5

Cyber Disinformation Risk Perception and Control

Integration of the Extended Theory of Planned Behavior and a Structural Equation Model

Małgorzata Pańkowska and Ioana Vasiu

The extensive use of digital platforms and services has expanded widely the range of potential attacks and targets, rendering individuals and the democratic values and institutions vulnerable to a substantial number of cyber-enabled threats. These threats can be sophisticated, conducted on a large scale, and capable of producing significant, viral consequences. Among these threats, cyber disinformation is regarded as a major threat. The phenomenon is widespread and complex, in certain cases, part of hybrid warfare, involving various cyberattacks by nefarious actors, which deceptively distribute fake or incomplete materials, with a view to influencing people's opinions or behavior.

Disinformation can involve numerous vectors and take several forms. The goal of disinformation campaigns is to promote or sustain certain economic or political interests, discrimination, phobia, hate speech, or harass individuals (European Parliament, 2022). Instances of alleged disinformation can be encountered with respect to a large variety of aspects, such as food (Diekman, Ryan, & Oliver, 2023); migrants (Culloty et al., 2022); fossil fuel;[1] sexual preferences (Carratalá, 2023); health hazards;[2] politics;[3] and so on.

Successful disinformation campaigns can negatively affect fundamental freedoms, undermine trust, subvert attention, change attitudes, sow confusion, exacerbate divides, or interfere with decision-making processes. Consequently, such campaigns can rightly be considered attacks on knowledge integrity (Pérez-Escolar, Lilleker, & Tapia-Frade, 2023, p. 77). The potential consequences can be disquieting, negatively affecting democratic values and institutions (Jungherr & Schroeder, 2021; Schünemann, 2022). The concerns over cyber disinformation are notable worldwide and received significant attention from researchers (Buchanan & Benson, 2019; Nenadić, 2019; Olan et al., 2022; Pierri, Artoni, & Ceri, 2020; Tenove

[1] *District of Columbia v. Exxon Mobil Corp.*, Civil Action No. 20-1932 (TJK) (D.C. 2022).
[2] *RJ Reynolds Tobacco Co. v. Rouse*, 307 So.3d 89 (Fla. Dist. Ct. App. 2020).
[3] *Nat'l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d 457 (S.D.N.Y. 2020).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

& Tworek, 2019; Ternovski, Kalla, & Aronow, 2022; Vaccari & Chadwick, 2020; Weikmann & Lecheler, 2022).

While there are laws that address the phenomenon (e.g., 18 U.S. Code § 35, the German Network Enforcement Act, the French Law on the fight against the manipulation of information), strengthened codes of practice (e.g., the European Commission's Strengthened Code of Practice on Disinformation 2022), assignment of anti-disinformation attributions to governmental agencies (e.g., the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency), awareness campaigns, and implementation of disinformation detection and blocking algorithms or filters, the control of the phenomenon still poses significant challenges.

The control of the cyber disinformation phenomenon plays a significant role in the protection of democratic values and systems. This chapter argues that an essential role in the control of the phenomenon is played by the individual behavior of users and aims to identify factors that impact on Behavioral Intentions (BIs) and Cyber Hygiene Behavior (CHB), in the circumstances of cyber disinformation. The chapter integrates the Extended Theory of Planned Behavior (ETPB) and a Structural Equation Model. The research data were collected using a questionnaire. The model's parameters were processed using the SmartPLS software.

The rest of this chapter is organized as follows. The next section outlines the phenomenon's main attributes and explains how cyber-enabled means can threaten democratic values and institutions. The third section discusses aspects regarding structural equation modeling (SEM), applied to disinformation. The fourth section presents the conceptual model and the proposed hypotheses. Finally, the fifth section presents the model evaluation. The chapter concludes with implications of findings.

CYBER DISINFORMATION ATTRIBUTES

"Disinformation" is a term difficult to define because the phenomenon is complex (Ó Fathaigh, Helberger, & Appelman, 2021) and covers many forms, such as "fabrications, fakeness, falsity, lies, deception, misinformation, disinformation, propaganda, conspiracy theory, satire or just anything with which one disagrees" (Andersen & Søe, 2020, p. 6). Wardle and Derakhshan (2017), for instance, contrast "disinformation," referred to as intentionally false or deceptive communication, with "misinformation," understood as communications that may contain false claims, however, not intended to cause or inflict harm. The European Commission (2020, p. 18) clearly distinguishes between misinformation, information influence operation, foreign interference in the information space, and disinformation, defining the latter as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm."

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

Disinformation can be orchestrated by individuals or by organized groups (state or non-state) and involve various sources, such as regular citizens, political leaders or officials, attention-seeking trolls, profiteers, or propagandistic media (Watson, 2021). Several factors were identified that favor the phenomenon, such as the tendency to believe unreliable statements (European Parliamentary Research Service, 2020) or people's difficulties in identifying disinformation (Machete & Turpin, 2020), the identity confirming problems, and deficiencies in platform filtering (Krafft & Donovan, 2020).

According to Bontcheva et al. (2020, pp. 22–23), disinformation can take various formats, such as false claims or textual narratives; altered, fake, or decontextualized audio and/or video; and fake websites and manipulated datasets. Cyber disinformation campaigns can involve, for example, deceptive advertising, propaganda, or the dissemination of forged materials, such as videos, photographs, audios, documents (including, for instance, fake web pages or maps), created through image altering or airbrushing or cover-up, or by audio camouflage.

One of the characteristics of disinformation campaigns regards the existence of deceptive goals. According to Fallis (2014, pp. 142–146), the deceptive goals can be classified as regarding the accuracy of the content, the source believing the content, the content source identity, and the content accuracy implication. Disinformation can cause significant harm, as it has the real potential to confuse or manipulate people, suppress the truth or critical voices, generate distrust in democratic institutions or norms, and even disrupt democratic processes (Bontcheva et al., 2020).

Social media is often regarded as a highly effective vector to promote political goals via disinformation campaigns (Aïmeur, Amri, & Brassard, 2023). Twitter, now called "X," for example, was used to spread misleading election memes and graphics, designed to demoralize opponent's voters, and even deter them from exercising their right to vote, which went viral.[4] For an illustration of the importance attached to X as a disinformation vector, according to Statista research, the number of disinformation and pro-Russian posts in Poland via X amounted, in January 2022, to 25,910 disinformation and pro-Russian posts on X, increasing to 358,945 during the year (Statista, 2023).

In practice, disinformation campaigns employ an impressive array of tactics, including the impersonation of organizations or real people; creation of fake or misleading online personas or websites; creation of deepfakes or synthetic media; devise or amplification of certain theories; astroturfing and flooding; exploitation of gaps in information; manipulation of unsuspecting people; and spread of targeted content (Cybersecurity and Infrastructure Security Agency, 2022). Of particular concern, given their massive disinformation potential, are the deepfakes. In video and/or audio form, deepfakes nowadays are very realistic, allowing morphing attacks and the creation of unreal faces or voices, allowing personalized messages to

[4] *United States v. Mackey*, No. 21-CR-80 (AMD)(SB) (E.D.N.Y. Oct. 17, 2023).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

individuals. Deepfakes can negatively affect the credibility of individuals, disrupt markets, facilitate frauds, manipulate public opinions, incite people to various forms of violence, and support extremist narratives, social unrest, or political polarization (Mattioli et al., 2023; Trend Micro, 2020). Moreover, deepfakes undermine conversations about reality and can disrupt democratic politics (Chesney & Citron, 2019).

Personalization algorithms can be employed to facilitate the spreading of disinformation, potentially making it thrive on digital platforms (Borges & Gambarato, 2019). The techniques or means employed in disinformation campaigns may also include, for instance, bots. These are increasingly difficult to distinguish from humans and can be effectively used to produce disinformation content, targeted at predetermined or general users (Edwards et al., 2016). For instance, bots are used to disseminate election disinformation (Knight Foundation, 2018) or disinformation regarding health issues (Benson, 2020).

Artificial neural network (ANN) and deep learning methods can be used in disinformation campaigns, with unlawful or nefarious potential (Rana et al., 2022). Amplifiers, such as influential people or artificial intelligence tools, via, for instance, cross-platform coordination or the manipulation of engagement metrics, can be used to maximize engagement or the spread of disinformation through networks, to retweet or to follow X accounts or to share Facebook, now called Meta, posts (European Commission, 2023; Michaelis, Jafarian, & Biswas, 2022). Clickbait is another disinformation method used to attract online users to click on disinformation links (Collins et al., 2021).

STRUCTURAL EQUATION MODELING OF DISINFORMATION

The original approach to SEM assumed that the use of technical systems could be explained and predicted by user motivation directly influenced by external factors (i.e., the functionalities and capabilities of those technical systems) (Chuttur, 2009; Davis, 1985). The Technology Acceptance Model (TAM) theory was proposed to explore behavior and user acceptance of Information Communication Technology (ICT) based on the social psychology perspective. The TAM theory assumes that two factors determine users' acceptance of a technology: (1) perceived usefulness and (2) perceived ease of use. The first refers to the user's belief in the degree to which they think that using the technology enhances their job performance, productivity, or overall effectiveness. The second represents the user's perception of how easy it is to apply the technology. In general, the acceptance of technology is a critical element and a necessary condition in the implementation of ICT in everyday life. An extensive literature survey was conducted utilizing the Scopus database, which covers 18,639 papers on TAM, published between 1964 and 2023.

Over decades, several theoretical models have been developed to understand the acceptance and the use of ICT. Researchers have been hesitant in selecting the appropriate theoretical model for the evaluation of the acceptance and usage of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

ICT. Recognition of the ICT needs and the ICT acceptance by individuals in business organizations is usually the beginning stage of any business activity and this understanding can be helpful to find the way of future implementation of the ICT.

In general, TAM models are estimated through the SEM, which is an approach for testing the hypotheses on relations among observable and latent variables (Sabi et al., 2016). The SEM is a statistical method applied in various fields of social sciences to estimate relationships among specified variables and verification of hypotheses if those relations are statistically dependable and valid. In this study, the SEM is realized through the Partial Least Square–Structural Equation Modeling (PLS_SEM), which represents the composite-based SEM method (Hair Jr. et al., 2017). Partial Least Square (PLS) is a statistical method for estimation of relationships between independent variables and dependent variables.

For the past thirty years, the research community has been strongly involved in the identification of the factors that have an impact on technology acceptance. The theory of reasoned action (TRA) and the theory of planned behavior (TPB) were predecessors of the TAM (Marikyan & Papagiannidis, 2021; Park & Park, 2020). The TRA explains and predicts human behaviors considering their attitudes and Subjective Norms (SN). That theory assumes that individuals make rational decisions based on their attitudes and social norms.

The TPB is an extension of the TRA, also provided by Ajzen (2005). The TPB explains and predicts individual behavior based on human intentions, which are dependent on three factors, that is, attitude identified with personal beliefs, SN referring to the social pressure, and Perceived Behavioral Control (PBC) encompassing self-efficacy, perceived obstacles, and facilitators. The TAM had further modifications (i.e., TAM2, TAM3); however, researchers have utilized the Unified Theory of Acceptance and Use of Technology (UTAUT) model, which suggests that the actual use of technology is determined by BI. The perceived BI is dependent on four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. The effect of variables is moderated by age, gender, experience, and voluntariness of use (Venkatesh et al., 2003). Further, researchers have noticed the importance of factors reflecting the costs and benefits of behavior, as well as the context of use.

Venkatesh, Thong, and Xu (2012) proposed the UTAUT2 model, which was developed to examine technology use in organizational settings. The authors of the UTAUT2 argue that the use of technology by individuals is determined by the following constructs: performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit, moderated by age, gender, and experience. In the UTAUT and UTAU2 models, BI has an impact on use behavior.

This study aims to identify factors having an impact on Behavioral Intentions (BIs) and Cyber Hygiene Behavior (CHB) in the circumstances of wide dissemination of disinformation in cyberspace. The BIs comprise an individual's predispositions and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

willingness to behave in a specific way. This concept is included in various human behavior theories to analyze and predict human actions. CHB covers all practices that allow avoiding the risk to be a victim of cyberattacks and reduce cyber vulnerabilities.

This study considered state-of-the-art research work on disinformation attitudes. The Scopus literature survey revealed 4,526 publications on the "disinformation" keyword search. These papers were published between 1974 and 2023. However, there are only nineteen publications on the "disinformation" AND "structural equation modelling," query, all between 2020 and 2023. Certain countries (i.e., China, Russia, and Turkey) have professionalized operations online to support social media campaigns and create an alternative informational space and effectively disseminate persuasive messages through symbols and emotions. Therefore, their action monitoring as well as online trolling are subjects of research (Alieva, Moffitt, & Carley, 2022; Uyheng, Moffitt, & Carley, 2022).

Several researchers examine the phenomenon of disinformation as a threat in the sphere of cybersecurity (Caramancion et al., 2022; Carrapico & Farrand, 2021). Hence, cybersecurity issues have been included as observable variables (i.e., Security (SEC) items) in the proposed survey. Arayankalam and Krishnan (2021) formulated some hypotheses, which were positively verified, concerning disinformation, as follows:

- Disinformation through social media is positively associated with online media development.
- Online media are positively associated with its social media-induced offline violence.
- The government control negatively moderates disinformation.

In social psychology, the TPB is one of the most influential behavioral models. The TPB links beliefs to behavior and assumes that the user's behavior is determined by their intentions to perform that behavior. In the conceptual model proposed by Jia et al. (2022), for example, several factors have an impact on Behavioral Attitudes (BA), Subjective Norm (SN), and Perceived Behavioral Control (PBC). Further, the three variables determine BI. Moreover, Shirahada and Zhang (2022) argue that TPB is used to predict and explain human intentions in a particular context. Intentions are influenced by SN, attitudes, and PBC. SN concern the expectations of other people and social pressures regarding desirable behavior. Attitude refers to evaluations of behavior, and PBC refers to the ease of performing a behavior.

Maheri, Rezapour, and Didarloo (2022) argue that the Perceived Risk (PR) refers to subjective assessments of the risk of disinformation and its potential consequences. SN refer to respondents' beliefs that significant others think they should or should not engage in a particular behavior. PBC concerns participants' perceptions of their ability to do verification.

Romero-Galisteo et al. (2022) consider that TPB explains the degree of correlation between variables, that is, entrepreneurial intention, perceived feasibility, and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

perceived desirability. Beyond that, Savari, Mombeni, and Izadi (2022) develop an Extended Theory of Planned Behavior (ETPB) including the variables, that is, Descriptive Norms (DN), Moral Norms (MN), Habits (HA), and Justification (JU). In their theoretical framework, Attitude, SN, DN, and PBC have impacts on Intention, while PBC, MN, and variables such as HA and JU influence Behavior.

MN define a sense of inherent moral commitment, according to a value system. The concept of DN explains personal attitude about how much other people exhibit a certain behavior. The norms are introduced as people learn not only from their own experiences but also from analyses of behaviors of others. Comparable extension of TPB was provided by Khani Jeihooni et al. (2022), who included attitude, among others, PBC, SN, and BIs in their survey.

According to Ababneh, Ahmed, and Dedousis (2022), the TPB proposes four major predictors of human behavior (i.e., attitude toward the behavior, SN, BI, and PBC). Ajzen (1991, p. 183) argues that attitude, norms, and control determine intentions and behavior. Cabeza-Ramirez et al. (2022) notice that literature has rarely considered the possible perception of risk associated with desirable behavior. Similarly, the risk is included in the TPB model proposed by Zhang et al. (2022). Security is considered in the TPB model developed by Al-Shanfari et al. (2022). Using the SEM method, they revealed factors having an impact on information security behavior adoption and employees' training.

THE CONCEPTUAL MODEL AND HYPOTHESES

Considering the literature survey on latent variables included in the TPB models, this study noticed that there is no standardized approach: The models are formulated according to the preferences of researchers and some extensions are possible. Therefore, this study focuses on the application of the ETPB model; however, additional constructs are added, which are expected to present the context of behavior.

This study defines the BA as the degree to which a person believes that they can properly recognize disinformation. The BA influences the decision on whether to accept or reject the information. The BA reveals the extent to which a person believes that the use of information is needed and not harmful. BA refers to personal predispositions to act in a specific way, regarding a particular object, person, situation, concept, or technology.

Beyond that, this study proposes to include three types of norms, that is, MN, SN, and DN. MN result from personal internal beliefs not to tolerate disinformation. In general, MN are principles or rules that govern human behavior and establishing what is right or wrong in a social community. SN concern a personal perception of social pressure or influence to perform or not perform a particular action. SN result from personal motivation, normative beliefs, individuals' knowledge, and impacts and experiences of third-party people, who may have influence on the questionnaire

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

recipient. DN concern the perceptions that individuals have about behaviors exhibited by others in a community.

In this study, DN reveal the degree to which the recipient creates themselves as the image of a person who knows how to avoid disinformation. PBC means personal beliefs that an individual has capabilities, that is, competencies and resources, to control factors that may influence their behavior. In this study, PBC refers to the degree to which the recipient believes in their abilities to self-control and avoid disinformation. Therefore, this study proposes the following hypotheses:

H1: Behavioral Attitude (BA) has an impact on Behavioral Intention (BI).

H2: Moral Norms (MN) have a positive impact on Behavioral Intention (BI).

H3: Subjective Norms (SN) have a positive impact on Behavioral Intention (BI).

H4: Descriptive Norms (DN) have a positive impact on Behavioral Intention (BI).

H5: Perceived Behavioral Control (PBC) has a positive impact on Behavioral Intention (BI).

H6: Perceived Behavioral Control (PBC) has a positive impact on Cyber Hygiene Behavior (CHB).

H7: Behavioral Intention (BI) has a positive impact on Cyber Hygiene Behavior (CHB).

Beyond variables considered in the TPB model, this study added other variables. Two of them, that is, HA and JU, have been introduced to the ETPB model by Savari, Mombeni, and Izadi (2022). HA are repetitive actions, which are performed regularly or automatically in human lives. They can be positive (i.e., good habits, e.g., teeth cleaning) and negative (i.e., unhealthy habits, e.g., avoiding physical activities). In this paper, HA includes individual practices and routines applied by the recipients, particularly avoiding internet news. JU refers to collecting and revealing the reasons for a particular action, decision, or belief. JU means a personal explanation of regulations, policies, and administrative practices to avoid disinformation.

This study also considered the impact of variables combined with security, Anxiety (AN), and risk. Hence, the conceptual model covers the impact of three additional factors that may influence CHB, which covers practices and habits to maintain an elevated level of cybersecurity and protection of digital assets. It may also include prevention to maintain mental health and avoiding unreliable and untested, unchecked, and malicious information. Cyber AN is a degree to which a person hesitates to use internet information because of its harmfulness. PR is defined as a degree of risk recognition by an individual. SEC means level of knowledge on Information Technology (IT) tools to protect in case of a human agent or software attack. Hence, the next hypotheses are as follows:

H8: Justification (JU) has an impact on Cyber Hygiene Behavior (CHB).

H9: Habits (HA) have an impact on Cyber Hygiene Behavior (CHB).

H10: Perceived Risks (PRs) have an impact on Cyber Hygiene Behavior (CHB).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

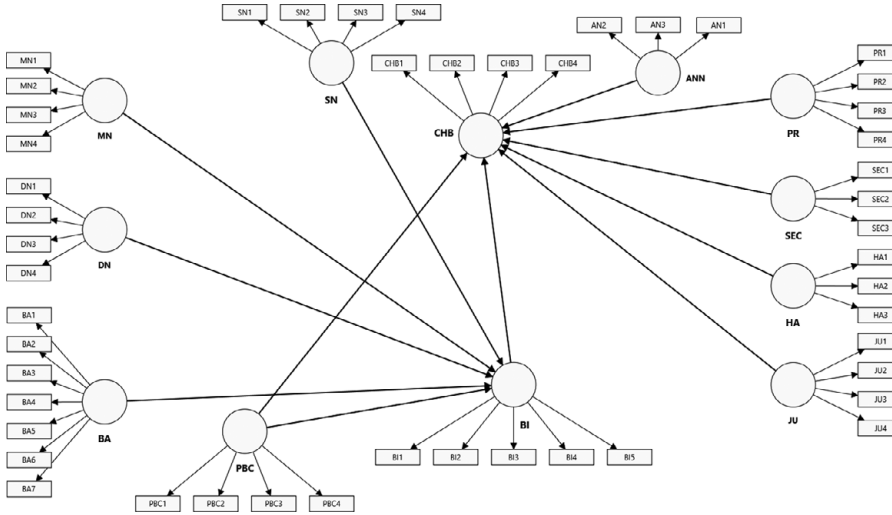


FIGURE 5.1 Conceptual model.

H11: Security (SEC) has an impact on Cyber Hygiene Behavior (CHB).

H12: Anxiety (AN) has an impact on Cyber Hygiene Behavior (CHB).

Figure 5.1 includes the conceptual model of variables having an impact on CHB. In this theoretical framework, relationships among constructs, that is, latent variables, as well as between constructs and their assigned indicators, that is, items or observable variables, are shown with arrows.

OBSERVABLE INDICATORS FOR CYBER HYGIENE BEHAVIOR MODEL

For the past thirty years, ICT, in general, and the internet have played a significant role in communications among people in all sectors of life (i.e., education, administration, business, health care, and agriculture). The benefits of ICT do overcome risks and wastes caused by disinformation. To evaluate young peoples' behavior and recognize factors having an impact on their BIs and actions, the TPB model has been specified and estimated. The literature survey on TAM, UTAUT, and the TPB models led to observations that researchers focus on the latent variable's identification. However, the specification of observable items, such as indicators, should also be discussed.

Considering the items identified in literature and proposed by other researchers, this study items are included in Table 5.1.

The research data were collected using a questionnaire and analyzed using SEM. The survey respondents were students at the University of Economics in Katowice (Poland) and the Babeş-Bolyai University (Romania). The questionnaires were

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.1 *Items included in the survey*

Latent variables		Items	Mean RO	Mean PL
Anxiety (AN)	**AN1**	I feel apprehensive about finding fake news on the internet	4.115	3.245
	AN2	I hesitate to use social media for fear of finding fake news	2.285	1.685
	AN3	Fake news are threats to democratic values and democratic institutions	5.394	4.925
Perceived Risk (PR)	**PR1**	Buying products promoted by an unreliable source adds to the uncertainty about the results	5.782	5.780
	PR2	Disinformation destroys a positive image and reputation	5.842	5.890
	PR3	I accept the risk to enable learning from uncertain sources	3.194	5.080
	PR4	I think there is no risk in using social media to meet new people	2.291	2.900
Security (SEC)	**SEC1**	Anti-spamming software allows me to avoid fake news	3.982	4.070
	SEC2	Internet service provider warns me about fake news	2.327	3.500
	SEC3	I pay consideration to website artifacts, i.e., Padlock/https	4.024	4.755
Moral Norms (MN)	**MN1**	Avoiding fake news dissemination is a matter of conscience for me	5.600	4.040
	MN2	I feel compelled by my conscience to punish fake news providers	4.279	5.040
	MN3	I feel uncomfortable when I observe that other people tolerate fake news dissemination	5.497	4.660
	MN4	I feel responsible for the true information inserted by me on the internet	6.115	5.110
Behavioral Attitude (BA)	**BA1**	I like to be engaged in the activity for fake news recognition	4.121	2.830
	BA2	I believe that constant monitoring of COVID-19 news has a positive impact on my mental health	2.521	3.410
	BA3	I have enough responsibility not to read fake news	5.370	4.995
	BA4	I think it is better to verify the information provenance	6.467	5.825
	BA5	I think that unreliable sources of data may provide fake news	5.697	4.660
	BA6	I think that losers and crazy people provide fake news on the internet	3.618	3.940
	BA7	I think fake news is like a joke	2.455	3.685

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

Latent variables		Items	Mean RO	Mean PL
Subjective Norms (SN)	**SN1**	Some of my colleagues have been deceived by fake news	5.091	4.620
	SN2	Public opinion will affect my choice of the internet news	3.303	4.300
	SN3	People whom I work with help each other to recognize fake news	4.327	4.360
	SN4	People whom I trust warn me and explain to me the fake news	5.164	4.930
Descriptive Norms (DN)	**DN1**	I think most of my friends know how to avoid fake news	4.709	4.875
	DN2	I am sure that people around me do not read unreliable news	3.273	3.895
	DN3	I believe that most of my family thinks that reading unreliable news is unreasonable and wrong	4.685	5.040
	DN4	Reading fake news is disgusting to the people around me	4.006	4.120
Perceived Behavioral Control (PBC)	**PBC1**	My technical ability is sufficient to avoid disinformation	5.079	5.270
	PBC2	I purposefully avoid nonverified information	5.364	5.005
	PBC3	I know how to avoid fake news	5.267	5.335
	PBC4	I think I have good self-control	5.818	5.175
Behavioral Intention (BI)	**BI1**	I would like to know more about the possibilities of verifying internet information	6.236	4.945
	BI2	I will recommend my friends/relatives to verify information from uncertain/ unknown sources	6.073	4.890
	BI3	Post COVID-19, I carefully check information on it	5.442	4.435
	BI4	I will take good care of myself, particularly when I am browsing unsafe portals	5.933	5.525
	BI5	I am still looking for news that allows me to verify the information received earlier	5.418	4.655
Habits (HA)	**HA1**	I do not think about the fake news on the internet because I do not read internet news	2.539	3.450
	HA2	I habitually always pay attention to reliability of news and always check the source of information	5.273	4.910
	HA3	I always read reliable information on the internet because it has become a habit for me	4.836	4.570

(*continued*)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.1 (*continued*)

Latent variables		Items	Mean RO	Mean PL
Justification (JU)	**JU1**	Due to the fake news dissemination, people do not trust each other and the internet is not reliable source of information	4.685	4.855
	JU2	Governmental activities to punish and reduce fake news are small and hard to notice	5.685	5.050
	JU3	The habit of reducing fake news on the internet is usually forgotten when people need to receive important information, e.g., on COVID-19 risks	5.333	4.550
	JU4	Increasing the punishment for fake news is often overlooked because there is so much everyday news and people do not remember nor recognize what is false or true	5.497	4.985
Cyber Hygiene Behavior (CHB)	**CHB1**	I avoid constantly studying the news on gossip portals	5.358	5.135
	CHB2	I will not encourage others to study the gossip portal news	5.430	5.545
	CHB3	I immediately remove emails from unknown senders	4.873	4.610
	CHB4	I do not click on links or attachments from unsolicited emails or texts	6.515	5.970

distributed to bachelor, master, and doctoral-level students. The responses to the questionnaire were voluntary and anonymized. This research collected 200 questionnaires from the University of Economics in Katowice and 165 questionnaires from the Babeş-Bolyai University.

The students were asked to express their degree of agreement or disagreement with the statements in Table 5.1 by marking the answers on the seven-grade Likert scale, considering the following meanings: 1 – absolutely disagree; 2 – disagree; 3 – rather disagree; 4 – irrelevant; 5 – rather agree; 6 – agree; and 7 – definitely agree.

Table 5.1 contains the items included in the survey and presents a list of questions with acronyms and a set of latent variables. The last column in Table 5.1 includes average (Mean) values of these research indicators. The Pearson correlation rate for the two last columns in Table 5.1 is 0.7854; hence, authors conclude on high comparability of responses of recipients from these two populations under research.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.2 *Construct reliability and validity – preliminary model estimated (sample size: 200 records from Poland)*

Construct	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
AN	0.454	0.553	0.696	0.447
BA	0.373	0.485	0.618	0.234
BI	0.678	0.704	0.795	0.442
CHB	0.609	0.617	0.775	0.468
DN	0.592	0.543	0.673	0.389
HA	0.272	0.521	0.508	0.404
JU	0.647	0.678	0.779	0.473
MN	0.599	0.697	0.752	0.443
PBC	0.685	0.70	0.806	0.512
PR	−0.115	0.267	0.005	0.321
SEC	0.325	0.226	0.533	0.356
SN	0.410	0.717	0.638	0.377

THE TPB MODEL EVALUATION

The presented conceptual model (see Figure 5.1) consists just of items connected to the variables. SmartPLS3 was used to calculate the model (Ringle, Hair, & Sarstedt, 2014). In the first run, the model was calculated with the PLS algorithm. The number of iterations was set to 1,000 and the stop criterion to 10^{-X} with selected 7. Then the model was calculated with the Bootstrap algorithm, in which the number of samples was set to 5,000 for the full version with bias-corrected and accelerated in two-tailed distribution. The significant level was equal to 0.05.

The conceptual model (Figure 5.1) was estimated twice. Firstly, data were gathered in Poland, then in Romania. The reliability of the variables was evaluated using Cronbach's Alpha and Composite Reliability (CR). The results for reliability and validity are presented for the overall sample. Cronbach's Alpha is a way of assessing reliability by comparing the amount of shared variance, or covariance, among the items in a psychological test or questionnaire (Collins, 2007). CR is an "indicator of the shared variance among the observed variables used as an indicator of a latent construct" (Fornell & Larcker, 1981). In psychology, all of Cronbach's Alpha and CR values are recommended to be higher than 0.600. Cronbach's Alpha values of 0.60 to 0.70 are acceptable in exploratory research, while values between 0.70 and 0.90 are regarded as satisfactory (Nunally & Bernstein, 1994). The Average Variance Extracted (AVE) and CR values are to be higher or close to 0.500 and 0.700, respectively, which corroborates convergent validity. Fornell and Larcker (1981) said that if AVE is less than 0.5, but CR is higher than 0.6, the validity of the construct is still adequate. The results for reliability and validity for the overall sample of 200 records from Poland are included in Tables 5.2 and 5.3. Unfortunately, in the first estimation, the chosen observed variables have not

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.3 *Construct reliability and validity – secondary model estimated (sample size: 200 records from Poland)*

Construct	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
BI	0.678	0.703	0.795	0.442
CHB	0.609	0.626	0.774	0.467
DN	0.592	0.540	0.665	0.386
JU	0.647	0.677	0.779	0.473
MN	0.599	0.695	0.751	0.443
PBC	0.685	0.701	0.806	0.512

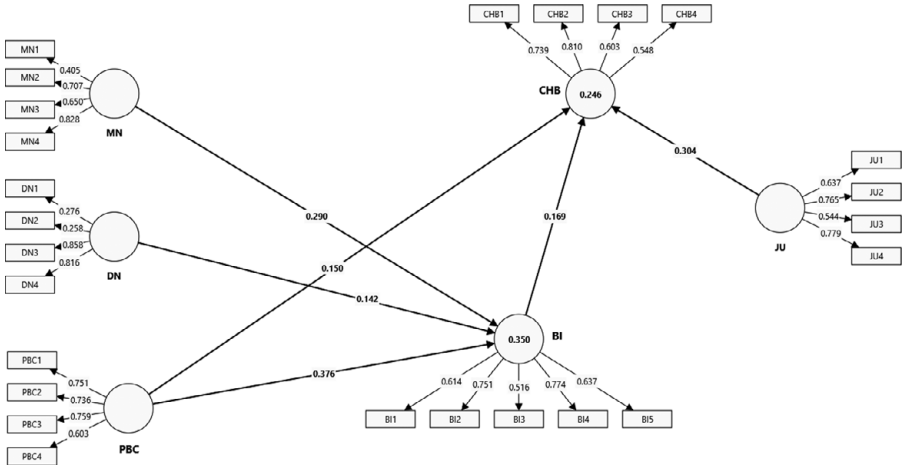


FIGURE 5.2 The final model with estimated coefficients (sample size: 200 records from Poland).

explained well the latent variables; therefore, model fitting was necessary. The preliminary conceptual model as unreliable has been changed, and Figure 5.2 includes the secondary estimated model covering the following hypotheses:

H1: Behavioral Intention (BI) has a positive impact on Cyber Hygiene Behavior (CHB).

H2: Descriptive Norms (DN) have a positive impact on Behavioral Intention (BI).

H3: Justification (JU) has an impact on Cyber Hygiene Behavior (CHB).

H4: Moral Norms (MN) have a positive impact on Behavioral Intention (BI).

H5: Perceived Behavioral Control has a positive impact on Behavioral Intention (BI).

H6: Perceived Behavioral Control has a positive impact on Cyber Hygiene Behavior (CHB).

Path coefficients and R^2 constructs are included in Table 5.4.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.4 *PLS Algorithm R^2 and Path Coefficients (sample size: 200 records from Poland)*

	R^2	BI	CHB	DN	JU	MN	PBC
BI	0.350		0.169				
CHB	0.246						
DN		0.142					
JU			0.304				
MN		0.290					
PBC		0.376	0.150				

TABLE 5.5 *Bootstrapping Path Coefficients for final model (sample size: 200 records from Poland)*

Hypothesis No	Hypothesis (impact direction à)	Original sample	Sample mean	Standard deviation	T-statistics	*P* values	Decision
H1	BI à CHB	0.169	0.174	0.078	2.175	0.030	Accepted
H2	DN à BI	0.142	0.156	0.085	1.673	0.094	Rejected
H3	JU à CHB	0.304	0.316	0.068	4.453	0.000	Accepted
H4	MN à BI	0.290	0.293	0.065	4.476	0.000	Accepted
H5	PBC à BI	0.376	0.378	0.063	6.019	0.000	Accepted
H6	PBC à CHB	0.150	0.150	0.075	1.994	0.046	Accepted

The goodness of the model is estimated by the strength of each structural path, determined by the R^2 value for the dependent variables (Jankelová, Joniaková, & Skorková, 2021). Generally, R^2 is a statistical measure of the goodness of the fit of a regression model. For the dependent variables, the R^2 value should be equal to or over 0.125 (Falk & Miller, 1992). The results in Table 5.4 show that all R^2 values are over 0.1.

The R^2 ranges from 0 to 1, higher values indicating stronger explanatory power. As a general guideline, R^2 values of 0.75, 0.50, and 0.25 can be considered substantial, moderate, and weak, respectively, in many social science disciplines (Hair Jr. et al., 2021). But acceptable R^2 values are based on the research context, and in some disciplines, an R^2 value as low as 0.10 is considered satisfactory, that is, for the large sample size research, it is statistically significant, but substantively meaningless (Falk & Miller, 1992).

Table 5.5 covers the Bootstrapping Path Coefficients values for the final model as well as the decisions on the proposed hypotheses' acceptance or rejection.

The results of the tests indicate that the proposed constructs (i.e., JU, MN, PBC) have a weak impact on the intention and behavior of students (expressed as BI, CHB) to avoid the disinformation. If a *P* value is below a certain threshold, then the corresponding hypothesis is assumed to be supported. The threshold is

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.6 *Construct reliability and validity – preliminary model estimated (sample size: 165 records from Romania)*

Construct	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
AN	0.453	0.461	0.733	0.480
BA	0.294	0.553	0.416	0.244
BI	0.707	0.721	0.808	0.459
CHB	0.487	0.505	0.703	0.381
DN	0.612	0.624	0.774	0.463
HA	0.045	0.711	0.508	0.593
JU	0.640	0.642	0.786	0.480
MN	0.705	0.726	0.819	0.535
PBC	0.674	1.104	0.711	0.400
PR	0.019	0.383	0.091	0.304
SEC	0.459	−0.254	0.177	0.309
SN	0.470	0.537	0.674	0.391

usually 0.05 (Kock, 2014). Therefore, in this research, hypotheses H1, H3, H4, H5, and H6 are supported, but hypothesis H2 is rejected. This means that: (1) Behavioral Intention (BI) impacts on Cyber Hygiene Behavior (CHB); (2) Justification (JU) has a positive impact on Cyber Hygiene Behavior; (3) Moral Norms (MN) have a weak impact on Behavioral Intention (BI); (4) Perceived Behavioral Control (PBC) has a positive impact on Behavioral Intention (BI); and (5) Personal Behavioral Control (PBC) has an impact on Cyber Hygiene Behavior (CHB).

Next, the study estimated the conceptual model considering data from Romania. However, for these data also, the reliability and validity measures have low values (Table 5.6), and authors eliminated some variables from that model.

Since the chosen observed variables have not explained well the latent variables, model fitting was necessary. The preliminary conceptual model as unreliable has been changed, and Figure 5.3 includes the secondary estimated model covering the following hypotheses:

H1: Behavioral Intention (BI) has a positive impact on Cyber Hygiene Behavior (CHB).

H2: Descriptive Norms (DN) have a positive impact on Behavioral Intention (BI).

H3: Justification (JU) has an impact on Cyber Hygiene Behavior (CHB).

H4: Moral Norms (MN) have a positive impact on Behavioral Intention (BI).

H5: Perceived Behavioral Control (PBC) has a positive impact on Behavioral Intention (BI).

H6: Perceived Behavioral Control (PBC) has a positive impact on Cyber Hygiene Behavior (CHB).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.7 *Construct reliability and validity – secondary model estimated (sample size: 165 records from Romania)*

Construct	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
BI	0.707	0.726	0.808	0.458
CHB	0.543	0.559	0.812	0.685
DN	0.612	0.622	0.774	0.463
JU	0.640	0.677	0.783	0.476
MN	0.705	0.726	0.819	0.535
PBC	0.674	1.239	0.688	0.382

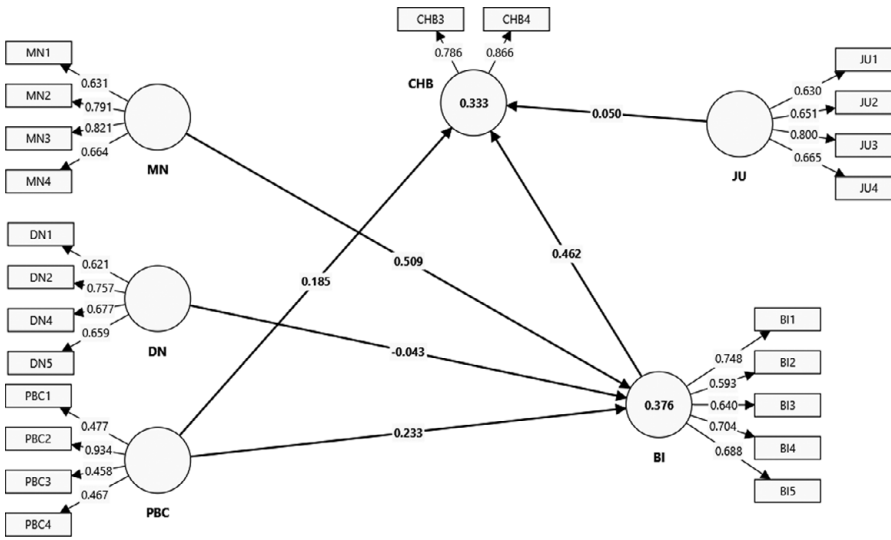


FIGURE 5.3 The final model with estimated coefficients (sample size: 165 records from Romania).

The same reliability and validity verification was done for the Romania model (Table 5.7).

Path Coefficients and R^2 constructs are included in Table 5.8.

Table 5.9 covers the Bootstrapping Path Coefficients values for the final model as well as the decisions on the proposed hypotheses acceptance or rejection.

The results of the tests indicate that the proposed constructs (i.e., MN, PBC) have a weak or moderate impact on the intention and behavior of students (expressed as BI, CHB) to avoid the disinformation. In this research, the threshold of the *P* value is also 0.05. Therefore, in this research, hypotheses H1, H4, H5, and H6 are supported, but hypotheses H2 and H3 are rejected. This means that: (1) Behavioral Intention (BI) impacts on Cyber Hygiene Behavior (CHB); (2) Moral Norms (MN) have a moderate

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

TABLE 5.8 *PLS Algorithm R^2 and Path Coefficients (sample size: 165 records from Romania)*

	R^2	BI	CHB	DN	JU	MN	PBC
BI	0.376		0.462				
CHB	0.333						
DN		−0.043					
JU			0.050				
MN		0.509					
PBC		0.233	0.185				

TABLE 5.9 *Bootstrapping Path Coefficients for the final model (sample size: 165 records from Romania)*

Hypothesis No	Hypothesis (impact direction à)	Original sample	Sample mean	Standard deviation	T-statistics	*P* values	Decision
H1	BI à CHB	0.462	0.450	0.101	4.578	0.000	Accepted
H2	DN à BI	−0.043	−0.007	0.098	0.434	0.665	Rejected
H3	JU à CHB	0.050	0.076	0.085	0.589	0.556	Rejected
H4	MN à BI	0.509	0.519	0.071	7.131	0.000	Accepted
H5	PBC à BI	0.233	0.232	0.090	2.591	0.010	Accepted
H6	PBC à CHB	0.185	0.191	0.077	2.413	0.016	Accepted

impact on Behavioral Intention (BI); (3) Perceived Behavioral Control (PBC) has a weak positive impact on Behavioral Intention (BI); (4) Perceived Behavioral Control (PBC) has a weak positive impact on Cyber Hygiene Behavior (CHB).

CONCLUSION

Cyber disinformation is a complex and concerning phenomenon. Successful disinformation campaigns can have a significant negative effect on democratic values and institutions. Defending democracy in the digital age requires a complex approach. The individual behavior of users can influence the spread and effects of the phenomenon.

This chapter argued that users' behavior plays an essential role in this phenomenon and aimed to identify factors that impact on users' BIs and CHB. The chapter integrated the ETPB and a Structural Equation Model, realized through PLS–SEM, applied to the cyber disinformation phenomenon. The analysis of the self-assessment survey on disinformation risk perception and control revealed that responses are highly similar, with a correlation rate of 0.7854. The research revealed the applicability of the TPB model and found that MN and PBC have an impact on BI and CHB.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

The findings of this chapter provide valuable insights that can be used to improve the overall responses to the phenomenon, such as policies, programs, and clinics, and to elaborate educational materials. To effectively address the phenomenon's relevant vectors, tactics, or methods, there is a clear need for a complex strategy, with multiple components, including research, to better understand the phenomenon's attributes and the behavior of users; frequent risk assessments; increased empowerment of people to detect and report disinformation; improved fact-checking procedures; enhanced international anti-disinformation enforcement and cooperation; technical assistance programs; better defined responsibility for secondary liability; awareness raising and education programs, with a view to improve the critical thinking abilities of people.

REFERENCES

Ababneh, K. I., Ahmed, K., & Dedousis, E. (2022). Predictors of cheating in online exams among business students during the Covid pandemic: Testing the theory of planned behavior. *International Journal of Management Education*, *20*(3), 1–15. https://doi.org/10.1016/j/ijme.2922.100713

Aïmeur, E., Amri, S., & Brassard, G. (2023). Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, *13*(1), 30. https://link.springer.com/article/10.1007/s13278-023-01028-5

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

(2005). *Attitudes, personality, and behavior*. New York: Open University Press.

Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. *International Journal of Advanced Computer Science and Applications*, *13*(8), 479–490.

Alieva, I., Moffitt, J. D., & Carley, K. M. (2022). How disinformation operations against Russian opposition leader Alexei Navalny influence the international audience on Twitter. *Social Network Analysis and Mining*, *12*(1), 1–13. https://doi.org/10.1007/s13278-022-00908-6

Andersen, J. & Søe, S. O. (2020). Communicative actions we live by: The problem with fact-checking, tagging or flagging fake news – The case of Facebook. *European Journal of Communication*, *35*(2), 126–139. https://doi.org/10.1177/0267323119894489

Arayankalam, J. & Krishnan, S. (2021). Relating foreign disinformation through social media, domestic online media fractionalization, government's control over cyberspace, and social media-induced offline violence: Insights from the agenda-building theoretical perspective. *Technological Forecasting and Social Change*, *166*, 1–14. https://doi.org/10.1016/j.techfore.2021.120661

Benson, T. (2020, July 29). *Twitter bots are spreading massive amounts of COVID-19 misinformation*. IEEE Spectrum. https://spectrum.ieee.org/twitter-bots-are-spreading-massive-amounts-of-covid-19-misinformation

Bontcheva, K., Posetti, J., Teyssou, D., Meyer, T., Gregory, S., Hanot, C., & Maynard, D. (2020). *Balancing act: Countering digital disinformation while respecting freedom of expression*. United Nations Educational, Scientific and Cultural Organization

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

(UNESCO). https://unesco.org/en/articles/balancing-act-countering-digital-disinformation-while-respecting-freedom-expression

Borges, P. M. & Gambarato, R. R. (2019). The role of beliefs and behavior on Facebook: A semiotic approach to algorithms, fake news, and transmedia journalism. *International Journal of Communication*, *13*, 603–618. https://ijoc.org/index.php/ijoc/article/view/10304/2550

Buchanan, T. & Benson, V. (2019). Spreading disinformation on Facebook: Do trust in message source, risk propensity, or personality affect the organic reach of "fake news"? *Social Media+ Society*, *5*(4), 1–9. https://doi.org/10.1177/2056305119888654

Cabeza-Ramirez, L. J., Sanchez-Canizares, S. M., Santos-Roldan, L. M., & Fuentes-Garcia, F. J. (2022). Impact of the perceived risk in influencers' product recommendations on their followers' purchase attitudes and intention. *Technological Forecasting and Social Change*, *184*, 1–16. https://doi.org/10.1016/j.techfore.2022.121997

Caramancion, K. M., Li. Y., Dubois, E., & Jung E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. *Data*, *7*(4), 1–18. https://doi.org/10.3390/data7040049

Carrapico, H. & Farrand, B. (2021). When trust fades, Facebook is no longer a friend: Shifting privatisation dynamics in the context of cybersecurity as a result of disinformation, populism and political uncertainty. *JCMS: Journal of Common Market Studies*, *59*(5), 1160–1176. https://doi.org/10.1111/jcms.13175

Carratalá, A. (2023). Disinformation and sexual and gender diversity in Spain: Twitter users' response, and the perception of LGBTQI+ organisations. *Social Sciences*, *12*(4), 1–19. https://doi.org/10.3390/socsci12040206

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*, 1753–1820.

Chuttur, M. (2009). Overview of the technology acceptance model: Origins, developments and future directions. *Sprouts: Working Papers on Information Systems*, *9*(37), 1–22.

Collins, B., Hoang, D. T., Nguyen, N. T., & Hwang, D. (2021). Trends in combating fake news on social media – A survey. *Journal of Information and Telecommunication*, *5*(2), 247–266. https://doi.org/10.1080/24751839.2020.1847379

Collins, L. M. (2007). Research design and methods, encyclopedia of gerontology. In *Encyclopedia of gerontology* (pp. 433–442). Elsevier. https://doi.org/10.1016/B0-12-370870-2/00162-1

Culloty, E., Suiter, J., Viriri, I., & Creta, S. (2022). Disinformation about migration: An age-old issue with new tech dimensions. In *World migration report* (pp. 1–23). International Organization for Migration.

Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Tactics of disinformation*. CISA. https://cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Doctoral dissertation, Massachusetts Institute of Technology. https://researchgate.net/publication/35465050

Diekman, C., Ryan, C. D., & Oliver, T. L. (2023). Misinformation and disinformation in food science and nutrition: Impact on practice. *Journal of Nutrition*, *153*(1), 3–9. https://doi.org/10.1016/j.tjnut.2022.10.001

Edwards, C., Beattie, A. J., Edwards, A., & Spence, P. R. (2016). Differences in perceptions of communication quality between a Twitterbot and human agent for information seeking and learning. *Computers in Human Behavior*, *65*, 666–671. https://doi.org/10.1016/j.chb.2016.07.003

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

European Commission. (2020). On the European Democracy Action Plan, COM (2020), 790. EU Monitor.

(2023). *Digital services act: Application of the risk management framework to Russian disinformation campaigns*. Publications Office of the European Union.

European Parliament. (2022). Resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268 (INI)) (2022/C 347/07). European Parliament. https://europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html

European Parliamentary Research Service. (2020, April 9). *Disinformation and science: A survey of the gullibility of students with regard to false scientific news*. European Parliament, Panel for the Future of Science and Technology (STOA). https://europarl.europa.eu/RegData/etudes/STUD/2020/656300/EPRS_STU(2020)656300_EN.pdf

Falk, R. F., & N. B. Miller (1992). *A primer for soft modeling*. The University of Akron Press.

Fallis, D. (2014). The varieties of disinformation. In Floridi, L., & Illari, P. (Eds.), *The philosophy of information quality* (pp. 135–161). Synthese Library.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.2307/3151312

Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage.

Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer Nature.

Jankelová, N., Joniaková, Z., & Skorková, Z. (2021). Perceived organizational support and work engagement of first-line managers in healthcare – The mediation role of feedback seeking behavior. *Journal of Multidisciplinary Healthcare*, *14*, 3109–3123. https://doi.org/10.2147/JMDH.S326563

Jia, H., Yu, J., Feng, T., Ning, L., Cao, P., Shang, P., Gao, S., & Yu, X. (2022). Factors influencing medical personnel to work in primary health care institutions: An extended theory of planned behavior. *International Journal of Environmental Research and Public Health*, *19*(5), 1–15. https://doi.org/10.3390/ijerph19052785

Jungherr, A., & Schroeder, R. (2021). Disinformation and the structural transformations of the public arena: Addressing the actual challenges to democracy. *Social Media+ Society*, *7*(1), 1–13. https://doi.org/10.1177/2056305121988928

Khani Jeihooni, A., Layeghiasl, M., Yari, A., & Rakhshani, T. (2022). The effect of educational intervention based on the theory of planned behavior on improving physical and nutrition status of obese and overweight women. *BMC Women's Health*, *22*(1), 1–9. https://doi.org/10.1186/s12905-022-01-01593-5

Knight Foundation. (2018, October). *Disinformation, 'fake news' and influence campaigns on Twitter*. Knight Foundation. https://s3.amazonaws.com/kf-site-legacy-media/feature_assets/www/misinfo/kf-disinformation-report.ocdbb232.pdf

Kock, N. (2014). *Stable P value calculation methods in PLS-SEM*. ScriptWarp Systems. https://researchgate.net/publication/269989910_Stable_P_value_calculation_methods_in_PLS-SEM

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

Machete, P., & Turpin, M. (2020). The use of critical thinking to identify fake news: A systematic literature review. In M. Hattingh, M. Matthee, H. Smuts, I. Pappas, Y. K.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

Dwivedi, & M. Mantymaki (Eds.), *Responsible design, implementation and use of information and communication technology* (pp. 235–246). Springer International Publishing. https://doi.org/10.1007/978-3-030-45002-1_20

Maheri, M., Rezapour, B., & Didarloo, A. (2022). Predictors of colorectal cancer screening intention based on the integrated theory of planned behavior among the average-risk individuals. *BMC Public Health*, *22*(1), 1–11. https://doi.org/10.1186/s12889-022-14191-9

Marikyan, M., & Papagiannidis, P. (2021). *Unified theory of acceptance and use of technology*. TheoryHub Book.

Mattioli, R., Malatras, A., Hunter, E. N., Biasibetti Penso, M. G., Bertram, D., & Neubert, I. (2023). *Identifying emerging cyber security threats and challenges for 2030*. ENISA.

Michaelis, M., Jafarian, J. H., & Biswas, A. (2022). The dangers of money and corporate power relating to online disinformation. In *2022 23rd IEEE international conference on mobile data management (MDM)* (pp. 470–475). IEEE.

Nenadić, I. (2019). Unpacking the "European approach" to tackling challenges of disinformation and political manipulation. *Internet Policy Review*, *8*(4), 1–22. https://doi.org/10.14763/2019.4.1436

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. McGraw-Hill.

Ó Fathaigh, R., Helberger, N., & Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, *10*(4), 1–25. https://doi.org/10.14763/2021.4.1584

Olan, F., Jayawickrama, U., Arakpogun, E. O., Suklan, J., & Liu, S. (2022). Fake news on social media: The impact on society. *Information Systems Frontiers*, *26*, 443–458. https://doi.org/10.1007/s10796-022-10242-z

Park, E. S., & Park, M. S. (2020). Factors of the technology acceptance model for construction IT. *Applied Sciences*, *10*(22), 1–15. https://doi.org/10.3390/app10228299

Pérez-Escolar, M., Lilleker, D., & Tapia-Frade, A. (2023). A systematic literature review of the phenomenon of disinformation and misinformation. *Media and Communication*, *11*(2), 76–87. https://doi.org/10.17645/mac.v11i2.6453

Pierri, F., Artoni, A., & Ceri, S. (2020). Investigating Italian disinformation spreading on Twitter in the context of 2019 European elections. *PLOS One*, *15*(1), 1–23. https://doi.org/10.1371/journal.pone.0227821

Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE Access*, *10*, 25494–25513.

Ringle, C. M., Hair, J. F., & Sarstedt, M. (2014). PLS-SEM: Looking back and moving forward. *Long Range Planning*, *47*(3), 132–137. https:/doi.org/10.1016/j.lrp.2014.02.008

Romero-Galisteo, R.-P., Gonzalez-Sanches, M., Galvez-Ruiz, P., Palomo-Carrion, R., Casuso-Holgado, M. J., & Pinero-Pinto E. (2022). Entrepreneurial intention, expectations of success and self-efficacy in undergraduate students of health sciences. *BMC Medical Education*, *22*(1), 1–7. https://doi.org/10.1186/s12909-022-03731-x

Sabi, H. M., Uzoka, F. M. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management*, *36*(2), 183–191. https://doi.org/10.1016/j.ijinfomgt.2015.11.010

Savari, M., Mombeni, A. S., & Izadi, H. (2022). Socio-psychological determinants of Iranian rural households' adoption of water consumption curtailment behaviors. *Scientific Reports*, *12*(1), 1–12. https://doi.org/10.1038/s41598-022-17560-x

Schünemann, W. J. (2022). A threat to democracies?: An overview of theoretical approaches and empirical measurements for studying the effects of disinformation. In M. D. Cavelty & A. Wenger (Eds.), *Cyber security politics* (pp. 32–47). Routledge.

Shirahada, K., & Zhang, Y. (2022). Counterproductive knowledge behavior in volunteer work: Perspectives from the theory of planned behavior and well-being theory. *Journal of Knowledge Management*, *26*(11), 22–41. https://doi.org/10.1108/JKM-08-2021-0612

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

Statista. (2023). Number of disinformation and pro-Russian Twitter posts in Poland 2023. *Statista*. https://statista.com/statistics/1365122/number-of-disinformation-and-pro-russian-twitter-posts-poland/

Tenove, C., & Tworek, H. J. S. (2019). Online disinformation and harmful speech: Dangers for democratic participation and possible policy responses. *Journal of Parliamentary and Political Law, 13*, 215–232.

Ternovski, J., Kalla, J., & Aronow, P. (2022). The negative consequences of informing voters about deepfakes: Evidence from two survey experiments. *Journal of Online Trust and Safety*, *1*(2), 1–16. https://doi.org/10.54501/jots.v1i2.28

Trend Micro. (2020). *Malicious uses and abuses of artificial intelligence*. United Nations Interregional Crime & Justice Research Institute. https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf

Uyheng, J., Moffitt, J. D., & Carley, K. M. (2022). The language and targets of online trolling: A psycholinguistic approach for social cybersecurity. *Information Processing and Management*, *59*(5), 1–15. https://doi.org/10.1016/j.ipm.2022.103012

Vaccari, C. & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media and Society*, *6*(1), 1–13. https://doi.org/10.1177/2056305120903408

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

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

Watson, A. (2021). Main sources of disinformation as ranked by journalists worldwide as of June 2020. *Statista*. https://statista.com/statistics/1249671/journalists-cite-sources-disinformation-worldwide/

Weikmann, T., & Lecheler, S. (2022). Visual disinformation in a digital age: A literature synthesis and research agenda. *New Media & Society*, *25*(12), 3696–3713. https://doi.org/10.1177/14614448221141648.

Zhang, H., Shi, Z., Chen, J., & Zhang, Z. (2022). Understanding combined health and business risk behavior: Small tourism firm owners reopening amid Covid-19 in Pingyao, China. *Behavioral Sciences (Basel)*, *12*(10), 1–18. https://doi.org/10.3390/bs12100358

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 13 Nov 2026 at 22:59:15, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009574105.006