus, this study extends TPB theory to examine the context of socialbot and disinformation.

Social media that allow users to create and share contents reach gigantic numbers of people worldwide. However, disguised socialbots engaged in creating links and

purposeful interactions with targeted users that change the fabric of online social networks (Mitter et al., 2013; Pundir et al., 2021). Disguised socialbots are human-like false social media accounts. Controlled by puppetry masters, they could craft content rapidly and interacted with human users who unconsciously shared bot-driven contents (Ferrara et al., 2016). Disguised socialbots have created millions of social media pages containing incorrect, unreliable, and misleading contents affecting targeted individuals (Hajli et al., 2021). Several studies analyzed how socialbots on Twitter and Facebook twisted public perceptions and opinions by spamming, sabotaging, perplexing public discourse, manipulating social attitude, and carrying on propaganda (Bradshaw & Howard, 2017; Ferrara et al., 2016; Woolley & Howard, 2016). Hajli et al. (2021) discovered that twitter bots were utilized to promote disinformation and undermine public trust. In the context of political debates, Luceri et al. (2019) identified socialbots with polarized political leaning show different attitudes and discussion topics. These socialbots amplify human negative affect and causes sentiment polarization (Shi, et al., 2020), which likely increases risks of disinformation. Additionally, the interaction of disinformation increases social media users' perceived severity of socialbot threat (Lin et al., 2022). With advancements in AI technologies, it is increasingly difficult in detecting these socialbots, and thus the threat caused by socialbot campaigns become increasingly severe. Therefore, it is crucial to examine how socialbot attitude and disinformation interaction influence disinformation threat.

To fit the context of socialbot, this research model specially investigates how socialbot attitudes, perceived bot control and privacy concern are associated with disinformation threat, a substitute dependent variable of specific user intention. The reason why replaces TPB's subjective norm with privacy concern was that people felt most concerned about privacy invasion and personal data protection when encountering socialbots. This modified TPB is appropriate to investigate the complex associations between socialbot attitude and disinformation interaction and related factors affecting disinformation threat. It will enhance the understanding of the treat of socialbots and disinformation to democracy and public health.

2.2 Attitude with Socialbot

This study defines disguised socialbots as fake social media accounts to engaging in malicious online activities through anthropomorphic interactions (Lin et al., 2021). It specifies the TPB variable to be attitude with socialbots. Adapted from Wiesenberg and Tench (2020), attitude to socialbots in this study examines how social media users perceive socialbots as a threat for societies and public debates, a threat to organizations and their reputation, and ethical challenges for communication professionals.

Chatbots' anthropomorphic design can improve social presence communication that is mediated by parasocial interaction and thus increases user engagement (Tsai et al., 2021). Human-like socialbots tend to befriend opinion leaders and join in popular virtual communities help disguise their real identities and distribute purposeful information to trick other users' sharing. Controlled by the rich and powerful, they are algorithmic automated programming to promote contents with specific agendas. Examining socialbot campaigns in 2016 US elections, Howard et al. (2018) demonstrated how political bots interfered with political communication by facilitating surreptitious campaign coordination to illegally solicit contributions or votes, or violating rules. Although there were notable differences in the content and quality of human or chatbot communication (e.g., chatbots with shorter messages and less rich vocabulary) (Hill et al., 2015), the sophisticated AI technology increases the challenges to detect bots. Past studies also found how partisan identities lead to bias in identifying socialbots and how political bots exacerbate political polarization (Yan et al., 2020).

Howard et al. (2018) demonstrated how socialbots were frequently employed as strategic communication tactics in political domains. When Ferrara (2017) investigated twitter bots in MacronLeaks disinformation campaign, he found that spikes in socialbot-generated contents often arise before spikes in human posts, implying that bots could influence disinformation sharing. He also discovered a black-market for reusable socialbots that were controlled by bot masters' scripts to disseminate harmful disinformation. Due to the prevalent use of socialbots, netizens increasingly agreeing with and arguing to non-human users unconsciously, which results in sharing unreliable and misleading disinformation and undermine public trust in online discussions and cause socio-political chaos. They pose the threat to corporations' reputation, as well as to societies and public discussions (Wiesenberg & Tench, 2020). Media literacy about socialbots is likely to increase perceived behavioral control and thus reduce threats (Schmuck & von Sikorski, 2020).

Socialbots can used for malevolent online activities, including promoting certain objectives, manipulating online public opinion, and spreading misinformation (Lin et al., 2022). These disguised socialbots increase risks to virally disseminating disinformation that is deliberately conveyed to harm the public. Malicious socialbots likely pose a threat to users, when they are used to disseminating disinformation to manipulate public opinions (Ferrara, 2017). Shi et al. (2020) found socialbots agitated negative emotions like fear and anger and propel polarized disputes in controversial issues (e.g., vaccine). Socialbots that collect personal data without prior consent for micro-targeting in specific users also raise privacy concerns about misusing personal data or invading privacy. Thus, social media users tend to have negative attitude and

emotions towards socialbots, and perceive them as a threat when exposing to related news coverage (Schmuck & von Sikorski, 2020).

2.3 Perceived Bot Control

In the context of socialbots, this study uses perceived bot control to replace perceived behavioral control, a TPB variable affecting human intentions and behaviors. TPB's perceived control relates to people's perceptions of the ease or difficulty of doing the behavior of interest (Ajzen, 1991). Bandura's (1982) perceived self-efficacy that is concerned with judgments of how well one can execute courses of action to deal with situations underpins the logic of perceived behavioral control. Past studies show the overarching concept of perceived behavioral consiss of two components: self-efficacy (i.e., confidence in ability to perform a behavior) and controllability (i.e., the perception that a performance is up to the actor) (Terry & O'Leary, 1995). Drawing from Ajzen's (2002) perceived behavioral control, Schmuck and von Sikorski (2020, p.3) developed perceived bot control which includes two dimensions: perceived controllability (i.e., to the degree that one perceives the impact of bots on one's information seeking behavior and opinion formation as controllable) and perceived self-efficacy (i.e., one's perceived confidence in their ability to detect a bot). People' self-estimated ability of recognizing bots improves their accuracy in bot recognition (Yan et al., 2020). Perceived bot control in this study refers to investigate people's perceived ability to identify socialbots and prevent their harmful impacts on manipulating opinions.

People's trust in online information and digital democratic processes depends on their feelings of control. News reports about socialbot activities without explicating how they work or how to detect them likely deteriorate people's sense of control (Schmuck & von Sikorski, 2020). In the context of socialbots and human-computer interaction, people who feel less control of socialbots are more likely to avoid the encountering and feel threatened. Schmuck and von Sikorski (2020) that developed perceived bot control with good construct validity found that perceived bot control positively influenced perceived personal threats from socialbots. They examined perceived threats and fear emotions from socialbots from news coverage which could undermine trust in online political processes. Mass-mediated information to support literacy about disguised socialbots could increase perceived behavioral control and thus reduce threats (Schmuck & von Sikorski, 2020).

2.4 Privacy Concern

This present study uses privacy concern to replace subjective norm, a TPB variable affecting human intentions and behaviors. Adapted from Wei et al.'s privacy concern (2010), privacy concern is defined as the awareness about individuals' personal

data and their ability to control the dissemination of their personal information in this study. The four-item measure encompasses individual concerns about personal information to be stolen, misused or used in an unforeseen way for political or propaganda purposes. Privacy concerns restrict sharing private information during interactions to others who do not participate in (Goodwin, 1991). It involves lack of knowledge and consent about ways of personal data collecting (Culnan, 1995) and data usage purposes (Nowak & Phelps, 1992). People who felt more concerned about privacy were less inclined to give personal information to the third party (Sheehan & Hoy, 2000) without prior consent (Wei et al., 2010).

As lots of private information are available on social media, data privacy and security have become crucial issues. Xiao (2021) elaborated the primary concern that some users agreed to data mining of their personal data in exchange with incentives. When Taneja et al.'s study (2014) examined privacy concerns in using social media, they found that cost of not using privacy controls was affected by beliefs regarding resource vulnerability, threat severity, privacy risk and privacy intrusion. Past studies show that social media users avoid transactions over the platforms due to privacy and security reasons (Earp & Baumer, 2003), in addition to feeling insecure in the platforms' trustworthiness (Wei et al., 2010).

Kerr and Bornfreund (2005) characterized chatbots on social media as buddy bots, as the apps were utilized to capture valuable personal information and private communication without lawful authorization. Li et al. (2020) further discovered that socialbots could be used in a range of cyberattacks targeted at automatically collecting users' private data. The misuse of intelligent agents jeopardized fair privacy policies and invaded privacy rights since socialbots have created easy interchange of private data; in response to users' increasing privacy concerns, organizations should disclose the reasons for which personal data is obtained at or before data collection (Kerr & Bornfreund, 2005).

2.5 Disinformation Interaction

Interaction with disinformation was adapted from Reuter et al.'s (2019)'s six-item measurement of interaction with fake news by asking individual's perception and behaviors (e.g., like/dislike, comment, share, delete/report) when encountering disinformation. Reuter et al. (2019) examined Germany's perception of fake news (similar to disinformation in this study) and their interaction with it. Their findings show that majority regards fake news poses a threat and harm to democracy; slightly less than half have noticed fake news, while most reported never liked, shared or commented on fake news.

The United Nations defines disinformation as false and deliberately created information disseminating with orchestrated attempts to confuse or manipulate people through delivering dishonest information to them (Ireton & Posetti, 2018). The U.S. State Department regards disinformation as "the purposeful dissemination of false information intended to mislead or harm" (Nemr & Gangware, 2019). Jackson (2017) argued that disinformation involved black propaganda. According to Petratos (2021), disinformation, an emerging cyber risk, refers to the propagation of intentionally misleading information. The European Commission (2018) warns that "the creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public, and which may cause public harm" (European Court of Auditors, 2020).

Disinformation has become prevalent as social media facilitate the spread and sharing of false or misleading information with ease (Hwang et al., 2021; Shu et al., 2020b). Disinformation campaigns comprise a number of activities such as undercover (digital) activities or explicit actions (Petratos, 2021). Past research found that younger and relatively educated people were more informed about disinformation and liberal people tended to be more critical of fake news (Reuter et al., 2019). According to Zhao et al. (2016), social media users' attitudes positively influenced combating rumor intentions during the crisis; their intentions increased when peer interactions regarded combating disinformation as a norm and made collective actions to curb the spread of online falsehood.

Socialbots accelerated the spread of disinformation virally which led to social media users' perceived severity of socialbot threat (Lin et al., 2022). Individuals' prior knowledge of socialbots and their self-perceived ability to comprehend them affect their identifying socialbots (Yan et al., 2020). Shu et al. (2020b) suggested analyzed users' postings and comments such as ideas, attitudes, and sentiments, which could be used to spot disinformation. It is crucial to increase user awareness of disinformation, especially in debunking falsehood and identifying disguised socialbots. Multi-stakeholders' collaborative effort (e.g., government, social media platforms, media, NGOs, and civic society) will be necessary to help debunk disinformation and detect socialbots so as to protect vulnerable public from being harmed and safeguard democracy.

2.6 Disinformation Threat

Examining disinformation and cyber threat, Petratos (2021) discovered that disinformation campaigns distracted and manipulated people by presenting false information. Adapted from Reuter et al. (2019), disinformation threat in this study encompasses socialbot threat, harm to democracy, manipulating opinions of

politicians, journalists, influential players and the public. After the 2016 US presidential election, the debates on truthfulness of media and the spread of inaccurate information have been considered a serious threat to democracy (Lewandowsky et al., 2012). Disinformation brought danger to people's health, impaired public health experts and governments' effort to manage the covid-19 pandemic crisis (Shi et al., 2020). In the digital environment, disinformation has consistently shown to be a prevalent threat (Caramancion, 2020). Disinformation takes numerous forms, including text, photographs, and videos (Shu et al., 2020a; Zellers et al., 2019).The most serious cyber threats to communication trustworthiness could be the manipulation of audiovisual contents like deepfakes (Hameleers et al., 2020).

The algorithm of social media platforms resulted in filter bubbles and echo chamber effects on reinforcing like-minded perspectives; socialbots could deteriorate disinformation threat, propel socio-political polarization and hurt democracy (McKay & Tenove, 2021). Cyberattacks launched by disguised socialbots could automatically collect victims' private data to manipulate their opinions, attitudes and behaviors (Li et al., 2020). Socialbots also posed a threat to users' privacy as it has been debated about the ways of collecting personal data without prior consent. Perceived threats and fearful emotions resulting from socialbots on news coverage could undermine public trust in online political processes (Schmuck & von Sikorski, 2020).Leading communication professionals in various European regions perceived different levels of ethical challenges with respect to using socialbots (Wiesenberg & Tech, 2020). When disguised socialbots are created with the intent of causing harm, they produce falsehoods, spam, and disinformation, they are likely to erode social media trust and raise the risk of disinformation.

According to McKay and Tenove (2021), early detection of disinformation is crucial to minimize the damage to the number of people caused by disinformation; however, it is challenging for automatic detection of disinformation. Users' interaction with disinformation is critical for comprehending and potentially defending against the widespread of digital threats (Shu et al., 2020b). Majority held social media companies and the government liable for combating disinformation (Reuter et al., 2019). Mass-mediated information to support literacy about social bots could increase perceived behavioral control and thus reduce threats (Schmuck & von Sikorski, 2020).

2.7 Hypotheses & research model

Based on aforementioned literature, this study proposes the following hypotheses:

H1a : Attitude with socialbot is positively associated with perceived bot control.

H1b : Attitude with socialbot is positively associated with privacy concern.

H1c : Attitude with socialbot is positively associated with interaction with disinformation.

H2a : Interaction with disinformation is positively associated with perceived bot control.

H2b : Interaction with disinformation is positively associated with privacy concern.

H3a : Perceived bot control is positively associated with disinformation threat.

H3b : Privacy concern. is positively associated with disinformation threat.

Figure 1 shows the research model consisting of above hypotheses.

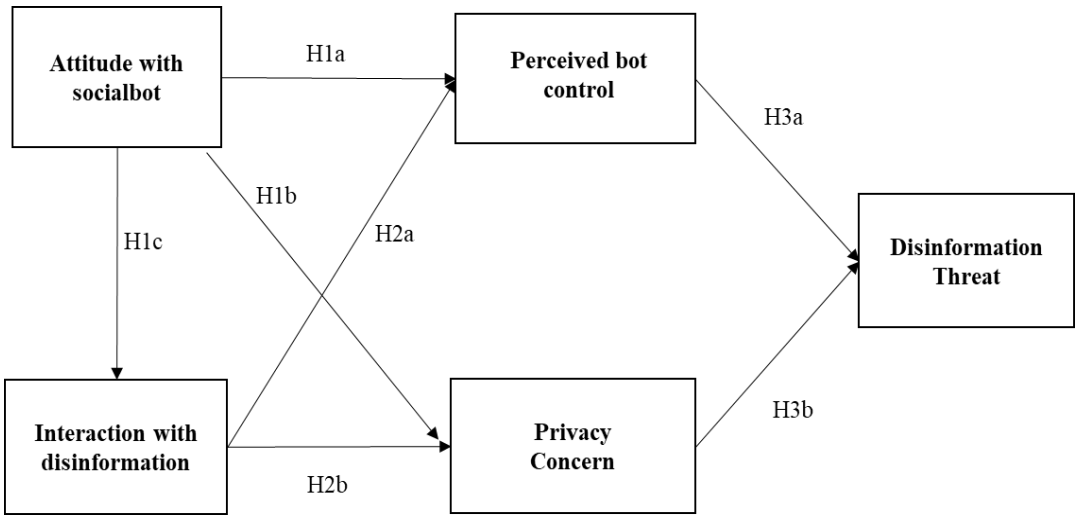


Figure 1. Proposed Research model

3. Methodology

3.1 Data Collection

The online survey was conducted to examine Taiwanese user perceptions and attitudes towards disguised socialbots in August 2021. The filtering criteria of the respondents from the cyberpanel of IXsurvey are Taiwanese social media above 20 years old with past experiences of socialbot use. The sample fit 2021 Taiwanese social media user profile in demographic quotas (i.e., gender, age and education attainments) based on InsightXplorer and Comscore data (IXresearch, 2020). Since socialbots are

emerging technologies, respondents were asked to watch a video about disguised socialbot before filling in the questionnaire. Disguised socialbot is defined in this study as human-like fake social media accounts used for malicious online activities to amplify selected agendas, manipulate online public opinions, and spread disinformation. The web survey research has obtained the approval from the Institute Review Board in the host university. Before data collection, the draft questionnaire has been pretest in July 2021 to improve the items' clarity and readability.

After data cleaning (e.g., removing with incomplete and invalid answers), 750 valid respondents were retained for data analysis. As G*power analysis shows that this study's sample size exceeds the minimum (N = 287) for model testing, indicating a power level of 80% for SEM analysis (Westland, 2010). The final sample fits the demographic quotas of Taiwanese social media users. Respondents' gender distribution is relatively equal (50.4% females and 49.6% males); more than half (51.7%) are aged 30-49 and were mostly well educated (65.46% with a Bachelor's degree and above). A majority (33.1%) earns a personal monthly income of NTD 20,001-40,000. Table 1 summarizes the respondents' demographic profile.

Table 1. Respondents' demographic profile

Sample characteristics (N =750).		Frequency	Percentage (%)
Gender	Male	372	49.6
	Female	378	50.4
Age	20-29	169	22.5
	30-39	192	25.6
	40-49	196	26.1
	50-59	154	20.5
	60 and older	39	5.3
Education	Elementary school	8	1.07
	Junior high school	16	2.13
	Senior high school/vocational high school	128	17.07
	Associate degree	107	14.27
	Bachelor's Degree	406	54.13
	Master's degree and above above	85	11.33
Individual Monthly income	Dependent/No income	36	4.8
	Unstable income	34	4.5
	NT20000 and below	53	7.1
	NT20001-40000	248	33.1

NT40001-60000	174	23.2
NT60001-80001	88	11.7
NT80001-100000	50	6.7
NT100001-150000	42	5.6
NT150001-200000	11	1.5
NT200,001 and above	14	1.9

Note: One Taiwan Dollar (NTD) is about US$0.036 as of September 1, 2021.

3.2 Measurement

Majority of measurements in this survey consists of items that derived from past studies and were modified to fit the context of disguised socialbots. Appendix 1 shows the list of items. Some items were dropped as their factor loadings were below the benchmark value of 0.70.

Attitude towards socialbots. The measure (α = 0.63, M = 2.99, SD =0.80) was adapted from Wiesenberg & Tench (2020)'s five-item measure of attitude towards about socialbot. Two items were dropped due to unsatisfied factor loading. A 5-point Likert scale was used to indicate responses (1 = strongly disagree, 5= strongly agree).

Privacy Concern. The measure (α = 0.94, M = 5.10, SD =1.25) was adapted from Wei, Hao & pang (2010)'s four-item measurement of about personal information. A 7-point Likert scale was used to indicate responses (1 = strongly disagree, 7= strongly agree).

Perceived Bot Control. The measure (α = 0.73, M = 4.52, SD =1.21) involved two dimensions: perceived controllability and perceived self-efficacy. Perceived controllability is a four-item measurement of perceived bot control adapted from Schmuck & von Sikorski (2020), but two items were dropped due to unsatisfied factor loading. Perceived self-efficacy is a three-item measurement of perceived bot control adapted from Yan, et al. (2020). Above of all a 7-point Likert scale was used to indicate responses (1 = strongly disagree, 7= strongly agree).

Disinformation Threat. The 10-item measure (α = 0.73, M = 3.73, SD =0.86) was adapted from Reuter et al. (2019). Two items were dropped as a result of unsatisfied factor loading. A 5-point Likert scale was used to indicate responses (1 = strongly disagree, 5= strongly agree).

Interaction with disinformation. Interaction with disinformation (α = 0.61, M = 3.23, SD =0.92) was adapted from Reuter et al. (2019)'s six-item measure of interaction with fake news. Two items that were modified to interacting with social media disinformation were retained after factor loading test. A 5-point Likert scale was used to indicate responses (1 = strongly disagree, 5= strongly agree).

Data analysis

This study first used SPSS 25 to compute for descriptive and reliability values. Next, it utilized Amos 26 to perform Structural equation modeling (SEM) analysis and indirect effects computation. SEM is a powerful, multivariate technique that was used increasingly in scientific investigations to detect the causal relationship between variables.

3.3 Results

Model fit

Prior to hypothesis testing, it is crucial to determine if the hypothesized model adequately fits the data. SEM results suggest that research model 1 has adequate fit to the data: X2/df = 3.67, CFI = 0.923, TLI = 0. 913, RMSEA =0.06 (90% CI= .056 .063), SRMR =0.09 (Hu & Bentler, 1999).

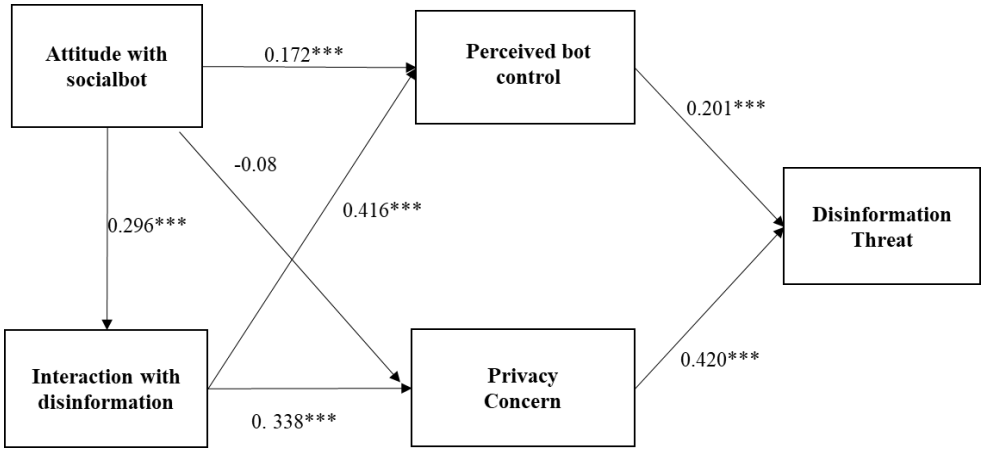


Figure 2. SEM analysis results of model 1

X^2/df = 3.67, CFI = 0.923, TLI = 0. 913, RMSEA =0.06 (90% CI= .056 .063), SRMR =0.09

*p <.05, ** p <.01, *** p <.001; n.s. = non-significant

SEM results and hypothesis testing

SEM results show that most of the hypothesis were accepted. Attitude with socialbot is positively associated with perceived bot control (b = .172, p <.001), thus H1a is supported. However, the results of H1b show non-significant, indicating that attitude with socialbot is not associated with privacy concern. Attitude with socialbot

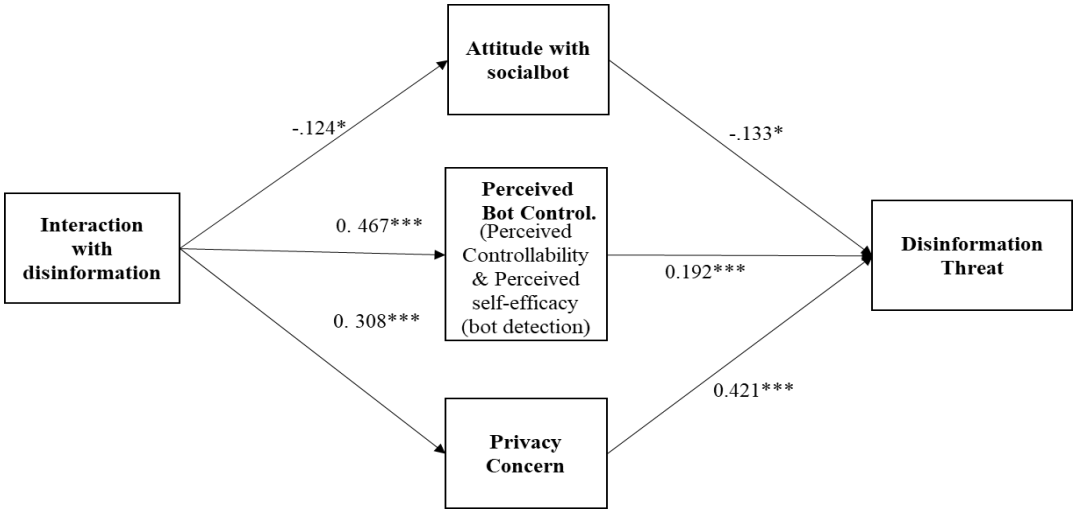
is positively associated with interaction with disinformation (b = .296, p <.001), thus H1c is supported. Interaction with disinformation is positively associated with Perceived bot control (b = .416, p <.001), thus H2a is supported. Interaction with disinformation is positively associated with privacy concern (b = .338, p <.001), thus H2b is supported. Perceived bot control is positively associated with disinformation threat (b = .201, p <.001), thus H3a is supported. Privacy concern is positively associated with disinformation threat (b = 0.420, p <.001), thus H3b is supported.

Table 3. Summary of hypothesis testing

Hypothesis		Path value	Decision
H1a	Attitude with socialbot → Perceived bot control	0.172***	Supported
H1b	Attitude with socialbot → Interaction with disinformation	n.s.	Rejected
H1c	Attitude with socialbot → Privacy concern	0.296***	Supported
H2a	Interaction with disinformation → Perceived bot control	0.416***	Supported
H2b	Interaction with disinformation → privacy concern	0.338***	Supported
H3a	Perceived bot control → disinformation threat	0.201***	Supported
H3b	Privacy concern → disinformation threat	0.420***	Supported

Notes: *p <.05, ** p <.01, *** p <.001, n.s. = non-significant. Results were controlled for age, gender, ethnicity, education and income

Next, this research conducted the SEM analysis for an alternative model that places three TPB variables as the mediators of the relationship between interaction with interaction with disinformation and disinformation threat.



X^2/df = 3.64, CFI = 0.932, TLI = 0. 923, RMSEA =0.059 (90% CI= .056 .063), SRMR =0.09

*p <.05, ** p <.01, *** p <.001; n.s. = non-significant

Figure 3. SEM analysis results of Model 2

After comparison, the model that treats socialbot attitudes as the precedent to bot control and privacy concern has stronger explanatory power than the one positioning three TPB variables in the middle. Thus, this study select model 1 (Figure 2) as the final research model.

4 Discussion & Conclusion

This study defines disguised socialbots as fake accounts to engage in malicious online activities via anthropomorphic social media interactions. Even though a growing body of western literature have studied malicious socialbots and disinformation (Al-Rawi et al., 2018), the present study is the first to investigate their relationship quantitatively and in Asian context. The modified TPB model regards socialbot attitude and disinformation interaction as the predictors to perceived bot control and privacy concern (replacing subjective norm), which thus influences disinformation threat. SEM results show that socialbot attitude is positively associated with perceived bot control and disinformation interaction, but it is not related to privacy concern. Taiwanese social media users who held negative attitudes towards disguised socialbots perceived their controllability and efficacy towards the emerging technology. Their attitudes towards socialbots positively predict their perception and behavioral responses to bots (e.g., like/dislike, share and comment). However, socialbot attitude has no impact on privacy concern. As Taiwan has two-party democracy and face China's cyberattacks, social media users likely feel more concerned about socialbots' spread of disinformation and manipulating public opinions, instead of socialbots' collecting personal data and invading privacy.

Next, disinformation interaction is positively associated with perceived bot control and privacy concern. The interactivity with disinformation could improve social media users' perceived controllability and perceived efficacy of socialbot use. If they could identify and debunk online false information, their perceived bot control would be boosted. However, when their experiences with disinformation interaction increased, they sensed severe digital threats and likely felt worried about personal information being illegally collected, misused or stolen. Finally, perceived bot control and privacy concern predicts disinformation threat. When social media users perceived their higher degree of bot control and privacy concern, they tended to be more critical of disinformation threat caused by malicious socialbot activities.

Theoretically, this research contributes to extend TPB to the context of socialbot and disinformation threat. Socialbot attitude is identified as the precedent to the other two TPB variables (perceived bot control and privacy concern as subjective norm), rather than being treated as a mediator. Meanwhile, interaction with disinformation is regarded as a type of media exposure. Its statistical results support the positive

relationship between socialbot attitude and interaction with disinformation as well as the overall impact on disinformation threat. Duplicate studies can be conducted in other contexts in Asia or western countries. Future studies are advised to examine how various emotions associated with socialbot attitudes affect disinformation threat. Two dimensions of perceived bot control (controllability efficacy) can be examined respectively to find out their influences on disinformation threat. Finally, the measure of disinformation threat could be further refined.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50(2): 179-211*. DOI: 10.1016/0749-5978(91)90020-T

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32(4): 665-683*. DOI: 10.1111/j.1559-1816.2002.tb00236.x

Al-Rawi, A., Groshek, J., & Zhang, L. (2018). What the fake? Assessing the extent of net worked political spamming and bots in the propagation of #fakenews on Twitter. *Online Information Review*. doi: 10.1108/oir-02-2018-0065

Anser, M., Zaigham, G., Rasheed, M., Pitafi, A., Iqbal, J., & Luqman, A. (2020). Social media usage and individuals' intentions toward adopting Bitcoin: The role of the theory of planned behavior and perceived risk. *International Journal of Communication Systems*, 33 (17). DOI: 10.1002/dac.4590

Bandura, A. (1982). Self-efficacy mechanism in human agency. *The American psychologist*, 37 (2): 122-147. DOI: 10.1037/0003-066X.37.2.122

Barlett, P. (2019). Social psychology theory extensions. *Predicting cyberbullying: Research, theory, and intervention* (pp. 37-47). DOI: 10.1016/B978-0-12-816653-6.00005-4

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238–246.

Bradshaw, S. & Howard, P. (2017). Troops,trolls and troublemakers: A global inventory of organized social media manipulation (Working paper No. 12). *Oxford*. Retrieved from Oxford Internet Institute website: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., Quinn, S. C., & Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *American Journal of Public Health*, 108(10), 1378-1384.

https://doi.org/10.2105/ajph.2018.304567

Burkhardt, J. (2017). Combating fake news in the digital age (Chapter 4: Can we save ourselves?). *American Library Association TechSource*, 53 (8). DOI: 10.5860/ltr.53n8. Retrieved from https://journals.ala.org/index.php/ltr/article/view/6500/8639

Caramancion, K. (2020). An exploration of disinformation as a cybersecurity threat. *2020 3rd International Conference on Information and Computer Technologies (ICICT), 440-444*. DOI: 10.1109/ICICT50521.2020.00076

Culnan, M. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, 9(2): 10-19. DOI: 10.1002/dir.4000090204

Earp, J. & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, 46 (4): 81-83. DOI: doi.org/10.1145/641205.641209

European Court of Auditors. (2020). *EU action plan against disinformation*. Retrieved from https://www.eca.europa.eu/Lists/ECADocuments/AP20_04/AP_Disinformation_EN.pdf

Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *Social and Information Networks.* DOI: 10.5210/fm.v22i8.8005

Ferrara, E. (2020). *Covid-19 on Twitter: Bots, conspiracies, and social media activism*. Retrieved from https://arxiv.org/vc/arxiv/papers/2004/2004.09531v1.pdf (accessed on 10 July 2021).

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM, 59 (7): 96-104.* DOI: 10.1145/2818717

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing*, 10 (1): 149-166. DOI: 10.1177/074391569101000111

Gretter, S. & Yadav, A. (2018). What do preservice teachers think about teaching media literacy?: An exploratory study using the theory of planned behavior. *The journal of media literacy education*, 10(1): 104-123. DOI: 10.23860/JMLE-2018-10-1-6

Hajli, N., Saeed, U., Tajvidi, M., & Shirazi, F. (2021). Social Bots and the Spread of Disinformation in Social Media: The Challenges of Artificial Intelligence. *British Journal of Management.* DOI: 10.1111/1467-8551.12554

Hill, J., Ford, W., & Farreras, I. (2015). Real conversations with artificial intelligence:

A comparison between human–human online conversations and human–chatbot conversations. *Computers in Human Behavior*, 245-250. DOI: 10.1016/j.chb.2015.02.026

Hameleers, M., Powell, T., Meer, T., & Bos, L. (2020). A picture paints a thousand lies? The effects and mechanisms of multimodal disinformation and rebuttals disseminated via social media. *Political Communication*, 37(2): 281-301. DOI: 10.1080/10584609.2019.1674979

Howard, P., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics, 15 (2): 81-93*. DOI: 10.1080/19331681.2018.1448735

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55.

Hwang, Y., Ryu, J., & Jeong, S. (2021). Effects of disinformation using deepfake: The protective effect of media literacy education. *Cyberpsychology, Behavior, and Social Networking, 24(3): 188-193*. DOI: 10.1089/cyber.2020.0174

IXresearch. (July 15, 2020). *Social services and Taiwan's two major social media management and use status quo*. *Ixresearch Bi-weekly*, 158. Retrieved from https://www.ixresearch.com/reports/%E5%89%B5%E5%B8%82%E9%9A%9B%E9%9B%99%E9%80%B1%E5%88%8A%E7%AC%AC%E4%B8%80%E4%BA%94%E5%85%AB%E6%9C%9F-20200715

Ireton, C., & Posetti, J. (2018). *Journalism, 'fake news,' and disinformation*. Paris, France: UNESCO.

Jackson, D. (October, 2017). Issue brief: Distinguishing disinformation from propaganda, misinformation, and "fake news". *National Endowment for Democracy.* Retrieved from https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/

Kerr, I. & Bornfreund, M. (2005). Buddy bots: How turing's fast friends are undermining consumer privacy. *Presence: Teleoperators and Virtual Environment, 14(6): 647-655.* DOI: 10.1162/105474605775196544

Kim, H. & Kim, Y. (2021). Protective behaviors against particulate air pollution: Self-construal, risk perception, and direct experience in the theory of planned behavior. *Environmental Communication*, 15(8): 1092-1108. DOI: 10.1080/17524032.2021.1944891

Lewandowsky, S., Ecker, U., Seifert, C., Schwarz, N., & Cook J. (2012). Misinformation and its correction: Continued influence and successful

debiasing. *Psychological Science in the Public Interest, 13(3): 106-131*. DOI: 10.1177/1529100612451018

Li, X., Smith, J., Pan, T., Dinh, T., & Thai, M. (2020). Quantifying privacy vulnerability to socialbot attacks: An adaptive non-submodular model. *IEEE Transactions on Emerging Topics in Computing, 8(3): 855-868*. DOI: 10.1109/TETC.2018.2840433.

Lin, T., Li, S., & Bautista, J. (2022). *Examining socialbot use, disinformation interaction and risk attitude in the extended parallel process model* [Paper presentatio]. Hybrid 72nd Annual International Communication Association, International Communication Association, Paris, France

Lin, T. T., & Bautista, J. R. (2017). Understanding the relationships between mHealth apps' characteristics, trialability, and mHealth literacy. *Journal of health communication*, 22(4), 346-354.

Lin, T. T. C. (2021). *Socialbot representations on cross-media platforms during 2020 Taiwanese Presidential Election: A big data research*. Paper presented at 2021 International Telecommunication Society Biennial Conference.

Luceri, L., Deb, A., Badawy, A., & Ferrara, E. (2019). Red bots do it better: Comparative analysis of social bot partisan behavior. *WWW '19: Companion Proceedings of the 2019 World Wide Web Conference,* 1007-1012. DOI: 10.1145/3308560.3316735

McKay, S. & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly, 74 (3): 703-717*. DOI: 10.1177/1065912920938143

Mitter, S., Wagner, C. & Strohmaier, M. (2013). Understanding the impact of socialbot attacks in online social networks. Social and Information Networks. Retrieved from https://arxiv.org/abs/1402.6289

Nowak, G & Phelps, J. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing,* 6(4): 28-39. DOI: 10.1002/dir.4000060407

Nemr, C., & Gangware, W. (2019). Weapons of mass distraction: Foreign state-sponsored disinformation in the digital age. *Park Advisors*. Available at https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf

Petratos, P. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons, 64(6): 763-774.* DOI: 10.1016/j.bushor.2021.07.012

Prabawanti, C., Dijkstra, A., Riono, P., & Hartana G. (2015). A survey on HIV-related health-seeking behaviors among transgender individuals in Jakarta, based on

the theory of planned behavior. *BMC Public Health*, 15, 1138. DOI: 10.1186/s12889-015-2480-0

Pundir, V., Devi, E., & Nath, V. (2021). Arresting fake news sharing on social media: a theory of planned behavior approach. *Management Research Review, 44(8): 1108-1138*. DOI: 10.1108/MRR-05-2020-0286

Rabello, E.T., Matta, G., Silva, T. (2020). Visualising Engagement on Zika Epidemic. In *Proceedings of the SMART Data Sprint: Interpreters of Platform Data*, Lisboa, Portugal. Retrieved from https://smart.inovamedialab.org/smart-2018/project-reports/visualising-engagement-on-zika-epidemic (accessed on 10 July 2021)

Reuter, C., Hartwig, K., Kirchner, J., & Schlegel, N. (2019). Fake news perception in Germany: A representative study of people's attitudes and approaches to counteract disinformation. *Wirtschaftsinformatik*. Retrieved from https://aisel.aisnet.org/wi2019/track09/papers/5/

Schmuck, D. & von Sikorski, S. (2020). Perceived threats from social bots: The media's role in supporting literacy. *Computers in Human Behavior, 113: 106507*. DOI: 10.1016/j.chb.2020.106507

Sheehan, K. & Hoy, M. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19 (1): 62-73. DOI:10.1509/jppm.19.1.62.16949

Shi, W., Liu, D., Yang, J., Zhang, J., Wen, S., & Su, J. (2020). Social bots' sentiment engagement in health emergencies: a topic-based analysis of the covid-19 pandemic discussions on Twitter. *International Journal of Environmental Research and Public Health*, 17 (22): 8701. DOI: 10.3390/ijerph17228701

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T., Ding, K., Karami, M., & Liu H. (2020a). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews, Data Mining and Knowledge Discovery, 10 (6).* DOI: 10.1002/widm.1385

Shu, K., Wang, S., Lee, D., & Liu, H. (2020b). Mining Disinformation and fake news: Concepts, methods, and recent advancements. *Disinformation, Misinformation, and Fake News in Social Media*. DOI: 10.1007/978-3-030-42699-6_1

Taneja, A., Vitrano, J., & Gengo, N. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation. *Computers in Human Behavior,* 38: 159-173. DOI: 10.1016/j.chb.2014.05.027

Terry, D. J., & O'Leary, J. E. (1995). The theory of planned behaviour: The effects of perceived behavioural control and self-efficacy. *British Journal of Social*

Psychology, 34(2), 199–220. https://doi.org/10.1111/j.2044-8309.1995.tb01058.x.

Tsai, W., Liu, Y., & Chuan, C. (2021). How chatbots' social presence communication enhances consumer engagement: The mediating role of parasocial interaction and dialogue. *Journal of Research in Interactive Marketing,* 15 (3): 460-482. DOI: 10.1108/JRIM-12-2019-0200

Wei, R., Xiaoming, H., & Pan, J. (2010). Examining user behavioral response to SMS ads: Implications for the evolution of the mobile phone as a bona-fide medium. *Telematics and Informatics,* 27 (1): 32-41. DOI: 10.1016/j.tele.2009.03.005

Westland, J. C. (2010). Lower bounds on sample size in structural equation modeling. *Electronic commerce research and applications*, *9*(6), 476-487.

Wiesenberg, M. & Tench, R. (2020). Deep strategic mediatization: Organizational leaders' knowledge and usage of social bots in an era of disinformation. *International Journal of Information Management, 51: 102042.* DOI: 10.1016/j.ijinfomgt.2019.102042

Woolley, S. & Howard, P. (2016). Political communication, computational propaganda, and autonomous agents. *Introduction. International Journal of Communication,* 10: 4882-4890.

Xiao, G. (2021). Bad bots: Regulating the scraping of public personal information. *Harvard Journal of Law & Technology, 34 (2): 701.*

Yan, H., Yang, K., Menczer, F., & Shanahan, J. (2021). Asymmetrical perceptions of partisan political bots. *New Media & Society, 23 (10): 3016-3037*. DOI: 10.1177/1461444820942744

Zellers, R., Holtzman, A., Rashkin, H., Bisk, Y., Farhadi, A., Roesner, F., & Choi, Y. (2019). Defending against neural fake news. *Computation and Language.* DOI: 10.48550/arXiv.1905.12616

Zhang, X., Liu, S., Wang, L., Zhang, Y., & Wang, J. (2020). Mobile health service adoption in china: Integration of theory of planned behavior, protection motivation theory and personal health differences. *Online Information Review,* 44 (1):1-23. DOI: 10.1108/OIR-11-2016-0339

Zhao, L., Yin, J., & Song, Y. (2016). An exploration of rumor combating behavior on social media in the context of social crises. *Computers in Human Behavior, 58: 25-36.* DOI: 10.1016/j.chb.2015.11.054

Appendix 1. List of items

Item	Factor Loading
Attitude with socialbot	
I have followed the debate about socialbots.	Dropped
Socialbots offer opportunities for strategic communication.	Dropped
Socialbots present ethical challenges for communication professionals.	0.572
Socialbots are a threat for organizations and their reputation.	0.770
Socialbotsare a threat for societies and public debates.	0.775
Privacy concern	
I am concerned that the information I submit to socialbots can be misused	0.826
I am concerned about submitting personal information to socialbots because it can be used in a way I do not foresee	0.872
I am concerned about submitting personal information to socialbots because others might use it for political or propaganda purposes	0.857
If I used socialbots, I would be concerned that my personal data and information can be stolen during interactions	0.800
Perceived Bot control	
Whether or not I am influenced by disguised socialbots on social media platforms is up to me	Dropped
I have a high level of personal control over whether or not disguised socialbots' false messages affect me	Dropped
Personally, I cannot control whether disguised socialbots on social media platforms affect my opinion	0.758
I am confident that I myself can prevent disguised socialbots from manipulating my opinion	0.710

I will recognize most disguised socialbots if I encounter them in the future	0.853
I can succeed at telling disguised socialbots apart	0.876
When facing disguised socialbots that highly resemble regular users, I can still find clues to weed them out.	0.810
Disinformation threat	
Disinformation poses a threat.	0.622
Socialbots pose a threat to disinformation.	0.522
It's the state's task to prevent disinformation.	0.534
It's the task of platform operators (e.g., Facebook, Line) to prevent disinformation.	0.566
Disinformation harms the democracy.	0.657
Disinformation can manipulate the opinion of politicians, journalists and other influential players.	0.685
Disinformation can manipulate the population's opinions.	0.680
Disinformation is just a pretext to be able to fight system-critical actors.	Dropped
The state censorship poses a threat to freedom of speech.	Dropped
Disinformation is at most annoying but does not pose a threat.	0.525
Interaction with disinformation	
I have perceived disinformation	0.82
I have "liked/disliked" disinformation	0.85
I have commented on disinformation	0.84
I have shared disinformation	0.85
I have deleted/reported disinformation	0.84
I have disliked disinformation	0.84